Ipconfig : est une commande qui permet d’afficher les valeurs de la configuration actuelle de votre réseau TCP/IP, et d’actualiser au besoin les paramètres DHCP et DNS.

Objectifs :

* Connaître les termes les plus utilisées et maîtrisé les notions de base de ce domaine : modèle de OSI, modèle TCPIP (profil de technicien réseaux)
* Comprendre le profit détaillé des paquets réseau et le fonctionnement des protocoles de communications (profit d’un connaisseur réseaux)
  + Routage et interconnexion
  + Administration des services réseaux
  + Sécurité informatique et cryptographie
  + Réseaux de nouvelles générations

Les métiers de cette formation

* Ingénieur systèmes et réseaux
* Sécurité Informatique

Architecture des réseaux

Le modele OSI

La norme établie par l’International Standard Organisation (ISO) est la norme OSI (Open System Interconnection). Il s’agit de l’interconnexion des systèmes ouverts.

Un système ouvert peut être un ordinateur, un terminal, un réseau, un smartphone, une puce, un capteur, un switch, un routeur, etc. N’importe quel équipement respectant cette norme est donc apte à échanger des informations avec d’autres équipements hétérogènes, issus de constructeurs différents. En résumé, un système ouvert est un système capable d’échanger des informations indépendamment de la nature de l’architecture.

L’ISO a défini une architecture logicielle formée de 7 couches. Chaque couche offre un service, utilise un protocole, possède un point d’accès à un service (N-SAP)

* La couche physique est la couche qui est directement connectée avec l’extérieur. Elle s’occupe de tout ce qui est traitement de signal suivant différents supports de transmission.
* La couche liaison de données assemble les données en blocs appelés trames, achemine les données sans erreurs, masque aux couches supérieur les informations physiques et utilise un système d’adressage.
* La couche réseaux s’intéresse à la détection d’un chemin via des routeurs, à l’adressage des machines (Adresses IP) ; elle contrôle le flux afin d’éviter des encombrements, des congestions. Pour effectuer ce transport de bout en bout, la couche réseau utilise quatre processus de base : Adressage des périphériques finaux, Encapsulation, Routage et Désencapsulassions. L’unité d’information de la couche réseau est le paquet IP ou datagramme IP.
* La couche transport gère les connexions de bout en bout, découpe et segmente les données transmises par la couche, s’intéresse à l’adressage des applications, assure que les éléments arrivent correctement de l’autre côté. L’unité d’information de la couche transport est le segment.
* La couche session permet de communiquer le bon utilisateur indépendamment de l’application, indépendamment du chemin, indépendamment des trames ; organise les dialogues, synchronise les dialogues (identification des noms utilisateur, mots de passe, etc.)
* La couche présentation s’intéresse au type de données. Elle permet de standardiser le type de message. Elle permet de fournir une représentation des données, indépendamment des ordinateurs, des systèmes d’exploitation. Elle inclue aussi des services tels que le format de données (texte, image, vidéo, …). Elle assure aussi la confidentialité des données (cryptographie).
* La couche application donne au processus d’application le moyen d’accéder à l’environnement OSI et fournit tous les services directement utilisables par l’application :
  + Des programmes de transfert de fichiers.
  + De soumission de travaux à distances.
  + D’échange de courrier électrique.

La couche liaison de données à des adresses mac, adresse physique uniquement entre les liaisons directes mais les adresses destinations ou adresses IP de la couche réseaux qui s’intéresse au routage de données de l’adresse source à l’adresse destination.

Pour chaque couche, les données ont un nom spécifique :

* Au niveau de la couche **physique**, les données sont représentées par des **bits**, des signaux électriques ;
* Au niveau de la couche **liaison** **de** **données**, les données sont appelées **trames** ;
* Au niveau de la couche **réseau**, les données sont appelées **paquets** ;
* Au niveau de la couche **transport**, les données sont appelées **segment** ;
* Et pour les trois premières couches, **session**, **présentation** et **application**, les données sont simplement appelées **données** ;

Si une machine A veut communiquer avec une machine B (serveur), celle-ci envoie une requête à la machine B et pour se faire, la machine A doit avoir un navigateur.

L’adresse IP d’une machine est localisée au niveau de la couche réseau. Et l’adresse MAC (adresse physique) appartient à la couche liaison de données. Le support de transmission appartient à la couche physique

La machine A va générer les données bruts ou données utilisateurs qu’il veut envoyer à la machine B.

Les données vont passer par la couche application de A qui va ajouter l’entête application et les données sont appelées « messages ». La couche application va ensuite envoyer les messages à la couche transport de la machine.

Cette dernière va à son tour ajouter l’entête transport (entête TCP). Il y a deux protocoles de transport : Le protocole TCP (fiable) et le protocole UDP. A ce niveau les données sont appelées « segment » (segment TCP, s’il s’agit du protocole TCP et Datagramme UDP, si c’est le protocole UDP). Ensuite les données sont envoyées à la couche internet.

La couche internet va ajouter à son tour l’entête IP et les données vont prendre le nom de datagramme IP. Ces données vont être transmises à la couche accès réseau.

La couche accès réseau ajoute l’entête Ethernet mais aussi une queue du nom de remorque Ethernet et puis données prendront le nom de Trame Ethernet.

Et maintenant ces trames seront envoyées sur le support de transmission qui vont arriver sur la carte réseau de la machine destinataire.

La carte réseau va enlever l’entête Ethernet et la queue Remorque Ethernet envoie les données à la couche internet (datagramme IP).

Le datagramme IP va être envoyé à la couche transport qui va enlever l’entête IP (segment TCP ou Datagramme UDP).

Le segment TCP ou le Datagramme UDP va être envoyé à la couche application qui va recevoir les données brutes.

L’encapsulation est le fait de prendre des données d’un niveau n et les mettre dans un niveau n-1.

L’encapsulation est le fait d’extraire des données d’un niveau n -1 dans les niveaux n.

Chapitre 4 : Couche 2, protocole Ethernet

Les appareilles qui sont connectées à un concentrateur, forment un domaine de collision, alors que pour un commutateur, chaque port constitue un domaine de collision.

Chaque port d’un routeur est un domaine de diffusion, mais le commutateur dans son ensemble est un domaine de diffusion.

NB : Plus il y a des domaines de collision plus le réseau est performant. De même plus y a des domaines de diffusion, plus le réseau est performant.

Le routeur ne transmet pas les messages de diffusion d’un réseau à un autre ; le message de diffusion est local.

* Le protocole CSMA/CD

Il est défini par la norme IEEE 802.3 qui permet de définir l’accès à un medium qui est partagé dans les réseaux locaux.

Le principe de base du CSMA/CD :

* CS : carrier send = écouter le canal
* MA : Multiple Access = accès multiple
* CD : Collision Detecte = détecter les collisions

Donc l’objectif du CSMA/CD est une méthode d’accès pour utiliser un canal qui est partagé.

Avant de transmettre, une machine doit écouter le canal (pour voir si le canal est libre ou pas) ; si le canal est libre elle peut envoyer le paquet puis détecter s’il y a collision (c’est une interférence entre deux signaux) ; s’il y a collision, on ne peut exploiter ni le signal envoyé ni le signal reçu.

Dans CSMA/CD, on utilise un délai de 9.6μs entre deux émissions ou réceptions appelé IFG pour Inter Fram Gap (Délai inter-trame) pour marquer une séparation entre les trames et permettre aux interfaces de se préparer à une nouvelle trame.

Lors d’une émission de données si une collision est détectée alors on envoie une séquence de 4 octets incohérents pour permettre à toutes les machines du réseau de s’assurer de la collision. Cet envoi de 4 octets incohérents est appelé **brouillage**.

En cas de détection de collision, pour éviter que plusieurs machines essaient de retransmettre au même moment elles attendent un temps tiré aléatoirement appelé délai de **BackOff ou délai aléatoire après collision.**

* En informatique, une donnée est la représentation numérique d’une information.

**8 bits = 1 octets** en anglais, elle se lit byte qui désigne la plus petite unité « logiquement » adressable par un programme. **1 byte = 8 bits = 1 octet**

**NB : le bit est abrégé par « b » et byte par « B »**

* En informatique, la **latence** (ou délai de transit, ou retard) est le délai de transmission dans les communications informatiques (lag en anglais). Il désigne le temps nécessaire à un paquet de données pour passer de la source à la destination à la source réception à travers un réseau.
* Le **débit** d’une transmission est quantité d’information réellement transmise par unité de temps. D = 1/temps bit
* Le **temps** **bit** est la durée d’un bit dans un signal transmettant une donnée.
* La **bande** **passante** caractérise la liaison en elle-même entre deux organes. C’est la quantité d’information maximale transmissible sur une connexion. **C’est le débit** **maximal**.

Topologie des réseaux

* Topologie en bus : il s’agit d’un seul câble relier à plusieurs appareils. Elle est simple à mettre en œuvre et peu robuste. Mais l’émission de se fait d’un appareil après l’autre sinon il y aura collision de données. On note aussi une faible vitesse de transmission.
* Topologie en Anneau : C’est comme une topologie en bus mais elle est refermée sur elle-même. Pour communiquer, il faudra avoir un jeton ; ce jeton est transféré à tour de rôle tout autour de l’anneau.
* Topologie en Etoile : Elle est constituée d’un nœud central qui fait lien entre tous les éléments du réseau. Ce nœud central doit être robuste afin que le réseau puisse bien fonctionner. Il n’y a pas de collision dans ce réseau.
* Topologie maillée : Elle est constituée de plusieurs câbles dont chacune reliant deux machines.

Les **protocoles** de communications définissent les règles que doivent respecter les machines pour communiquer.

* Les périphériques finaux (ou terminaux) sont les périphériques qui envoient ou reçoivent des trames sur un réseau. Ce sont les organes qui utilisent le réseau pour communiquer. On parle aussi **d’hôte** du réseau. Ils ont tous une carte réseau leur communiquant un identifiant unique : adresse MAC.

On distingue deux types d’hôtes :

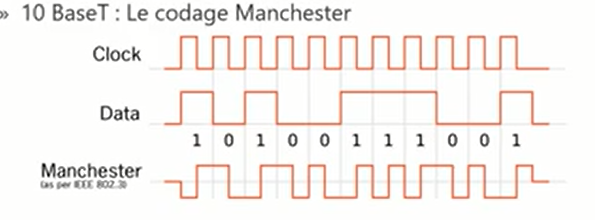
* Les **serveurs** sont des hôtes équipés des logiciels leur permettant de fournir des informations comme des messages électroniques ou des pages Web, à d’autres hôtes sur le réseau.
* Les **clients** sont des ordinateurs équipés d’un logiciel qui leur permet de demander des informations auprès du serveur et de les utiliser.
* Les périphériques intermédiaires ou appareils d’interconnections
* Les périphériques de communications ou supports de transmission

Le protocole Ethernet

Il agit sur les deux premières couches : la couche physique et la couche liaison de données.

1. Sur la couche physique, il définit :

* Les supports physiques
* 10 BaseT : 10Mbits/s (paires torsadée)
* 100 BaseT : 100Mbits/s (paires torsadée)
* 1000 BaseT : 1Gbits/s (paires torsadée)
* 1000 BaseX : 1Gbits (fibre optique)
* Wifi : 54Mbits/s à 433Mbits/s (liaison hertzienne)
* Le format des données



1. Sur la couche liaison de données, il définit :

* L’adresse MAC : Elle est codée sur 6 octets

La Trame Ethernet :

Elle est composée de :

* **Préambule** : permet de synchroniser les appareils (sur **7** **octets**)
* **SFD** : Délimitateur de début ce Trame (Start Frame Delimiter) codé sur **1** **octet** (c’est-à-dire qu’on commence à envoyer les données)
* **Destinataire** : Adresse MAC du nœud destinataire (sur **6 octets**)
* **Expéditeur** : Adresse MAC du nœud expéditeur (sur **6 octets**)
* **Longueur/Type** : Définit le type (ou parfois la longueur) de la trame (sur **2 octets**).
* Dans le cas d’envoie de trame TCP/IP, le type vaudra toujours 0 800
* **Données** **encapsulées** : Données à envoyer ((**de 46 à 1500 octets**)
* **CRC** : Séquence de contrôle permettant de vérifier s’il n’y a pas d’erreur lors de la transmission des données (sur **4** **octets**).

NB : La longueur minimale et la longueur maximale d’une Trame Ethernet sont respectivement 72 et 1526 octets.

Dans un réseau informatique, il y a plusieurs moyens d'envoyer des données.

* L'unicast : dans ce cas, on envoie des données à un seul ordinateur ;
* Le multicast : l'envoi des données se fait vers un groupe d'ordinateurs ;
* Le broadcast : on envoie des données à tous les ordinateurs du réseau.

Mise à jour table MAC

Dans un réseau constitué de machines tous connectées à un commutateur, ne machine A envoie des données à toutes les autres machines du réseau. Ces derniers vont répondre à l’expéditeur (ce qui permettre d’obtenir leurs adresse MAC) qui à son tour recopie l’adresse MAC de la machine qu’il veut envoyer. On parle de mise à jour de la table MAC.

Couche 3 : Protocole IP

Question : Dans un réseau local, chaque hôte peut connaitre l’adresse de tous les autres, mais comment faire lorsque l’on connecte plusieurs réseaux ensemble, à grande échelle (internet) ?

La réponse à cette question se trouve dans l’étude de l’adresse IP.

IP = Internet Protocole

C’est une logique qui est modifiable. Elle est codée sur 4 octets.

On parle d’adresse hiérarchique puisqu’il contient :

* Une partie réseau

Elle identifie le réseau ; donc tous les hôtes d’un réseau ont le même ID réseau.

* Une partie hôte

Elle identifie un hôte au sein d’un réseau.

Adressage par classe :

La partie réseau de l’adresses IP peuvent différer d’un réseau à un autre. On parle de classe :

* Classe A : Elle mesure 1 octet et sa partie réseau est de la forme : **0xxx xxxx**

**Les adresses vont de 0.0.0.0 à 127.255.255.255 dont 2^7 = 128 réseaux différents et 2^24 = 16777216 adresses par réseau possible.**

* Classe B : Elle mesure 2 octets et sa partie réseau est de la forme : 1**0xxx xxx**

**Les adresses vont de 128.0.0.0 à 191.255.255.255 dont 2^14 = 16384 réseaux différents et 2^16 = 65536 adresses par réseau possible.**

* Classe c : Elle mesure 3 octets et sa partie réseau est de la forme : 11**0xxx xx**

**Les adresses vont de 192.0.0.0 à 223.255.255.255 dont 2^21 = 2097152 réseaux différents et 2^8 = 256 adresses par réseau possible.**

* Classe D : Elle sert de multidiffusion pour s’adresser à plusieurs hôtes et sa partie réseau est de la forme : 111**0xxx x**

**Les adresses vont de 224.0.0.0 à 239.255.255.255**

* Classe E : Elle est réservée pour des expérimentations, il ne faut donc adresser aucun hôte sur cette classe sa partie réseau est de la forme : 111**0xxx x**

**Les adresses vont de 240.0.0.0 à 255.255.255.255**

Le masque de sous-réseau

C’est une adresse qui permet de récupérer l’adresse IP d’une machine par l’opération IP & MASQUE. Le masque de sous-réseau sert à séparer la partie hôte de la partie réseau.

* Les adresses de la classe A ont pour masque de sous-réseau : 255.0.0.0
* Les adresses de la classe B ont pour masque de sous-réseau : 255.255.0.0
* Les adresses de la classe C ont pour masque de sous-réseau : 255.255.255.0

On peut représenter le masque de réseau :

* Sous forme décimale :
* Ex : 255.0.0.0
* Sous forme CIDR : En écrivant le nombre de 1 du masque, à la suite de l’adresse IP.
* 10.23.4.32/8 pour une adresse de classe A.

Principe

* L’administrateur dispose d’une adresse de réseau (telle que 196.1.0.0) mais de plusieurs réseaux physiques, appelés sous-réseaux
* La présence de plusieurs réseaux physiques est une question interne
* Les routeurs d’Internet se contentent d’acheminer les datagrammes vers "le réseau” 196.1.0.0
* À charge des routeurs internes d’acheminer les datagrammes à travers les sous-réseaux

Identifiant de sous-réseau

Pour distinguer les sous-réseaux, l’administrateur réserve une partie d’Host-ID, appelée l’identifiant de sous-réseau :

* Les stations et routeurs internes doivent en tenir compte pour leurs décisions de routage (accessibilité directe ou indirecte de la destination)
* La taille de l’id. sous-réseau dépend du nombre de sous-réseaux, notamment si on suit la recommandation obsolète suivante :
  + l’id. sous-réseau tout à 0 est réservé (conflit avec l’adresse du réseau)
  + l’id. sous-réseau tout à 1 est réservé (conflit avec l’adresse de diffusion dirigée) De nos jours, le all-zeros subnet et le all-ones subnet sont utilisables.

Alors 2^n – 2 sous réseaux avec n bits l’id. sous réseaux

Adresse réseau et de diffusion

* La première adresse d’un réseau est l’adresse réseau.
* La dernière adresse d’un réseau est l’adresse de diffusion

EX : 172.23.43.5/16 🡪 masque = 255.255.0.0

Adresse réseau = 172.23.0.0

Adresse de diffusion = 172.23.255.255

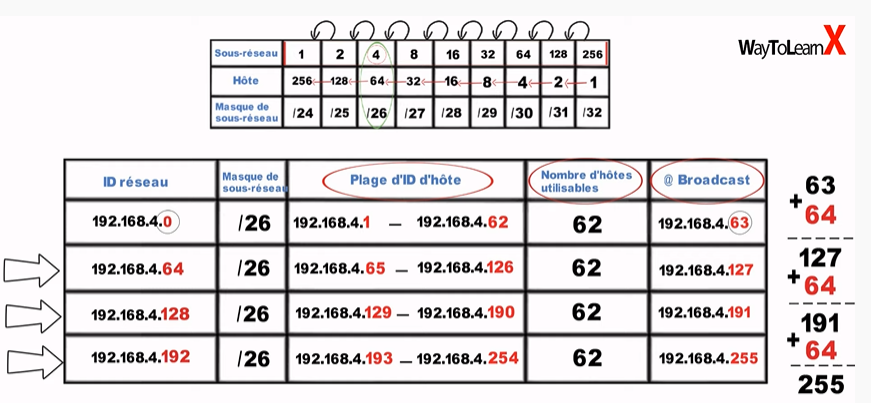
Alors

* Le Subnetting

Le calcul de sous-réseau ou subnet est un découpage logique d’un réseau IP. Ainsi le subnetting est le processus de découpage d’un réseau en deux réseaux ou plus ; on parle de cloisonner des réseaux.

Son objectif principal est de contribuer à la réduction de l’encombrement du réseau et à l’amélioration de la sécurité des performances du réseau.

L’inconvénient est que si on veut réserver x sous-réseau différent de 2^n, on aura une perte de 2^n – x réseau.



* Adresses Privées

Ceux sont des adresses non routées sur internet et qui peuvent être attribuée librement sur un réseau local. Ils permettent d’économiser le nombre d’adresse IP.

En effet à la sortie du réseau privé un routeur remplace l'adresse IP source des paquets par des adresses IP routables avant d'envoyer les paquets sur internet : c'est le principe de translation d'adresse appelé NAT (Network Address Translation).

Dans le cas où on met un réseau à usage privé (non connecté à internet), choisir de préférence les adresses réservées à l’usage privé :

* 10.0.0.1 à 10.255.255.254
  + 0000 1010. XXXX XXXX. XXXX XXXX. XXXX XXXX
* 172.16.0.1 à 172.31.255.254
  + 1010 1010. 0001 XXXX. XXXX XXXX. XXXX XXXX
* 192.168.0.1 à 192.168.255.254 (les plus courantes)
  + 1100 0000. 1010 XXXX. XXXX XXXX. XXXX XXXX

Protocole IP

C’est au niveau de la couche réseau qu’intervient le protocole IP. La couche réseau détermine le parcours et l’adressage logique. Elle manipule la trame Ethernet où est encapsulé le paquet IP qui lui-même encapsule des données.

Paquet IP

Au sein d’un même réseau, il y a une correspondance directe entre l’adresse IP et l’adresse MAC. Un hôte adresse la trame Ethernet à l’hôte destinataire et le paquet IP à l’hôte destinataire.

Comment une machine A se trouvant dans le réseau 1 peut envoyer un message à une machine B se trouvant dans le réseau 2 ?

1. La machine A va d’abord écrire son adresse MAC et son adresse IP au niveau du paquet IP