1. **Le Binaire en Informatique :**

Le système binaire est le fondement de l'informatique. Il s'agit d'un système de numération utilisant seulement deux chiffres : 0 et 1. Ces deux chiffres sont appelés "bits".

**Pourquoi le binaire ?** Les ordinateurs utilisent l'électricité pour traiter l'information. Un circuit électrique peut être soit allumé (1) soit éteint (0), ce qui en fait une représentation naturelle pour le système binaire.

**Comment ça fonctionne ?** Quand nous comptons normalement, nous utilisons le système décimal qui va de 0 à 9. En binaire, nous ne comptons qu'avec des 0 et des 1. Par exemple, le nombre 2 en binaire est représenté par "10" et le nombre 3 est représenté par "11".

**Conversion :** Il est possible de convertir des nombres d'un système à l'autre. Par exemple, le chiffre décimal 5 se traduit en binaire par "101".

**Application en Informatique :** Tous les programmes, images, textes ou tout autre fichier sur un ordinateur sont, au fond, stockés sous forme de séquences de bits. Quand vous tapez une lettre sur votre clavier, l'ordinateur la traduit en une combinaison binaire spécifique.

1. **IPv4 (Internet Protocol version 4) :**
2. **Définition** : IPv4 est la quatrième version du protocole Internet. Il est actuellement le protocole le plus largement utilisé pour la communication de données sur les réseaux.
3. **Format d’adresse :** Une adresse IPv4 est composée de 32 bits, habituellement affichée comme quatre blocs de nombres allant de 0 à 255, séparés par des points. Par exemple : 192.168.1.1.
4. **Espace d’adressage :** Du fait de sa structure à 32 bits, IPv4 peut supporter environ 4,3 milliards d'adresses uniques. Ce nombre peut sembler énorme, mais avec la croissance rapide d'Internet, cet espace d'adressage est devenu insuffisant.
5. **IPv6 (Internet Protocol version 6) :**
6. **Définition** : IPv6 est la dernière version du protocole Internet, développée pour pallier l'épuisement des adresses IPv4.
7. **Format d’adresse :** Une adresse IPv6 est composée de 128 bits et est représentée par huit groupes de quatre caractères hexadécimaux. Un exemple d'adresse IPv6 pourrait être : 2001 :0db8:85a3:0000:0000:8a2e:0370:7334.
8. **Espace d’adressage :** Grâce à sa structure à 128 bits, IPv6 peut gérer un nombre quasiment illimité d'adresses IP. Pour être précis, il peut supporter environ 340 undécillions (3,4 x 10^38) d'adresses.
9. **Différences principales entre IPv4 et IPv6 :**
10. **Taille de l’adresse :** IPv4 utilise des adresses de 32 bits, tandis qu'IPv6 utilise des adresses de 128 bits.
11. **Représentation de l’adresse :** IPv4 utilise une notation décimale ponctuée, tandis qu'IPv6 utilise une notation hexadécimale.
12. **Espace d’adressage :** IPv6 offre un espace d'adressage bien plus grand que IPv4.
13. **Configuration** : Dans de nombreux cas, IPv6 peut auto-configurer ses adresses, ce qui n'est généralement pas le cas pour IPv4.
14. **Sécurité** : La sécurité était un élément optionnel dans IPv4, alors qu'elle est intégrée dans la conception de IPv6.
15. **Gestion du trafic** : IPv6 possède des améliorations pour la gestion du trafic et de la qualité de service (QoS) par rapport à IPv4.
16. La transition de l'IPv4 à l'IPv6 est principalement due aux raisons suivantes :
17. **Épuisement des adresses IPv4** : Le format IPv4, avec ses adresses de 32 bits, permet d'avoir environ 4,3 milliards d'adresses uniques. Avec la croissance rapide d'Internet et l'augmentation du nombre d'appareils connectés, cet espace d'adressage s'est révélé insuffisant. Mais aussi, au début d'Internet, de grands blocs d'adresses IPv4 ont été alloués à des organisations sans qu'elles n'aient vraiment besoin d'autant d'adresses. Ces allocations, souvent généreuses, ont réduit la disponibilité d'adresses pour les autres.
18. **Meilleure gestion du trafic** : IPv6 offre une meilleure prise en charge de la qualité de service, permettant une gestion plus efficace du trafic de données.
19. **Auto-configuration** : Contrairement à IPv4, IPv6 a la capacité de configurer automatiquement des adresses pour les appareils, simplifiant le processus de configuration.
20. **Sécurité intégrée** : La sécurité est intégrée au niveau de la conception avec IPv6, alors qu'elle était souvent considérée comme une extension pour IPv4.
21. **Espace d'adressage quasi-illimité** : Grâce à ses adresses de 128 bits, IPv6 peut gérer un nombre presque inconcevable d'adresses, assurant une capacité d'adressage pour l'avenir prévisible.
22. **Masque de sous-réseau :**
23. **À quoi ça sert ?**

Un masque de sous-réseau est utilisé pour diviser une adresse IP en deux composantes : l'adresse réseau et l'adresse hôte. Cette division est cruciale pour le routage des paquets au sein des réseaux et entre eux.

1. **Comment il fonctionne ?**

Le masque de sous-réseau est généralement une suite de bits 1 suivie d'une série de bits 0. Les bits 1 indiquent la portion de l'adresse IP qui représente le réseau, tandis que les bits 0 indiquent la portion hôte.

Par exemple, le masque de sous-réseau 255.255.255.0 peut être représenté en binaire par 11111111.11111111.11111111.00000000. Les trois premiers octets (24 bits) identifient le réseau, et le dernier octet (8 bits) identifie un hôte particulier au sein de ce réseau.

**7. Classeful (Class-based) vs. Classless :**

**a. Classeful (Avec classes) :**

Historiquement, les adresses IP étaient divisées en classes (A, B et C) pour faciliter le routage.

**Classe A :**

* **Plage d'adresses : 1.0.0.0 à 126.0.0.0**
* **Masque de sous-réseau par défaut : 255.0.0.0 (ou /8 en notation CIDR)**
* **Utilisation : Grands réseaux avec un grand nombre d'hôtes.**
* **Nombre de réseaux : 128 (de 0 et 127 sont réservés)**
* **Nombre d'hôtes par réseau : 16,777,214**

**Note : L'adresse 127.0.0.0 est réservée pour les communications de bouclage (loopback) et n'est pas utilisée dans les réseaux publics.**

**Classe B :**

* **Plage d'adresses : 128.0.0.0 à 191.255.0.0**
* **Masque de sous-réseau par défaut : 255.255.0.0 (ou /16 en notation CIDR)**
* **Utilisation : Réseaux de taille moyenne.**
* **Nombre de réseaux : 16,384**
* **Nombre d'hôtes par réseau : 65,534**

**Classe C :**

* **Plage d'adresses : 192.0.0.0 à 223.255.255.0**
* **Masque de sous-réseau par défaut : 255.255.255.0 (ou /24 en notation CIDR)**
* **Utilisation : Petits réseaux.**
* **Nombre de réseaux : 2,097,152**
* **Nombre d'hôtes par réseau : 254**

**Classe D (Multicast) :**

* **Plage d'adresses : 224.0.0.0 à 239.255.255.255**
* **Utilisation : Adresses multicast, utilisées pour un trafic qui doit être distribué à un groupe d'ordinateurs.**

**Classe E (Expérimental) :**

* **Plage d'adresses : 240.0.0.0 à 255.255.255.254**
* **Utilisation : À l'origine destiné à des fins expérimentales, mais n'est généralement pas utilisé dans les réseaux publics.**
  1. **Classless (Sans classes) :**

Avec l'évolution des besoins en adressage et la pénurie d'adresses IP, la division classful est devenue inefficace. Par conséquent, on a introduit le CIDR (Classless Inter-Domain Routing).

* Permet une subdivision plus flexible et efficiente des espaces d'adresses.
* Utilise la notation "slash", comme 192.0.2.0/24, où /24 indique les 24 premiers bits pour le réseau (équivalent au masque de sous-réseau 255.255.255.0).

Le CIDR est essentiellement une méthode qui permet de spécifier le masque de sous-réseau en utilisant la notation slash plutôt que le masque de sous-réseau complet.

Les adresses IP, qu'il s'agisse d'IPv4 ou d'IPv6, peuvent être classées en deux grandes catégories : **privées** et **publiques**. Voici une explication détaillée de ces deux notions :

**Adresses IP Privées :**

* 1. **Définition** : Les adresses IP privées sont des adresses qui sont réservées pour une utilisation à l'intérieur d'un réseau privé. Elles ne sont pas routables sur l'Internet public. Cela signifie que ces adresses ne peuvent pas être directement accessibles depuis Internet.
  2. **Plages d'adresses privées en IPv4** :

Classe A : 10.0.0.0 à 10.255.255.255

Classe B : 172.16.0.0 à 172.31.255.255

Classe C : 192.168.0.0 à 192.168.255.255

* 1. **Usage** : Étant donné que ces adresses ne sont pas routables sur Internet, elles sont souvent utilisées dans des réseaux domestiques, d'entreprise, et d'autres environnements internes. Si des dispositifs utilisant des IP privées doivent accéder à Internet, ils passent généralement par un périphérique qui effectue une traduction d'adresse réseau (NAT).

**Adresses IP Publiques :**

1. **Définition** : Les adresses IP publiques, en revanche, sont des adresses uniques attribuées à des dispositifs qui sont directement accessibles sur Internet. Chaque adresse IP publique est unique sur tout l'Internet.
2. **Allocation** : Ces adresses sont attribuées par l'Internet Assigned Numbers Authority (IANA) et gérées par des registres régionaux d'adresses Internet (RIRs) tels que RIPE, ARIN, et APNIC.
3. **Usage** : Les adresses IP publiques sont utilisées par les serveurs web, les serveurs de messagerie, et d'autres dispositifs qui ont besoin d'être accessibles depuis Internet.

**Pourquoi cette distinction ?**

Avec la croissance rapide d'Internet et la pénurie d'adresses IPv4, il est devenu essentiel de réutiliser les adresses IP. Si chaque appareil dans chaque maison, chaque entreprise et chaque école avait besoin d'une adresse IP publique, nous aurions épuisé les adresses IPv4 bien avant.

La solution a été d'introduire des adresses IP privées pour les réseaux internes et d'utiliser le NAT (Network Address Translation) pour traduire ces adresses en une adresse IP publique lorsque les dispositifs ont besoin d'accéder à Internet. Ainsi, une seule adresse IP publique peut représenter des milliers d'adresses IP privées.

1. Le ET et le OU logique, qu’est ce que c’est et à quoi ça sert ?

**1. ET logique (AND) :**

L'opération ET renvoie 1 si et seulement si les deux entrées sont 1. Sinon, elle renvoie 0.

Voici la table de vérité pour l'opérateur ET :

A | B | A ET B

-------------------

0 | 0 | 0

0 | 1 | 0

1 | 0 | 0

1 | 1 | 1

**Utilité de l'opération ET :**

L'opération ET est souvent utilisée pour vérifier si deux conditions sont vraies simultanément. Par exemple, dans le contexte des réseaux, le "ET" logique est utilisé avec les masques de sous-réseau pour déterminer à quel réseau une adresse IP appartient.

**2. OU logique (OR) :**

L'opération OU renvoie 1 si au moins l'une des entrées est 1. Elle ne renvoie 0 que si les deux entrées sont 0.

Voici la table de vérité pour l'opérateur OU :

A | B | A OU B

--------------

0 | 0 | 0

0 | 1 | 1

1 | 0 | 1

1 | 1 | 1

**Utilité de l'opération OU :**

L'opération OU est souvent utilisée pour vérifier si au moins l'une des conditions données est vraie. Par exemple, dans le contexte de la programmation, le "OU" logique peut être utilisé pour exécuter une action si l'une ou l'autre des conditions est satisfaite.

1. Méthode pour déterminer le l’IDSR et la BRD :
2. **IDSR (ID de sous-réseau)** :

L'IDSR est l'adresse qui représente le début d'un sous-réseau. Pour le déterminer, on effectue un ET logique (bit à bit) entre l'adresse IP de l'hôte et le masque de sous-réseau. Le résultat donne l'IDSR.

Par exemple, pour l'adresse IP 192.168.1.10 et le masque de sous-réseau 255.255.255.0:

IP : 11000000.10101000.00000001.00001010 (192.168.1.10)

Masque : 11111111.11111111.11111111.00000000 (255.255.255.0)

------------------------------------------------------------------------------ ET logique

IDSR : 11000000.10101000.00000001.00000000 (192.168.1.0)

Donc, l'IDSR est 192.168.1.0.

1. **BRD (adresse de diffusion)** :

La BRD est l'adresse qui représente la fin d'un sous-réseau et est utilisée pour envoyer un paquet à tous les hôtes du sous-réseau. Pour la déterminer, vous prenez l'IDSR et mettez tous les bits qui ne sont pas définis par le masque de sous-réseau à 1.

Vous pouvez aussi trouver l'adresse de diffusion en effectuant un OU logique entre l'IDSR et l'inverse du masque de sous-réseau.

Prenons l'exemple précédent, avec l'IP 192.168.1.10 et le masque 255.255.255.0:

IDSR : 11000000.10101000.00000001.00000000 (192.168.1.0)

Inverse du masque : 00000000.00000000.00000000.11111111 (0.0.0.255)

------------------------------------------------------------------------------------------ OU logique

BRD : 11000000.10101000.00000001.11111111 (192.168.1.255)

Donc, la BRD est 192 . 168 . 1 . 255

Matériel actif :

**Switch (commutateur) :**

Un switch, ou commutateur en français, est un équipement réseau qui opère principalement au niveau 2 (couche de liaison de données) du modèle OSI. Il est utilisé pour interconnecter des dispositifs au sein d'un réseau local (LAN). Contrairement à un hub (concentrateur) qui diffuse les paquets de données à tous les dispositifs connectés, le switch est plus intelligent : il achemine les paquets uniquement vers le port du dispositif destinataire.

**Caractéristiques clés d'un switch :**

Il utilise des adresses MAC pour prendre des décisions d'acheminement.

Il améliore la performance du réseau en limitant les collisions.

Il segmente le réseau et crée des domaines de collision individuels.

* + 1. **ARP (Address Resolution Protocol) :**

ARP est un protocole utilisé pour mapper une adresse IP (couche 3) à une adresse MAC (couche 2) sur un réseau local. Quand un dispositif souhaite envoyer un paquet à une autre machine sur le même réseau local, il a besoin de connaître l'adresse MAC de cette machine. Si l'adresse MAC n'est pas déjà connue, le protocole ARP est utilisé pour la découvrir.

* + 1. **Fonctionnement basique d'ARP :**

Le dispositif émetteur envoie une requête ARP sur le réseau local demandant "Qui a cette adresse IP ? S'il vous plaît, annoncez votre adresse MAC."

Le dispositif ayant cette adresse IP répond avec son adresse MAC.

* + 1. **Table CAM (Content Addressable Memory) :**

La table CAM est une composante clé d'un switch. Elle stocke les informations sur les adresses MAC et les associe aux ports spécifiques du switch. Lorsqu'un paquet arrive sur un port du switch, le switch consulte la table CAM pour déterminer vers quel port il doit acheminer le paquet.

* + 1. **Fonctionnement basique de la table CAM :**

Lorsqu'un paquet arrive sur un port, le switch regarde l'adresse MAC source et l'ajoute à sa table CAM, l'associant au port sur lequel le paquet est arrivé.

Quand le switch doit acheminer un paquet, il regarde l'adresse MAC destinataire, consulte sa table CAM pour trouver le port associé à cette adresse MAC, puis achemine le paquet vers ce port spécifique.

Routeur :

Un **routeur** est un dispositif matériel ou logiciel utilisé pour connecter et acheminer des paquets de données entre différents réseaux. Sa principale fonction est de déterminer le meilleur chemin pour qu'un paquet de données se rende de sa source à sa destination.

1. **Fonction principale du routeur :**

* **Routage :** Le routeur évalue les informations contenues dans le paquet de données, comme l'adresse IP source et l'adresse IP destination, pour déterminer le chemin optimal à travers le réseau ou entre plusieurs réseaux. C'est comme un carrefour routier qui oriente la circulation en fonction de la destination.

1. **Autres fonctions importantes :**

* **Isolation du trafic :** Un routeur peut segmenter un grand réseau en sous-réseaux plus petits, ce qui aide à isoler le trafic et à réduire la congestion.
* **Traduction d'adresses (NAT) :** Les routeurs, en particulier ceux utilisés dans les environnements domestiques, peuvent traduire les adresses IP privées des dispositifs d'un réseau local en une adresse IP publique unique pour la communication sur Internet.
* **Sécurité :** De nombreux routeurs sont équipés de fonctions de sécurité telles que les pares-feux, le filtrage des paquets et les VPN (réseaux privés virtuels) pour protéger le réseau contre les menaces externes.

TCP et UDP :

* 1. **TCP (Transmission Control Protocol) :**
* C'est comme une conversation téléphonique : fiable, orientée connexion, garantit que les données arrivent dans le bon ordre.
* Si un morceau de la conversation est manqué, l'expéditeur le répète.
* Utilisé pour des tâches nécessitant une haute fiabilité, comme la navigation web, les e-mails, les transferts de fichiers.
  1. **UDP (User Datagram Protocol) :**
* C'est comme envoyer une lettre par la poste sans demander de reçu : non fiable, pas de connexion.
* Il envoie simplement des données sans s'assurer qu'elles arrivent.
* Plus rapide car il y a moins de vérifications. Utilisé pour des tâches où la vitesse est plus importante que la fiabilité, comme la diffusion de vidéos ou de jeux en ligne.

A partir du moment où on parle de communication, il faut parler des ports et protocoles :

* 1. **Ports :** Imaginez un grand immeuble d'appartements. L'adresse de l'immeuble est comme l'adresse IP de votre ordinateur, et chaque appartement a un numéro spécifique, qui est comme un port. Quand vous envoyez ou recevez des données, elles doivent aller à un appartement spécifique (port) pour une application ou un service spécifique sur votre ordinateur. Par exemple, le port 80 est généralement utilisé pour le web (HTTP).
  2. **Protocoles :** Ce sont comme des langues ou des sets de règles. Si deux ordinateurs veulent "parler" ou échanger des données, ils doivent utiliser le même protocole, tout comme deux personnes doivent parler la même langue pour se comprendre. Par exemple, pour naviguer sur le web, votre ordinateur utilise le protocole HTTP. Pour envoyer un e-mail, il utilise le protocole SMTP.
  3. **Plages de numéros de ports :**
* **Ports bien connus (0-1023) :** Ils sont associés à des services standard et couramment utilisés sur le réseau. Par exemple, le port 80 est associé au protocole HTTP (pour la navigation Web) et le port 22 est associé à SSH (pour les connexions sécurisées à distance).
* **Ports enregistrés (1024-49151) :** Ils sont utilisés par des applications logicielles qui ne font pas partie du noyau du système d'exploitation, mais qui sont largement reconnues dans la communauté.
* **Ports dynamiques ou privés (49152-65535) :** Ils sont utilisés pour des communications temporaires, souvent attribués dynamiquement à des applications lorsqu'elles établissent une session réseau.
  1. **Pourquoi les ports sont-ils importants ?**

Imaginez une adresse IP comme l'adresse d'un hôtel, et chaque port comme une chambre à l'intérieur de cet hôtel. Lorsqu'une lettre (donnée) est livrée à l'hôtel, elle doit avoir un numéro de chambre (port) pour s'assurer qu'elle arrive au bon destinataire.

* 1. **Quelques numéros de ports courants :**
* **Port 20 & 21 :** FTP (File Transfer Protocol)
* **Port 22 :** SSH (Secure Shell)
* **Port 23 :** Telnet
* **Port 25 :** SMTP (Simple Mail Transfer Protocol)
* **Port 53 :** DNS (Domain Name System)
* **Port 80 :** HTTP (HyperText Transfer Protocol)
* **Port 110 :** POP3 (Post Office Protocol, version 3)
* **Port 143 :** IMAP (Internet Message Access Protocol)
* **Port 443 :** HTTPS (HTTP Secure)

L’encapsulation :

L'encapsulation est un concept fondamental des communications réseau. Elle fait référence au processus par lequel une couche du modèle de communication ajoute ses propres en-têtes (et parfois des pieds de page) à la charge utile (données) qu'elle reçoit de la couche supérieure, avant de transmettre le tout à la couche inférieure.

Prenons l'exemple du modèle OSI, qui est un modèle conceptuel à 7 couches utilisé pour comprendre et décrire les communications réseau :

1. **Couche d'application :** C'est là que réside la donnée initiale ou la charge utile.
2. **Couche de présentation :** Cette couche peut éventuellement transformer la charge utile (par exemple, pour la crypter).
3. **Couche de session :** Elle établit, gère et termine les sessions de communication.
4. **Couche de transport :** Elle segmente la donnée en paquets appropriés et ajoute des informations sur le contrôle de la communication entre les deux machines. Les protocoles tels que TCP et UDP fonctionnent à ce niveau. Par exemple, un en-tête TCP contiendrait les numéros de ports source et destination.
5. **Couche réseau :** Cette couche s'occupe de la livraison des paquets d'une machine à une autre dans un réseau, souvent en utilisant des adresses IP. Ici, un en-tête IP serait ajouté, contenant, entre autres, les adresses IP source et destination.
6. **Couche liaison de données :** Elle s'occupe de la transmission des données sur le médium physique au sein d'une même zone réseau. Un en-tête (et souvent un pied de page) est ajouté, ce qui comprend généralement les adresses MAC source et destination.
7. **Couche physique :** C'est là que les données sont effectivement transmises sous forme de signaux électriques, optiques ou radio.

À chaque étape de descente dans le modèle, la charge utile est "encapsulée" avec de nouvelles informations. Lorsque les données sont reçues à l'autre bout, le processus est inversé, un processus appelé "désencapsulation". À chaque couche, les en-têtes (et pieds de page) ajoutés à l'étape précédente sont supprimés, et les données sont passées à la couche supérieure jusqu'à ce que la charge utile originale soit récupérée et traitée.

Ce processus d'encapsulation permet à chaque couche de se concentrer uniquement sur ses responsabilités spécifiques sans se soucier des détails des autres couches. Cela facilite la modularité, la standardisation et le débogage dans les communications réseau.

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

Une adresse web, souvent appelée URL (Uniform Resource Locator), est une référence ou une adresse pour un site web ou une ressource spécifique sur Internet. Elle permet aux navigateurs de localiser et d'accéder à du contenu sur le web.

Par exemple :

<https://www.example.com:8080/directory/file.html?param1=value1&param2=value2#section>

1. **Schéma (ou protocole):** https://
   * Cela indique le protocole utilisé pour accéder à la ressource. Les protocoles courants sont http (HyperText Transfer Protocol) et https (version sécurisée avec chiffrement).
2. **Sous-domaine:** www.
   * C'est une partie optionnelle de l'URL qui précise un sous-domaine du domaine principal. Dans de nombreux cas, "www" est utilisé pour les sites web, mais d'autres sous-domaines peuvent être utilisés pour d'autres services ou applications, comme "mail" pour les services de messagerie.
3. **Nom de domaine:** example.com
   * C'est l'adresse principale du site ou de la ressource. Elle est unique et est utilisée pour identifier un site web spécifique.
4. **Port:** :8080
   * C'est également une partie optionnelle de l'URL. Si spécifié, il indique le port réseau sur lequel le serveur écoute. Les ports par défaut pour HTTP et HTTPS sont respectivement 80 et 443, et ils ne sont généralement pas spécifiés dans l'URL.
5. **Chemin:** /directory/file.html
   * Il précise le chemin exact de la ressource sur le serveur web. Cela peut pointer vers un fichier, un dossier, ou même une application web.
6. **Chaîne de requête:** ?param1=value1&param2=value2
   * Commence généralement par un point d'interrogation (?). Elle permet de passer des paramètres supplémentaires qui peuvent être utilisés par la ressource côté serveur. Les paramètres sont souvent séparés par des &.
7. **Fragment (ou ancre):** #section
   * C'est une partie de l'URL qui pointe vers une section spécifique d'une page web. Les fragments sont souvent utilisés pour pointer directement vers un point précis d'une page longue.

Chaque partie de l'URL a une fonction précise, aidant les navigateurs à localiser et accéder au contenu souhaité sur le web.

Une image contenant texte, Police, capture d’écran, ligne

Description générée automatiquement

