TABLE DES MATIERES

I. Concepts réseaux fondamentaux

A. Définitions de base

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 à chaque appareil.

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.

Adresse MAC (Media Access Control) : Identifiant unique attribué à chaque carte réseau, permettant d'identifier un appareil sur un réseau.

Protocole : Ensemble de règles et normes qui permettent la communication entre différents composants d'un réseau (ex: TCP/IP, HTTP, DHCP).

Un octet : Est une unité de mesure de l'information informatique équivalant à 8 bits. Chaque bit peut prendre la valeur 0 ou 1, ce qui donne à un octet 256 combinaisons possibles. Les octets sont largement utilisés pour représenter des caractères, des nombres et d'autres types de données dans les systèmes informatiques.

B. Types d'adresses IP

Unicast :

- Les adresses unicast sont utilisées pour établir des communications point à point entre deux appareils sur un réseau.
- Chaque adresse unicast identifie de manière unique un seul appareil sur le réseau.
- Exemple : 192.168.1.10
- Plage d'adresses : Toutes les adresses IP sauf celles réservées pour le broadcast et le multicast.

Broadcast :

- Les adresses de diffusion (broadcast) sont utilisées pour envoyer des données à tous les appareils sur un réseau local.
- Lorsqu'un appareil envoie des données à une adresse de diffusion, ces données sont reçues par tous les appareils connectés au même réseau.
- Exemple : 192.168.1.255
- Plage d'adresses : 255.255.255.255 (adresse de diffusion globale) et 192.168.1.0/24 (pour un réseau local).

Multicast :

- Les adresses multicast sont utilisées pour envoyer des données à un groupe spécifique d'appareils sur un réseau.
- Contrairement aux adresses de diffusion, les adresses multicast ciblent un groupe sélectionné d'appareils qui ont des besoins similaires.
- Exemple : 239.255.0.1
- Plage d'adresses : 224.0.0.0 à 239.255.255.255

C. Classes d'adresses IP

Classe A :

- Début de l'adresse IP: 0.0.0.0
- Fin de l'adresse IP: 127.255.255.255
- Premier octet (8 bits) est réservé pour le réseau.
- Convient aux grands réseaux avec de nombreux hôtes.

Classe B :

- Début de l'adresse IP: 128.0.0.0
- Fin de l'adresse IP: 191.255.255.255
- Deux premiers octets (16 bits) sont réservés pour le réseau.
- Convient aux réseaux de taille moyenne.

Classe C :

- Début de l'adresse IP: 192.0.0.0
- Fin de l'adresse IP: 223.255.255.255
- Trois premiers octets (24 bits) sont réservés pour le réseau.
- Convient aux petits réseaux.

Classe D :

- Début de l'adresse IP: 224.0.0.0
- Fin de l'adresse IP: 239.255.255.255
- Utilisé pour les adresses IP multicast, ne sont pas assignées à des hôtes individuels mais à des groupes d'hôtes intéressés par un service multicast.

Classe E :

- Début de l'adresse IP: 240.0.0.0
- Fin de l'adresse IP: 255.255.255.255
- Réservé à des fins expérimentales ou futures, n'est pas utilisé pour les réseaux publics.

D. Bits réseau (netID) et bits hôte (hostID)

Classe A :

- Premier octet entre 0 et 127
- NetID = Premier octet
- HostID = Octet 2 + Octet 3 + Octet 4

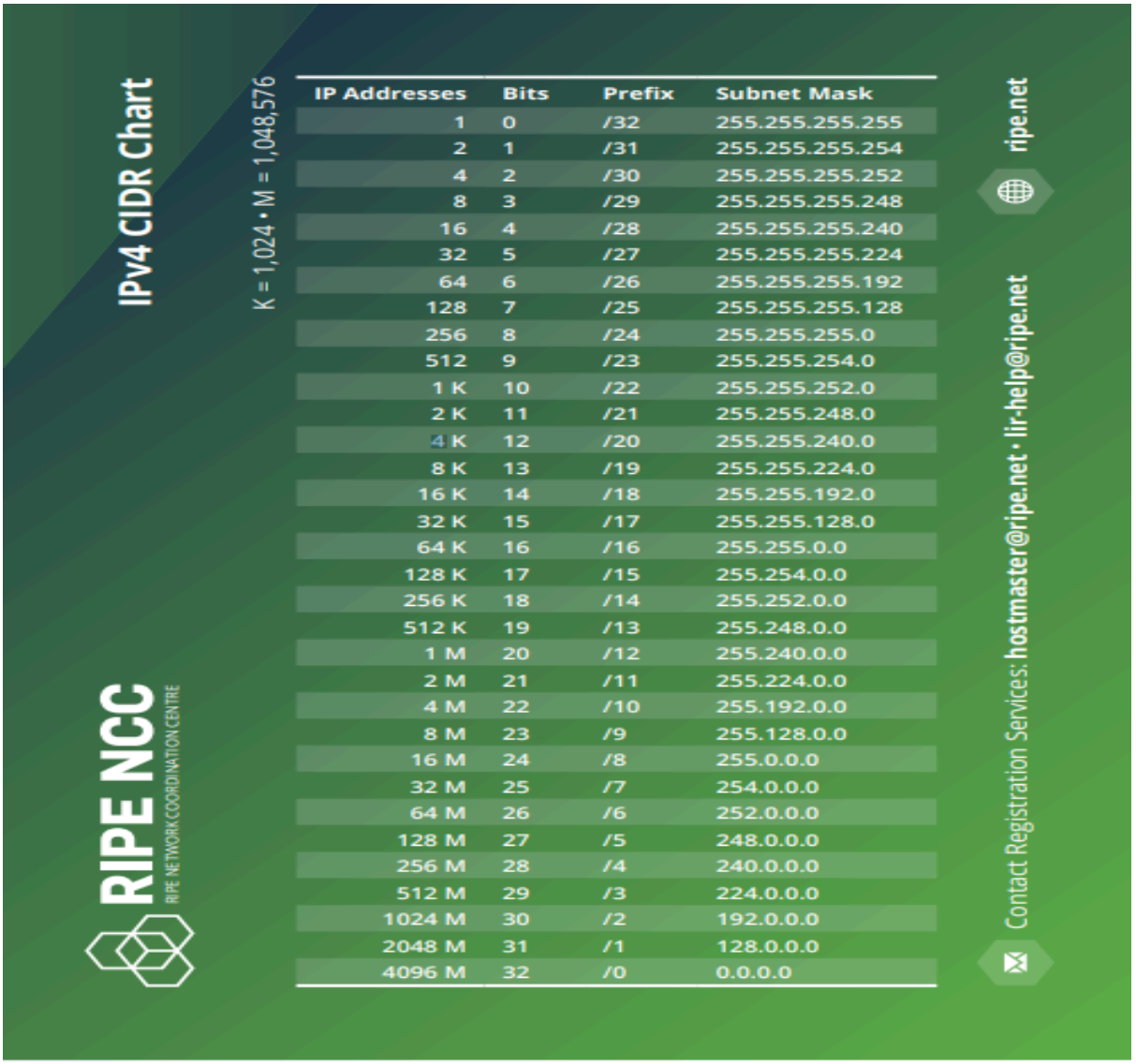
- Masque par défaut : 255.0.0.0

Classe B :
- Premier octet entre 128 et 191
- NetID = Premier octet + Deuxième octet
- HostID = Octet 3 + Octet 4
- Masque par défaut : 255.255.0.0

Classe C :
- Premier octet entre 192 et 223
- NetID = Premier octet + Deuxième octet + Troisième octet
- HostID = Quatrième octet
- Masque par défaut : 255.255.255.0

E. Sous-réseaux et masque de sous-réseau

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.



IPv4 CIDR Chart

K = 1,024 • M = 1,048,576

IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0
64 K	16	/16	255.255.0.0
128 K	17	/15	255.254.0.0
256 K	18	/14	255.252.0.0
512 K	19	/13	255.248.0.0
1 M	20	/12	255.240.0.0
2 M	21	/11	255.224.0.0
4 M	22	/10	255.192.0.0
8 M	23	/9	255.128.0.0
16 M	24	/8	255.0.0.0
32 M	25	/7	254.0.0.0
64 M	26	/6	252.0.0.0
128 M	27	/5	248.0.0.0
256 M	28	/4	240.0.0.0
512 M	29	/3	224.0.0.0
1024 M	30	/2	192.0.0.0
2048 M	31	/1	128.0.0.0
4096 M	32	/0	0.0.0.0

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

ripe.net

Contact Registration Services: hostmaster@ripe.net • lir-help@ripe.net

F. Notation CIDR

II. Protocoles et standards

A. Modèles TCP/IP et OSI

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) :

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

B. Protocoles majeurs

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.
1. **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....
2. **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
3. **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.

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.).

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.

III. Équipements réseaux

A. Routeur

Appareil qui achemine les données entre différents réseaux (Internet, réseaux locaux, etc.) en choisissant les meilleurs chemins.

B. Commutateur (switch)

Dispositif qui connecte plusieurs appareils sur un même réseau local et achemine les données entre eux.

C. Autres (pont, proxy, firewall)

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.

IV. Réseaux locaux

A. LAN

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.

B. VLAN

Séparation logique des réseaux voix et données sur la même infrastructure physique.

C. Wi-Fi

Chiffrement WPA/WPA2 : Protocoles de sécurité pour chiffrer les données sur un réseau Wi-Fi.
SSID : Identifiant du réseau Wi-Fi diffusé pour permettre la connexion des clients.

D. PoE

(Power over Ethernet) : Technologie permettant d'alimenter des appareils réseau par les câbles Ethernet.

V. Qualité de service

A. Bande passante

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

B. Latence

Temps requis pour qu'un paquet de données soit transmis d'un point à un autre dans un réseau.

C. QoS

Capacité à fournir un traitement différencié aux flux de données selon leur criticité.

D. MTU

Taille maximale des paquets pouvant transiter sur un lien réseau sans être fragmentés.

VI. Sécurité réseaux

A. Chiffrement

Processus qui rend les données illisibles pour quiconque n'a pas la clé de déchiffrement, protégeant ainsi la confidentialité.

B. Authentification multifacteur

Méthode d'authentification qui combine plusieurs éléments (mot de passe, empreinte, code reçu par SMS, etc.) pour une meilleure sécurité.

C. IPS/IDS

Systèmes de détection/prévention d'intrusion qui analysent le trafic réseau pour détecter des activités malveillantes.

VII. Accès à distance

A. VPN

Technologie qui crée un tunnel sécurisé et chiffré sur Internet, permettant de se connecter à un réseau distant comme si on était physiquement connecté.

VIII. Virtualisation réseaux

A. 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.

B. 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.

C. Bridged

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.
