Présentation : Glossaire réseaux

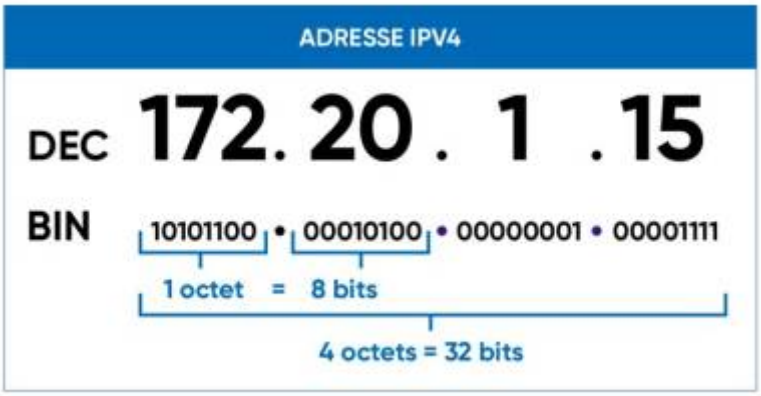
Box Internet

Une box internet c'est donc une boite dans laquelle il y a : **un modem, un routeur, une borne d'accès Wi-Fi, un switch, un pare-feu, un serveur (web, ftp, voip)** qui permet d'orchestrer tout ca mais aussi de vous fournir une interface de paramétrage

IPV4

Une adresse IPv4 est une adresse IP dans la version 4 du protocole IP (IPv4). Cette adresse permet d'identifier chaque machine connectée sur un réseau informatique utilisant le protocole IP version 4.

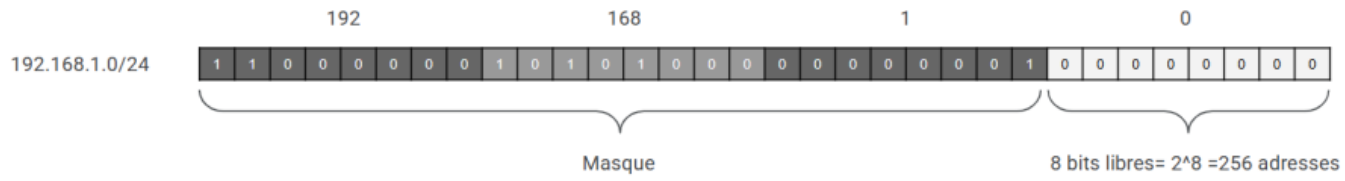
Cette adresse est composée de quatre octets , 4×8= 32bits, chacun ayant leur valeur décimale comprise entre 0 et 255, séparés par des points ; exemple : 212.85.150.133.



Masque Reseau

Par exemple, pour 192.168.1.0/24:

- Les 24 premiers bits (192.168.1) identifient le réseau (le masque)
- Les 8 derniers bits (<taille de l'adresse IP: 32> - <taille du masque: 24> = 8) sont libres, et peuvent être utilisés pour les hôtes



Notre adresse IP est découpée en deux parties : la partie réseau et la partie hôte. La question c'est, comment est positionnée cette limite entre les deux blocs ? Cette limite entre la partie réseau et la partie hôte est déterminée par le masque de sous-réseau. Le masque de sous-réseau va permettre de découper un réseau en plusieurs sous-réseaux.

✔ Notation décimale :

255.255.255.0

255.0.0.0

255.255.248.0

etc.

✔ Notation CIDR

/24 pour 255.255.255.0

CIDR

CIDR (Classless Inter-Domain Routing : Routage Inter-Domaine Sans Classe) est une méthode d'allocation et de notation des adresses IP qui a été introduite en 1993 pour remplacer le système d'adressage classique basé sur les classes (Class A, B, C). Principes fondamentaux

Un bloc CIDR est représenté par une adresse IP suivie d'une barre oblique (/) et d'un nombre qui indique la longueur du préfixe réseau. Par exemple : 192.168.1.0/24

- L'adresse IP 192.168.1.0 représente l'adresse de base du réseau
- Le nombre après la barre oblique (24) indique combien de bits, en partant de la gauche, sont utilisés pour identifier le réseau

	@IP V4				Masque Classless Inter-Domain Routing =>				CIDR
Décimal	192	168	1	25	255	255	255	0	/24
binaire	11000000	10101000	00000001	00011001	11111111	11111111	11111111	00000000	
Masque	11111111	11111111	11111111	00000000					
Et entre Masque et binaire	11000000	10101000	00000001	00000000					
Reseau	192	168	1	0					
1er @ Reseau	192	168	1	1					
Der @ reseau	192	168	1	254					
Broadcast	192	168	1	255					
Nb de PC			2^(32-CIDR)-2 =>	254					

3X8

IPV6

IPv6 signifie « Internet Protocol version 6 ». Il a été introduit par l'IETF (Internet Engineering Task Force) et constitue l'un des processus standardisés de transfert de paquets de données sur les réseaux informatiques.

IPv6 versus IPv4

Un simple coup d'œil permet déjà de constater que le format d'adresse de la sixième version d'IP est très différent de la version précédente d'IPv4 :

- Adresse IPv4 : 203.0.120.195 ⇒ Espace d'adressage de IPv4: 32 bits ≈ **4,3 milliards d'adresses**
- Adresse IPv6 : 2001:0620:0000:0000:0211:24FF:FE80:C12C ⇒ Espace d'adressage de IPv6: 128 bits ≈ **340 sextillions d'adresses**

IPV6

Routeur

Un routeur est un équipement réseau physique **responsable de l'acheminement des paquets vers leur destination**.

Les routeurs **se connectent à deux ou plusieurs réseaux ou sous-réseaux IP** et se transmettent des paquets de données entre eux selon les besoins.

Ils sont utilisés pour les particuliers et les bureaux pour établir les connexions au réseau local.

Des routeurs plus puissants sont présents partout sur Internet, afin d'aider les paquets de données à atteindre leur destination.

Un protocole de routage est un protocole utilisé pour identifier ou annoncer les chemins réseau.

Le plus célèbre est sans nul doute **BGP : Border Gateway Protocol.** Il est utilisé sur internet pour échanger des informations de routage entre les systèmes autonomes.

Nom domaine

Pour communiquer entre eux, les périphériques reliés à internet sont identifiés par une adresse internet unique, dite adresse IP (Internet Protocol). Cette adresse se présente sous forme d'une suite de chiffres, par exemple : 192.134.4.20.

Le nom de domaine permet de traduire en un nom intelligible et facilement mémorisable une adresse IP, et ainsi accéder à un site web (afnic.fr) ou adresser un courrier électronique (support@afnic.fr).

Nom de domaine gratuit :

1. dynu.com , Nom de sous domaine gratuit
2. Dyn6
3. Noip
4. Freedns
5. Cloudns
6. Duckdns

Nom de domaine (payant) (Liste totalement subjective)

1. OVH
2. Ionos
3. Gandi
4. Amen
5. Lws
6. Afnic
7. Nordnet
8. Mon domaine
9. ....

DNS

Serveur DNS, c'est l'abréviation de Domain Name System — ou, en bon français, **système de noms de domaine.**

Il permet de traduire des noms de domaine lisibles par l'humain (comme fablab37110.ovh) en adresses IP compréhensibles par les machines (comme 192.0.2.1).

DHCP

Le serveur DHCP (Dynamic Host Configuration Protocol) est un protocole réseau essentiel pour attribuer dynamiquement des adresses IP à chaque hôte sur le réseau local, que ce soit le réseau d'une entreprise ou le réseau du logement d'un particulier.

Le protocole DHCP a été utilisé la première fois en 1993. Il est défini par la RFC1531 et a été, par la suite, modifié et complété par les RFC1534, RFC2131 et RFC2132. Ce protocole fonctionne aussi bien en IPv4 qu'en IPv6. Dans ce cas, il s'appelle DHCPv6 et les adresses peuvent être auto configurées, sans DHCP.

Le protocole fonctionne en mode client/serveur et s'appuie essentiellement sur un mécanisme de requêtes DHCP, traitées par le serveur et émises par les clients. Le moteur principal de ce protocole est adossé à la communication BOOTP (utilisant des trames UDP).

Le serveur DHCP va distribuer une configuration réseau complète à la machine : une adresse IP, un masque de sous-réseau, une passerelle par défaut, un ou plusieurs serveurs DNS, etc...

Switch

Le Switch permet de mettre tous les ordinateurs d'un réseau ensemble afin qu'ils s'envoient des données. Il est lié à la norme Ethernet . Le routeur est bien entendu branché sur le switch car c'est un élément du réseau.

un switch Ethernet se présente sous la forme d'un boîtier doté de ports Ethernet RJ45. Le nombre de ports peut aller d'un faible nombre (4, 5, 10, 20, etc.) à plusieurs centaines pour les structures

importantes (centres d'affaires, salles de serveurs informatiques, etc.).

Ainsi, cette solution matérielle assure la communication, la réception et la redistribution de messages, entre les différents ordinateurs et serveurs d'un même réseau. Contrairement à un hub, le switch informatique opte pour une répartition « intelligente » de l'information. En se basant sur une table d'adressage (adresse MAC et port), il va ainsi redistribuer l'information uniquement aux appareils informatiques concernés.

À l'inverse, un hub transmet la donnée à l'ensemble des appareils actifs sur le réseau local.

SSID

Le SSID est l'acronyme de « Service Set Identifier » et désigne tout simplement le nom d'un réseau Wi-Fi qu'il soit privé ou public, composé d'un maximum de 32 caractères. Grâce à cette longueur, un SSID se doit être unique et ne pas inclure d'informations personnelles dans l'intitulé.

Exemple : Livebox-5400

Avec le chiffrement WPA, le SSID est l'une des plus fortes mesures de sécurité d'un réseau sans fil,

NAT

Le NAT/PAT permet de créer des règles nécessaires pour autoriser une communication initiée depuis Internet à atteindre un équipement spécifique de votre réseau. Vous pouvez aussi définir le port sur lequel cette communication sera acheminée.

Ports Réseaux

Un port réseau est un numéro (entre 0 et 65535) utilisé pour identifier un service ou une application sur un appareil (ordinateur, serveur, routeur…). Il permet à plusieurs applications d'utiliser la même connexion réseau sans interférer.

Les ports sont divisés en 3 catégories :

Catégorie	Numéros	Description
——————————-	———	———————————
Ports connus (Well-known)	0 à 1023	Réservés aux services système et protocoles standards
Ports enregistrés (Registered)	1024 à 49151	Utilisés par des applications et services utilisateurs
Ports dynamiques / privés	49152 à 65535	Utilisés temporairement (ex : connexions sortantes)

Service	Port	Protocole	Rôle
———	—-	———	——————————-
HTTP	80	TCP	Navigation web non sécurisée
HTTPS	443	TCP	Navigation web sécurisée
FTP	21	TCP	Transfert de fichiers
SSH	22	TCP	Connexion distante sécurisée
DNS	53	UDP/TCP	Résolution des noms de domaine
SMTP	25	TCP	Envoi d’emails
POP3	110	TCP	Récupération d’emails
IMAP	143	TCP	Consultation d’emails
RDP	3389	TCP	Connexion bureau à distance Windows
DHCP	67/68	UDP	Attribution automatique d’adresses IP

@Ip Fixe

L’IP fixe : une adresse permanente pour des accès sécurisés et durables, sur le LAN comme sur Internet. Pour les imprimantes réseaux, les périphériques IOT (tasmota, cameras, capteurs,...) les serveurs de fichiers.

Doit être entrée manuellement sur le périphérique ou via la configuration du serveur DHCP (box ou serveur) Il faut aussi indiquer l@IP du serveur DNS et de la passerelle (qui est souvent la même sur une box , mais pas nécessairement.)

ATTENTION : on ne peut pas mettre 2 @IP identiques dans un même reseau

@Ip Dynamique

l'adresseIP dynamique est amenée à changer et à être modifiée, parfois en cours de connexion.

Ce type d'IP est attribué par des serveurs DHCP, pour Dynamic Host Configuration Protocol, ou protocole de configuration dynamique des hôtes.Avec un temps maximum d'attribution .

Que ce soit sur des appareils fixes ou mobiles, l'IP dynamique, attribuée par votre routeur réseau, est aujourd'hui devenue la norme. Pour les FAI, ce type de protocole se montre facile à lire et plus économique, et se veut plus fiable et rapide.

Sur certaines Box internet , **l'@Ip externe** peut changer de temps en temps , ce qui demande à paramétrer un nom de domaine qui s'adaptera à chaque changement de cette @ip , si l'on veut accéder à son ou ses serveurs internes

Pare Feux

Unpare-feu, ou firewall, est un dispositif de sécurité chargé de surveiller le trafic réseau et de contrôler l'accès aux ressources internes d'une organisation.

Ce système repose sur un ensemble de règles prédéfinies permettant de bloquer ou d'autoriser le passage de paquets de données.

Placé à l'interface entre un réseau privé et l'extérieur (comme Internet), il bloque les connexions non autorisées et surveille les activités suspectes afin de prévenir les intrusions potentielles.

Les organisations peuvent configurer des règles pour autoriser ou refuser le trafic en fonction de divers critères, tels que les adresses IP source et de destination, les numéros de port et le type de protocole.

Il existe plusieurs niveaux d'inspection dans les pare-feux.

Certains fonctionnent uniquement au niveau du réseau, tandis que d'autres effectuent une analyse approfondie des paquets de données.

L'objectif principal est de maintenir l'intégrité, la confidentialité et la disponibilité des données de l'entreprise.

Liens Doc