

SYNTHESE BY AGLORIOS

IP (internet protocol):

C'est un numéro d'identification attribuer de façon temporaire ou permanente à chaque périphérique relié à un réseau informatique.

Il existe des IP de version 4 sur 32bits et de version 6 sur 128bits, mais on utilise actuellement celle de v4. Exemple : 172.16.254.1 (nb de 0-255).

Il existe cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités quant à la répartition du nombre d'octets servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

L'adresse IP par défaut est celle de classe C.

- Une adresse IP de classe A dispose d'une partie *net id* comportant uniquement un seul octet.
- Une adresse IP de classe B dispose d'une partie *net id* comportant deux octets.
- Une adresse IP de classe C dispose d'une partie *net id* comportant trois octets.
- Les adresses IP de classes D et E correspondent à des adresses IP particulières.

Afin d'identifier à quelle classe appartient une adresse IP, il faut examiner les premiers bits de l'adresse

IP privé :

C'est les IP de classes A B et C, elle ne permet pas d'accéder à internet et elles sont uniquement visible sur le réseau local.

- Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255
- Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255
- Les adresses privées de la classe C : 192.168.1.0 à 192.168.255.255

IP publique :

Uniquement utilisable sur internet, les routeurs disposent d'une adresse visible sur internet et permet d'accéder au serveur web.

L'adresse publique est unique alors que celle privée peuvent être réutiliser car elles ne sont jamais routées sur internet mais seulement sur le réseau local.

Les adresses IP publique sont de classe A B C différentes des IP privées.

Exceptions :

- Le réseau 127.0.0.0 est réservé pour les tests de boucle locale avec notamment l'adresse IP 127.0.0.1 qui est l'adresse « localhost » c'est-à-dire de boucle locale de votre PC.
- Le réseau 0.0.0.0 est lui aussi réservé (et utilisé notamment pour définir une route par défaut sur un routeur).

Masque de sous-réseau :

Les adresses IPV4 sont constituées de deux parties, le sous-réseau et l'hôte.

Un masque distingue les bits d'une adresse IP utilisés pour identifier le sous-réseau utilisés pour identifier l'hôte. Une adresse IP est codée sur 4 octets soit 32 bits, le masque de sous-réseau aussi.

Il y a donc 32 masques possibles

pour identifier l'hôte. Une adresse IP est codée sur 4 octets soit 32 bits, le masque de sous-réseau aussi.

Il y a donc 32 masques possibles.

Exemple :

Adresse 192.168.1.2 et masque 255.255.255.0

$192.168.1.2 \& 255.255.255.0 = 192.168.1.0$

$192.168.1.2 \& 0.0.0.255 = 0.0.0.2$

Soit en binaire :

11000000.10101000.00000001.00000010

11000000.10101000.00000001.00000010

& 11111111.11111111.11111111.00000000

& 00000000.00000000.00000000.11111111

= 11000000.10101000.00000001.00000000

= 00000000.00000000.00000000.00000010

• 0 ET 0 = 0

• 0 ET 1 = 0

• 1 ET 0 = 0

• 1 ET 1 = 1

CIDR (Classless Inter-Domain Routing):

C'est le numéro du réseau suivi par une barre oblique et le nombre de bits.

Le masque 255.255.224.0, équivalent en binaire à 11111111.11111111.11100000.00000000, sera donc représenté par /19

Exemple :

	Notation décimale	Notation binaire
Adresse IPv4	91.198.174.2	01011011.11000110.10101110.00000010
Masque de sous-réseau	255.255.224.0	11111111.11111111.11100000.00000000
Adresse du sous-réseau	91.198.160.0	01011011.11000110.10100000.00000000
Adresse de l'hôte	0.0.14.2	00000000.00000000.0001110.00000010

Broadcast et sous-réseau d'un sous-réseau :

Broadcast : Transmission ou liaison. Le principe est le même que la télédiffusion vu que l'on diffuse des paquets de données à plusieurs clients.

Un commutateur recevant une trame sur l'un des ports la diffusera sur tous les autres. (Les routeurs ne les diffusent pas)

En IPV4 on peut faire un ping (commande test d'accessibilité) `ping -b 192.168.1.255` sous Linux ou aussi `ping -b 255.255.255.255` . PING OU ICMP

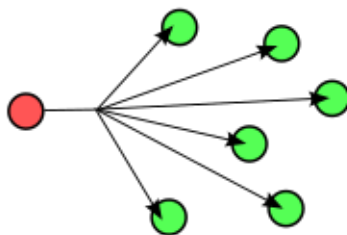


Illustration d'une communication *broadcast* : le message part d'un émetteur unique (rouge) vers l'ensemble des récepteurs (vert)

Sous-réseau : division d'un réseau de taille plus importante.

Couche réseau :

Les couches réseaux sont définies en fonction du Protocol, TCP/IP et OSI.

TCP (Transmission Control Protocol) :

C'est un protocole de transport fiable.

Fonctionnement :

- Etablir la connexion
- Transfert des données
- Fin de la connexion

TCP/IP ensemble des règles de communication sur internet basées sur l'adressage IP.

- Fractionnement des messages en paquets
- Utilisation d'un système d'adresses
- Acheminement de données sur le réseau
- Contrôle des erreurs de transmission

Notion de standard/notion d'implémentation utilisée par les devs.

Modélisé en couche qui communique avec les couches inférieures et fournit aux couches supérieures.

Notion de standard/notion d'implémentation utiliser par les devs.

Modélisé en couche qui communique avec les couches inférieure et fourni aux couches supérieures.

Modèle TCP/IP

Couche Application

Couche Transport (TCP)

Couche Internet (IP)

Couche Accès réseau

Les rôles des différentes couches sont les suivants :

- Couche Accès réseau : elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé
- Couche Internet : elle est chargée de fournir le paquet de données (datagramme)
- Couche Transport : elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaître l'état de la transmission
- Couche Application : elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...) Voici les principaux protocoles faisant partie de la suite TCP/IP :

Modèle TCP/IP

Couche Application

TCP ou [UDP](#)

Couche Internet

[IP](#), [ARP](#), [RARP](#)

Couche Accès réseau

[FDDI](#), [PPP](#), [Ethernet](#), [Anneau à jeton \(Token ring\)](#)

UDP (User Datagram Protocol) :

Envoi de datagrammes sans connexions dans des réseaux basés sur le protocole IP. L'UDP intervient au niveau de la couche de transport. Permet aux applications d'envoyer des données rapidement dans des réseaux IP mais il n'y a pas de protection des paquets ni même une assurance que les paquets arrivent dans l'ordre. L'UDP est utilisé pour les requêtes DNS (Domain Name System, conversion de noms de domaines en IP), connexion de VPN et le streaming vidéo et audio.

UDP est structuré en bloc de 32 bits :

Bits 0 à 15 Bits 16 à 31

zero Port source Port de destination

32 Longueur Somme de contrôle

IPv6 = la somme de contrôle est obligatoire.

Modèle OSI (Open Système Interconnection) :

Le rôle du modèle OSI est utilisé pour standardiser la communication entre les machines afin que différents constructeurs puissent mettre au point des produits.

Le modèle comporte 7 couches tandis que le TCP/IP seulement 4.

Niveau	Ancien modèle	Nouveau modèle
Niveau 7	Couche Application	Niveau Application
Niveau 6	Couche Présentation	Niveau Présentation
Niveau 5	Couche Session	Niveau Session
Niveau 4	Couche Transport	Niveau Message
Niveau 3	Couche Réseau	Niveau Paquet
Niveau 2	Couche Liaison Données	Niveau Trame
Niveau 1	Couche Physique	Niveau Physique

- **La couche physique** définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).
- **La couche liaison données** définit l'interface avec la carte réseau et le partage du média de transmission.
- **La couche réseau** permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.
- **La couche transport** est chargée du transport des données, de leur découpage en

- **La couche réseau** permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.
- **La couche transport** est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission.
- **La couche session** définit l'ouverture et la destruction des sessions de communication entre les machines du réseau.
- **La couche présentation** définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.
- **La couche application** assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.

Serveur DHCP (Dynamic Host Configuration Protocol) :

Les serveurs maintiennent les paramètres de configuration de client comme les IP, les noms de domaines, les passerelles, ...

Lorsqu'un périphérique client est connecté au réseau, il envoie une demande DHCP pour récupérer les informations. Le serveur va alors toutes les informations dont il a besoin par un bail (temps limité).

Permet d'économiser les adresses IP (unique).

Exemple : Entreprise

ADMIN -> SERVEUR DHCP -> tous les appareils clients.

Utilise le Protocole UDP au niveau des couches de transport.

Protocole DHCP :

Il est chargé de la configuration automatique des IP dans un réseau informatique. Elles sont tirées d'une page d'adresse et peuvent être attribuées de manière permanente ou pas. C'est un service essentiel à un réseau local.

DHCP apporte une solution à ces trois inconvénients :

- Seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage ;
- Toute modification des paramètres (adresse de la passerelle, des serveurs de noms) est répercutée sur les stations lors du redémarrage ;
- La modification de ces paramètres est centralisée sur les serveurs DHCP.

Serveur DNS (Domain Name System) :

Analyse récursive du nom de domaine pour définir l'IP

Protocole DNS :

Conversion de noms de domaines en IP.

Routage IP :

Le routage va permettre d'envoyer une information en dehors du réseau. Chaque appareil lié aux réseaux peut jouer le rôle de routeur qui va permettre la communication entre les réseaux.

La table de routage est importante dans le procédé, elle va lister les routeurs capables de recevoir des datagrammes. Le principe est d'avoir un côté avec la liste des réseaux disponibles et de l'autre la liste des routeurs.

En résumé :

- Un routeur est une machine possédant plusieurs interfaces ;
- Chaque interface d'un routeur est connectée à un réseau, le routeur relie ainsi plusieurs réseaux entre eux ;
- Toute machine ayant plusieurs interfaces peut jouer le rôle de routeur ;
- Un routeur se différencie d'une simple machine, car il accepte de relayer des paquets qui ne lui sont pas destinés ;
- Un routeur aiguille les paquets grâce à sa table de routage ;
- La table de routage indique quelle passerelle utiliser pour joindre un réseau.

Config min pour faire communiquer 2 appareils en utilisant l'IP :

- Attribuer une adresse IP et le masque de sous-réseau
- Utiliser le masque 255.255.255.0 pour 2 pc c'est suffisant.
- Grâce au TCP/IP donner au pc l'adresse IP qu'il doit utiliser ainsi que le masque de sous-réseau.
- Sur le deuxième pc, il faut faire la même chose, sauf que l'adresse IP doit avoir les 3 premiers octets identiques et modifier le dernier.
- Créer un groupe de travail pour faire communiquer les 2 pc ensemble.

- Sur le deuxième pc, il faut faire la même chose, sauf que l'adresse IP doit avoir les 3 premiers octets identique et modifier le dernier.
- Créer un groupe de travail pour faire communiquer les 2 pc ensemble.

Passerelle par défaut :

C'est le nom générique pour un dispositif qui relie deux réseaux de types différents (local et publique).

- Répéteur = passerelle de niveau 1
- Pont (switch 2 couche d'ISO) = passerelle de niveau 2
- Routeur = passerelle de niveau 3

Généralement l'on définit passerelle le routeur (BOX) et le terme par défaut est utilisé alors qu'il s'agit de routage d'IP.

Qu'est-ce qu'un port d'un point de vue IP et comment est-ce utilisé pour se connecter à un autre appareil :

Lorsque deux réseaux communiquent via un routeur il fait appelle au routeur NAT.

Le routeur permet à un hôte de rediriger le port sur un port spécifique.

La connexion ne peut pas être ciblée que sur l'adresse IP du routeur NAT car le réseaux interne est caché derrière le NAT.

NAT (Network Address Translation) : c'est lorsqu'un routeur fait correspondre une IP avec une autre. La fonction NAT traduit une adresse IP source interne en adresse IP globale.