SYSTÈME D'EXPLOITATION PARTIE 3

Introduction aux réseaux

Les modèles OSI et TCP/IP

Introduction aux réseaux : Modèles OSI et TCP/IP

Dans le monde des réseaux informatiques, deux modèles sont souvent utilisés pour comprendre comment les données circulent à travers un réseau :

- le modèle OSI : Un modèle théorique à 7 couches, utilisé principalement pour comprendre le fonctionnement des réseaux.
- Le modèle TCP/IP : Un modèle pratique et réel à 4 couches, utilisé pour l'Internet et les réseaux modernes. et le modèle TCP/IP.

Introduction aux réseaux : Modèles OSI

Le modèle OSI est un modèle théorique qui décrit comment les communications se produisent dans un réseau informatique. Il est divisé en 7 couches, chacune ayant une fonction spécifique.

1. **Couche 1 - Physique :** Bits

   Les données sont envoyées sous forme de signaux binaires (0 et 1) sur le support physique, comme les câbles ou la fibre optique.

2. **Couche 2 - Liaison de données :** Trame

   Une trame est un paquet de données contenant l'adresse MAC d'origine et de destination. Elle est utilisée pour la transmission sur le réseau local.

3. **Couche 3 - Réseau :** Paquet

   Un paquet contient l'adresse IP source et de destination. Il permet d'acheminer les données à travers différents réseaux (routeur).

Introduction aux réseaux : Modèles OSI

4. **Couche 4 - Transport :** Segment

Un segment contient les données de l'application et les informations de contrôle nécessaires au transport, comme le numéro de port. C'est le cas avec TCP ou UDP.

5. **Couche 5 - Session :**

Cette couche gère l'ouverture et la fermeture des sessions de communication. Elle ne crée pas d'unité de données distincte comme les autres couches, mais elle organise la gestion de la communication.

Exemple : Lorsqu'un utilisateur se connecte à un site web, une session HTTP est ouverte entre le navigateur et le serveur web. Si l'utilisateur navigue entre plusieurs pages, la session est maintenue ouverte pour la durée de la visite.

6. **Couche 6 - Présentation :**

La couche de présentation gère la syntaxe et la sémantique des données. Elle a pour rôle de convertir les données dans un format compréhensible pour l'application de destination. Elle peut aussi compresser les données ou les chiffrer.

Exemple : avant d'envoyer un fichier compressé (ZIP), les données sont transformées en un format compressé pour économiser de l'espace.

Introduction aux réseaux : Modèles OSI

7. **Couche 7 - Application :** Données (ou PDU - Protocol Data Unit)

   Les données qui sont envoyées et reçues par les applications de l'utilisateur.

Exemple : Lorsque tu ouvres un navigateur web et accèdes à un site, le protocole HTTP ou HTTPS permet à ton navigateur d'envoyer et de recevoir des données au serveur du site web.

Introduction aux réseaux : Modèles TCP/IP

Le modèle TCP/IP, contrairement à l'OSI, est plus simple et plus directement lié à la manière dont Internet fonctionne. Il est composé de 4 couches. Ce modèle est largement utilisé dans les réseaux réels, y compris l'Internet.

1. **Couche 1 - Accès au réseau :** Bits ou trame

   Cette couche concerne la transmission physique. Elle peut aussi utiliser des trames, comme dans le modèle OSI, selon le type de technologie utilisée (Ethernet, Wi-Fi, etc.).

2. **Couche 2 - Internet :** Paquet

   Comme dans l'OSI, le paquet est l'unité de données qui contient l'adresse IP pour le routage entre les réseaux.

3. **Couche 3 - Transport :** Segment (pour TCP) ou Datagramme (pour UDP)

   Les segments (pour TCP) ou datagrammes (pour UDP) contiennent les données de l'application et des informations supplémentaires pour assurer la communication fiable (pour TCP) ou non fiable (pour UDP).

4. **Couche 4 - Application :** Données (ou PDU - Protocol Data Unit)

   Cette couche utilise les mêmes unités de données que la couche 7 du modèle OSI. Les données envoyées par les applications peuvent être sous forme de fichiers, requêtes, réponses, etc.

Introduction aux réseaux : Modèles OSI et TCP/IP

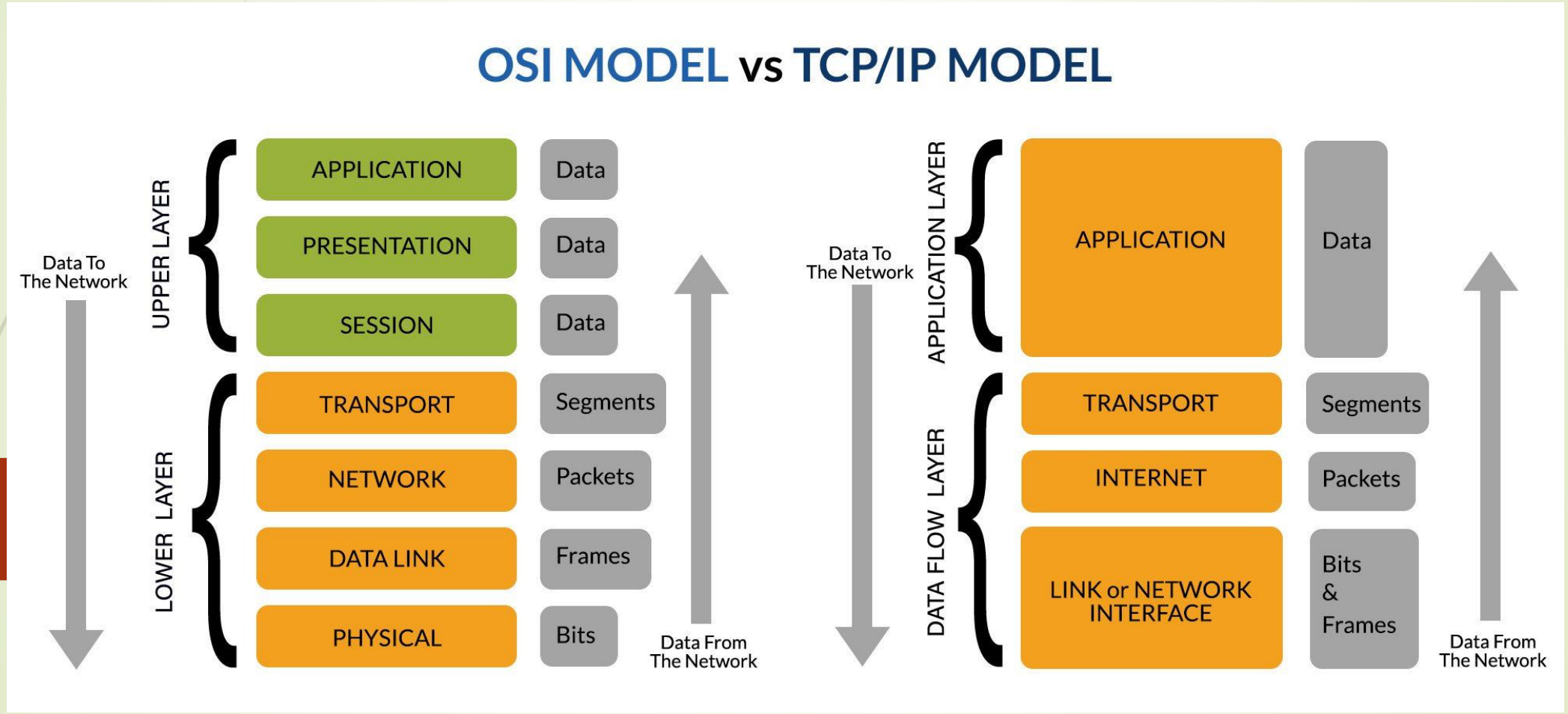


Image récupérée depuis le site : https://www.rtautomation.com/rtas-blog/a-refresher-course-on-osi-tcp-ip/

Les protocoles de transport TCP et UDP

Introduction aux réseaux : TCP et UDP

1. TCP (Transmission Control Protocol)

TCP est un protocole fiable, utilisé pour assurer que les données arrivent correctement et dans le bon ordre à destination. Il établit une connexion entre l'expéditeur et le destinataire avant de commencer l'échange de données, et il garantit que toutes les données envoyées sont reçues, avec un mécanisme de contrôle des erreurs et de retransmission en cas de perte de données.

Exemple : Lorsque vous visitez un site web, TCP est utilisé pour établir une connexion fiable entre votre navigateur et le serveur web afin d'assurer que toutes les pages et éléments de la page arrivent correctement.

2. UDP (User Datagram Protocol)

UDP est un protocole non fiable et plus rapide que TCP. Contrairement à TCP, il n'établit pas de connexion avant d'envoyer les données et il ne vérifie pas si les données sont bien arrivées. Cela le rend plus rapide, mais moins sûr.

Exemple : Les jeux en ligne utilisent UDP pour envoyer les données de manière rapide entre le serveur et le joueur. La vitesse de la communication est essentielle, et il est préférable de sacrifier la fiabilité pour éviter un retard dans le jeu (par exemple, un déplacement rapide du personnage).

Introduction aux réseaux : TCP et UDP

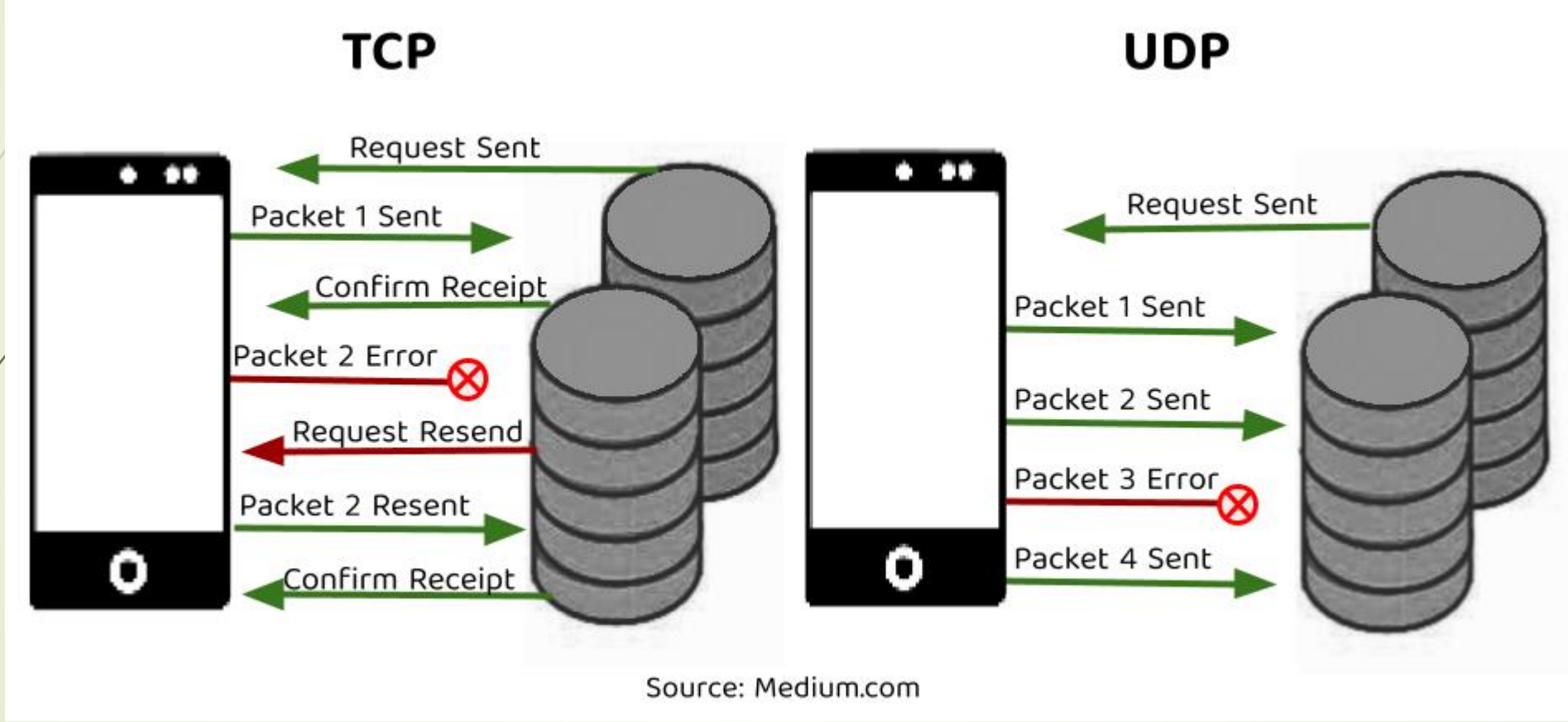


Image récupérée depuis le site : https://www.privateinternetaccess.com/blog/tcp-vs-udp-understanding-the-difference/

Les adresse IP et adresses MAC

Introduction aux réseaux : Adresse IP et adresse MAC

1. Adresse IP :

L'adresse IP (Internet Protocol) est un identifiant unique utilisé pour localiser un appareil (ordinateur, smartphone, serveur, etc.) sur un réseau. Il existe deux types principaux d'adresses IP : IPv4 et IPv6.

- **IPv4** : C'est la version la plus courante. Elle se compose de 4 nombres séparés par des points, chaque nombre étant compris entre 0 et 255. Par exemple :192.168.1.1.
- **IPv6** : C'est une version plus récente de l'adresse IP, utilisée pour gérer le manque d'adresses IP disponibles avec IPv4. Elle utilise des groupes de chiffres hexadécimaux séparés par des colons. Exemple :2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Introduction aux réseaux : Adresse IP et adresse MAC

IP publique et IP privée

- Adresse IP publique :

C'est l'adresse qui est attribuée à votre réseau lorsque vous êtes connecté à Internet. Elle est unique à l'échelle mondiale, et c'est cette adresse qui permet à votre réseau de communiquer avec d'autres réseaux, comme Internet.

Exemple : 203.0.113.45.

- Adresse IP privée :

Ce sont des adresses utilisées à l'intérieur d'un réseau local (LAN). Elles ne sont pas visibles sur Internet et sont utilisées pour connecter des appareils entre eux dans une maison, une entreprise, etc. Les plages d'adresses IP privées sont définies par la norme :

Classe A : 10.0.0.0 à 10.255.255.255

Classe B : 172.16.0.0 à 172.31.255.255

Classe C : 192.168.0.0 à 192.168.255.255

Introduction aux réseaux : Adresse IP et adresse MAC

2. Adresse MAC :

L'adresse MAC (Media Access Control) est un identifiant unique attribué à une carte réseau (ou à un appareil réseau). Une adresse MAC est composée de 6 octets (48 bits) et peut être divisée en deux parties principales :

- Les 3 premiers octets (OUI - Organizationally Unique Identifier) :

Identifient le fabricant de l'appareil. Par exemple, dans l'adresse 00:14:22:01:23:45, 00:14:22 indique le fabricant.

- Les 3 derniers octets (NIC - Network Interface Controller) :

Identifient l'appareil spécifique du fabricant, garantissant que chaque appareil a une adresse unique. Dans l'exemple 00:14:22:01:23:45, 01:23:45 identifie l'appareil particulier.

Cette division permet d'assurer des adresses MAC uniques pour chaque appareil tout en identifiant le fabricant.

Fonction des composants du réseau

Introduction aux réseaux : composants du réseau

Les routeurs

Introduction aux réseaux : composants du réseau

Les routeurs

Les routeurs fonctionnent au niveau de la couche réseau du modèle OSI et utilisent l'adressage logique (tel que les adresses IP) pour déterminer le meilleur chemin pour que les paquets atteignent leur destination.

Ils analysent l'adresse IP de destination dans l'en-tête du paquet et la comparent à leur table de routage pour déterminer le prochain saut sur le chemin vers la destination.

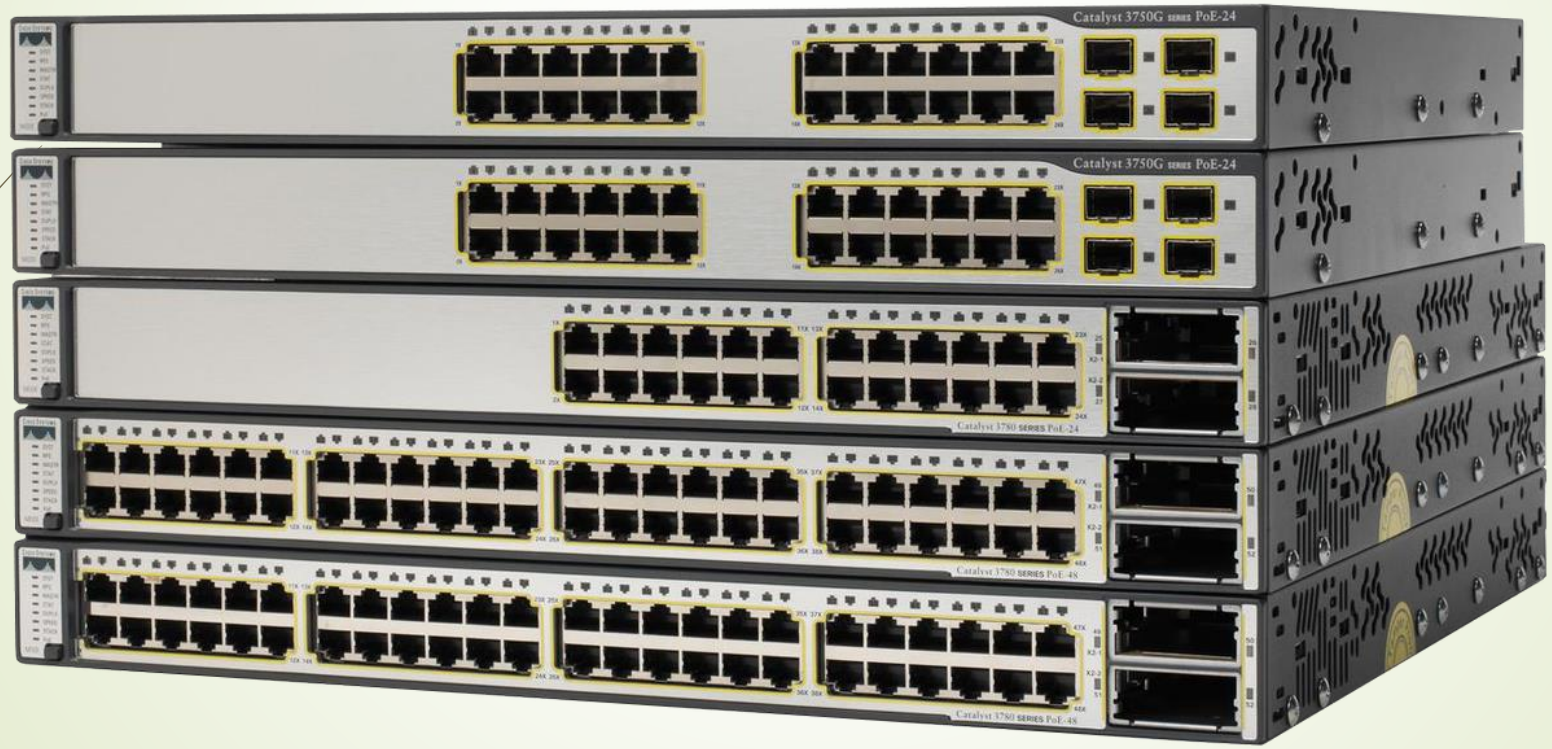
Introduction aux réseaux : composants du réseau

Les routeurs (fonctions)

Transfert de paquets	transfert de paquets entre différents réseaux. Ils examinent l'adresse IP de destination dans l'en-tête du paquet et transmettent le paquet au prochain saut sur le chemin vers la destination.
Détermination du chemin	détermine le meilleur chemin pour que les données circulent entre différents réseaux en utilisant des protocoles de routage, tels que OSPF ou BGP, pour échanger des informations de routage avec d'autres routeurs.
Filtrage du trafic	filtre le trafic en fonction de divers critères, notamment l'adresse IP source, l'adresse IP de destination, le numéro de port et le type de protocole. Cela permet aux administrateurs réseau de contrôler quel trafic est autorisé à transiter par le routeur.
Segmentation du réseau	utilisée pour diviser un réseau plus vaste en sous-réseaux plus petits, chacun avec sa propre plage d'adresses IP unique. Cela contribue à améliorer les performances et la sécurité du réseau en réduisant la taille du domaine de diffusion.

Introduction aux réseaux : composants du réseau

Les switchs



Introduction aux réseaux : composants du réseau

Les switchs (commutateur couche 2)

Les commutateurs couche 2 connectent les appareils au sein du même réseau en utilisant des adresses MAC pour transférer les données vers le bon appareil, aidant ainsi à organiser et à contrôler efficacement le trafic réseau.

Ils utilisent une technique appelée apprentissage d'adresse MAC(MAC learning) pour remplir un tableau avec les adresses MAC des appareils connectés à chacun de leurs ports.

Lorsqu'un appareil envoie une trame à un autre appareil sur le même segment de réseau, le commutateur transmet la trame uniquement au port où se trouve l'adresse MAC de destination, réduisant ainsi le trafic réseau inutile.

Introduction aux réseaux : composants du réseau

Les switchs (commutateur couche 3)

Les commutateurs couche 3 combinent les fonctionnalités des routeurs et des commutateurs. Ils peuvent diriger les données au sein d'un réseau à l'aide d'adresses IP (contrairement aux commutateurs L2).

Ceci est utile pour gérer le trafic entre différents sous-réseaux, ainsi que de la possibilité d'effectuer un routage IP entre différents sous-réseaux ou réseaux.

Il utilise des protocoles de routage, tels que OSPF ou BGP, pour échanger des informations de routage avec d'autres appareils et déterminer le meilleur chemin pour que les paquets IP atteignent leur destination.

Introduction aux réseaux : composants du réseau

Les pare-feu next generation et IPS

Introduction aux réseaux : composants du réseau

Les Pare-feu next generation et IPS

Un pare-feu est un système de sécurité qui protège un réseau informatique en surveillant et en contrôlant le trafic (les données qui entrent et sortent) en fonction de règles de sécurité pré-définies.

Un Pare-feu Next-Generation (NGFW) est une version plus avancée et plus intelligente d'un pare-feu traditionnel. En plus de bloquer les connexions non autorisées (comme un pare-feu classique), le NGFW fait bien plus :

- Analyse du contenu : Il peut analyser le contenu des données pour détecter des menaces, comme des virus ou des attaques qui utilisent des fichiers malveillants.
- Contrôle des applications : Il peut identifier et bloquer des applications spécifiques, même si elles utilisent des ports qui sont habituellement ouverts.
- Protection contre les attaques avancées : Il offre une défense contre les menaces de plus en plus complexes, comme les attaques provenant de l'intérieur du réseau.
- Gestion des utilisateurs : Il permet de gérer qui peut accéder à quoi, selon l'identité de l'utilisateur et le type d'appareil qu'il utilise.

Introduction aux réseaux : composants du réseau

Les Pare-feu next generation et IPS

Un pare-feu est un système de sécurité qui protège un réseau informatique en surveillant et en contrôlant le trafic (les données qui entrent et sortent) en fonction de règles de sécurité pré-définies.

Un Pare-feu Next-Generation (NGFW) est une version plus avancée et plus intelligente d'un pare-feu traditionnel. En plus de bloquer les connexions non autorisées (comme un pare-feu classique), le NGFW fait bien plus :

- Analyse du contenu : Il peut analyser le contenu des données pour détecter des menaces, comme des virus ou des attaques qui utilisent des fichiers malveillants.
- Contrôle des applications : Il peut identifier et bloquer des applications spécifiques, même si elles utilisent des ports qui sont habituellement ouverts.
- Protection contre les attaques avancées : Il offre une défense contre les menaces de plus en plus complexes, comme les attaques provenant de l'intérieur du réseau.
- Gestion des utilisateurs : Il permet de gérer qui peut accéder à quoi, selon l'identité de l'utilisateur et le type d'appareil qu'il utilise.

Concepts Clés et Pratiques Avancées en IT

HA (High Availability) / Haute Disponibilité

Définition :

La haute disponibilité fait référence à un système conçu pour être opérationnel pendant une période prolongée sans interruption. Cela implique souvent des architectures redondantes pour minimiser les pannes.

Exemple :

Un serveur ayant plusieurs points de redondance, comme un système de basculement (failover), où si un serveur tombe en panne, un autre serveur prend immédiatement la relève.

Concepts Clés et Pratiques Avancées en IT

Best Practices (Bonnes Pratiques)

Définition :

Des méthodes et des pratiques recommandées qui, au fil du temps et de l'expérience, ont prouvé leur efficacité dans la gestion de systèmes et dans le développement de logiciels.

Exemple :

Utilisation de gestionnaires de versions comme Git pour un développement collaboratif ou mise en place de tests unitaires pour assurer la qualité du code.

Concepts Clés et Pratiques Avancées en IT

Load Balancing

Définition :

Le processus de distribution uniforme de la charge de travail (requêtes, processus, etc.) sur plusieurs serveurs ou ressources afin d'assurer la performance, la disponibilité et la redondance du système.

Exemple :

Un répartiteur de charge (load balancer) qui envoie les requêtes utilisateurs à différents serveurs afin d'éviter qu'un seul serveur soit surchargé.