TSSR

By kAly

Created : 21/04/2024 - Modified : 24/04/2024

TABLE DES MATIÈRES

LEXIQUE

A. Concepts réseaux fondamentaux

Réseau : Ensemble d'équipements (ordinateurs, serveurs, périphériques, etc.) interconnectés dans le but de partager des ressources (données, applications, accès Internet, etc.) et de communiquer entre eux.
IP (Internet Protocol) : Ensemble de règles qui permettent aux appareils connectés à Internet de communiquer entre eux en attribuant une adresse unique (adresse IP) à chaque appareil.
Protocole : Ensemble de règles et normes qui permettent la communication entre différents composants d'un réseau (ex: TCP/IP, HTTP, DHCP).
Adresse MAC (Media Access Control) : Identifiant unique attribué à chaque carte réseau, permettant d'identifier un appareil sur un réseau.

B. Protocoles et standards majeur

TCP (Transmission Control Protocol) : Protocole qui assure la transmission fiable et ordonnée des données entre deux appareils. Il vérifie que toutes les données sont bien reçues et dans le bon ordre.

Modèle TCP/IP :

- Couche Application
- Couche Transport
- Couche Internet (ou Réseau)
- Couche Accès réseau

OSI (Open Systems Interconnection) :

Modèle OSI (Open Systems Interconnection) :

- Couche Application
- Couche Présentation
- Couche Session
- Couche Transport
- Couche Réseau
- Couche Liaison de données
- Couche Physique

UDP (User Datagram Protocol) : Protocole plus rapide que TCP mais moins fiable, utilisé lorsque l'ordre de réception des données n'est pas important (streaming vidéo, jeux en ligne, etc.).

DNS (Domain Name System) : Système qui fait la correspondance entre les noms de domaine faciles à mémoriser (exemple.com) et les adresses IP utilisées par les appareils.
DHCP (Dynamic Host Configuration Protocol) : Protocole qui attribue automatiquement une adresse IP et d'autres paramètres de configuration aux appareils qui se connectent à un réseau.

Les 4 phases du processus DHCP

1. **Phase de découverte (DHCP Discover) :** Le client DHCP diffuse un message de découverte pour localiser un serveur DHCP sur le réseau.
2. **Phase d'offre (DHCP Offer) :** Si un serveur DHCP reçoit le message de découverte, il répond au client avec un message d'offre contenant une adresse IP proposée, ainsi que d'autres paramètres de configuration comme le masque sous réseau, la passerelle par défaut etc....
3. **Phase de requête (DHCP Request) :** Le client DHCP répond au serveur avec un message de requête pour accepter l'offre proposée. Ce message peut également être diffusé si le client a reçu plusieur offre et doit en choisir une
4. **Phase d'accusé de réception (DHCP Ackowledge) :** Enfin, le serveur DHCP envoie un message d'accusé de réception pour confirmer l'attribution de l'adresse IP et des autres paramètres de configuration au client.

Ces quatre phases permettent au client DHCP d'obtenir automatiquement une configuration IP fonctionnelle sur le réseau. Le processus DHCP simplifie grandement la gestion des adresses IP dans les environnements réseau dynamiques.
SSL/TLS : Protocoles cryptographiques qui chiffrent les données échangées sur Internet, assurant une communication sécurisée (utilisés notamment pour le https://).
HTTP (Hypertext Transfer Protocol) : Principal protocole utilisé pour la transmission des données sur le World Wide Web. Il définit la syntaxe et les règles de communication entre un client (généralement un navigateur web) et un serveur web pour échanger des pages web, des images, des vidéos et d'autres contenus.
HTTPS (Hypertext Transfer Protocol Secure) : Version sécurisée et chiffrée du protocole HTTP. HTTPS utilise un mécanisme de chiffrement (généralement SSL/TLS) pour crypter les données échangées entre le client et le serveur web. Cela garantit la confidentialité et l'intégrité des communications, protégeant contre les écoutes et les altérations des données. HTTPS est essentiel pour les transactions sécurisées comme les opérations bancaires en ligne.

C. Equipements réseaux

Routeur : Appareil qui achemine les données entre différents réseaux (Internet, réseaux locaux, etc.) en choisissant les meilleurs chemins.
Commutateur (Switch) : Dispositif qui connecte plusieurs appareils sur un même réseau local et achemine les données entre eux.
Pont : Dispositif permettant de relier deux segments de réseau local et de filtrer le trafic entre eux.
Proxy : Serveur intermédiaire qui fait transiter les requêtes des utilisateurs vers Internet et vice-versa, permettant de filtrer ou cacher les connexions.
Firewall : Dispositif de sécurité réseau qui applique des règles pour contrôler le trafic entrant et sortant d'un réseau.

D. Réseaux Locaux

LAN (Local Area Network) : Réseau informatique couvrant une zone géographique restreinte, comme un bureau ou un bâtiment, permettant l'interconnexion d'équipements locaux (ordinateurs, imprimantes, etc.) afin de partager des ressources et échanger des données.
VLAN voix/données : Séparation logique des réseaux voix et données sur la même infrastructure physique.
Wi-Fi : Norme permettant la connexion sans fil à un réseau local.
SSID : Identifiant du réseau Wi-Fi diffusé pour permettre la connexion des clients.
PoE (Power over Ethernet) : Technologie permettant d'alimenter des appareils réseau par les câbles Ethernet.

E. Sécurité Réseaux

Chiffrement : Processus qui rend les données illisibles pour quiconque n'a pas la clé de déchiffrement, protégeant ainsi la confidentialité.
Chiffrement WPA/WPA2 : Protocoles de sécurité pour chiffrer les données sur un réseau Wi-Fi.
Authentification multifacteur (MFA) : Méthode d'authentification qui combine plusieurs éléments (mot de passe, empreinte, code reçu par SMS, etc.) pour une meilleure sécurité.
IPS/IDS : Systèmes de détection/prévention d'intrusion qui analysent le trafic réseau pour détecter des activités malveillantes.

F. Qualité de service

Bande passante : Quantité de données qu'un réseau ou une liaison peut transmettre par unité de temps, généralement mesurée en bits par seconde.

Latence : Temps requis pour qu'un paquet de données soit transmis d'un point à un autre dans un réseau.
QoS (Qualité de Service) : Capacité à fournir un traitement différencié aux flux de données selon leur criticité.
MTU (Maximum Transmission Unit) : Taille maximale des paquets pouvant transiter sur un lien réseau sans être fragmentés.

G. Accés distance

VPN (Virtual Private Network) : Technologie qui crée un tunnel sécurisé et chiffré sur Internet, permettant de se connecter à un réseau distant comme si on était physiquement connecté.

H. Virtualisation réseaux

Réseau NAT (Network Address Translation) : Le mode NAT permet à la machine virtuelle d'accéder à Internet via l'adaptateur réseau de l'hôte. La machine virtuelle reçoit une adresse IP privée dans un réseau privé, et l'hôte fait office de routeur NAT, traduisant les adresses IP sources des paquets sortants en son adresse IP publique sur Internet. Cela permet à la machine virtuelle d'accéder à Internet sans avoir d'IP publique dédiée. Cependant, les autres machines sur Internet ne peuvent pas établir de connexion entrante avec la machine virtuelle.
Réseau Host-Only : Le mode Host-Only crée un réseau privé totalement isolé, dans lequel seules les machines virtuelles connectées à ce réseau peuvent communiquer entre elles. Aucune connexion Internet n'est possible. C'est utile pour tester des configurations réseau, des serveurs web locaux ou pour transférer des fichiers entre machines virtuelles sur le même hôte. Les adresses IP de ce réseau sont généralement de la forme 192.168.x.x.
Réseau Bridged (Pont) : Le mode Bridge permet à la machine virtuelle d'être connectée au même réseau physique que la machine hôte, comme si elle était un ordinateur physique supplémentaire sur ce réseau. La machine virtuelle reçoit une adresse IP dans la même plage que les autres appareils du réseau, et peut communiquer directement avec eux et avec Internet. C'est utile pour simuler un environnement de production, tester des serveurs accessibles depuis l'extérieur, etc. Cependant, cela peut poser des problèmes de sécurité si la machine virtuelle est compromise.

I. Sous-réseaux et masquage

Masque de sous-réseau : Un modèle binaire de 32 bits (pour IPv4) qui divise une adresse IP en deux parties : la partie réseau et la partie hôte. Les bits à 1 représentent la portion réseau, tandis que les bits à 0 représentent la portion hôte. Il permet de subdiviser un réseau IP en plusieurs sous-réseaux plus petits, optimisant ainsi l'utilisation des adresses IP disponibles et améliorant l'organisation et la sécurité du réseau.

Notation CIDR	Masque de sous-réseau	Nombre de sous-réseaux	Nombre d'hôtes par sous-réseau
/30	255.255.255.252	4	2
/29	255.255.255.248	8	6
/28	255.255.255.240	16	14
/27	255.255.255.224	32	30
/26	255.255.255.192	64	62
/25	255.255.255.128	128	126
/24	255.255.255.0	256	254
/23	255.255.254.0	512	510
/22	255.255.252..0	1024	1022
/21	255.255.248.0	2048	2046
/20	255.255.240.0	4096	4094
/19	255.255.224.0	8192	8190
/18	255.255.192.0	16384	16382
/17	255.255.128.0	32768	32766
/16	255.255.0.0	65536	65534

Remarques

- Les adresses se terminant par .0 et .255 sont réservées et ne peuvent pas être attribuées aux hôtes.
- Plus le préfixe CIDR est petit, plus le masque de sous-réseau a de bits à 1, et plus le nombre de sous-réseaux possibles est élevé, mais avec moins d'hôtes par sous-réseau.
- Inversement, plus le préfixe CIDR est grand, plus le masque a de bits à 0, et moins il y a de sous-réseaux, mais avec davantage d'hôtes par sous-réseau.

Author : kAly
Created : 21/04/2024 - Modified : 24/04/2024