

Le réseau

16.10.2023

Caractéristiques

Après l'évolution de nos ordinateurs, il a fallu permettre la communication entre ces machines. Initialement, les premiers réseaux informatiques étaient de portée limitée, ne couvrant que quelques dizaines de mètres. Cependant, au fil du temps, ces réseaux ont connu une expansion et une amélioration constantes, jusqu'à ce que nous soyons désormais capables de communiquer depuis l'espace. Nous allons alors à travers ce run track tenter de répondre à la question de savoir comment nous en sommes arrivés là.

Job 01:

Téléchargement de Cisco Packet Tracer:

I. Description du logiciel

Cisco Packet Tracer est un logiciel permettant de simuler le fonctionnement d'un réseau informatique. Avec Cisco Packet Tracer, nous pouvons concevoir, configurer et dépanner des réseaux informatiques simples et complexes.

Job 02:

Avant de commencer : le réseau :

I. Qu'est-ce qu'un réseau ?

D'après le dictionnaire un réseau est un ensemble formé de lignes ou d'éléments qui communiquent ou s'entrecroisent. Il peut être physique ou virtuel.

II. À quoi sert un réseau informatique ?

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil.

III. Quel matériel avons-nous besoin pour construire un réseau ? Détaillez les fonctions de chaque pièce.

Les nœuds et les liens sont les éléments de base des réseaux informatiques. Un nœud de réseau peut être un équipement de communication de données tel qu'un modem, ou un commutateur (hub ou switch), voire un équipement de terminal de données, comme deux ordinateurs et imprimantes ou plus. Une liaison désigne le support de transmission qui connecte deux nœuds. Les liaisons peuvent être physiques, comme des câbles ou les fibres optiques, ou l'espace libre utilisé par les réseaux sans fil (WIFI, Bluetooth, etc...)

Le routeur sert à connecter notre réseau privé à internet.

Le hub et le switch servent à connecter différents ordinateurs à un même réseau. Ils s'occupent de gérer l'information entre nos différents ordinateurs.

Les câbles RJ45 sont utilisés pour connecter les ordinateurs et les switch.

Un réseau peut être formé seulement par deux ordinateurs.

Job 03:

Connecter deux ordinateurs :

I. Quel cable choisir

Les câbles droits sont couramment utilisés pour connecter des ordinateurs à des commutateurs, routeurs, ou concentrateurs, ou pour connecter des périphériques tels que des imprimantes ou des scanners à un ordinateur.

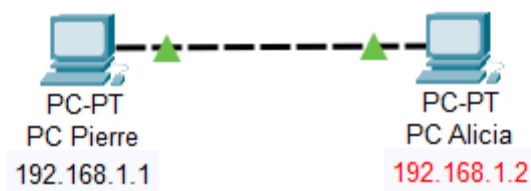
Les câbles croisés sont principalement utilisés pour relier deux ordinateurs directement, sans passer par un commutateur ou un routeur intermédiaire. Ils sont également utilisés pour connecter des dispositifs similaires, tels que deux commutateurs ou deux ordinateurs, sans utiliser de commutateur intermédiaire. Ceci est dû au fait qu'il faut croiser les fils pour s'assurer que les signaux de transmission de l'un parviennent à la réception de l'autre de manière appropriée

Dans notre cas, il vaut mieux alors utiliser les câbles en cuivre croisés.

Job 04:

Configuration réseau des ordinateurs :

Voici le schéma du réseau:



I. Qu'est-ce qu'une adresse IP ?

IP, c'est l'abréviation de Internet Protocol, soit "protocole internet" en français. L'adresse IP, c'est une sorte de code qui permet l'identification de chaque terminal connecté au réseau internet.

Le format classique d'une adresse IP se compose de quatre blocs, eux-mêmes composés de nombre pouvant aller jusqu'à 255, ces derniers séparés par des points.

II. À quoi sert une IP ?

L'adresse IP permet d'identifier chaque appareil, de les distinguer les uns des autres. Toutefois, dans la réalité, plusieurs appareils peuvent partager la même adresse IP. Par exemple, pour clarifier le sujet, si vos appareils à la maison sont connectés à internet par votre box, ils partagent une adresse IP, celle de votre box (adresse du réseau).

Son rôle est de permettre que l'acheminement des données se fasse vers le bon endroit, ce qu'on appelle "le routage" dans le jargon informatique.

III. Qu'est-ce qu'une adresse MAC ?

MAC signifie "Media Access Control" et cette adresse correspond à l'adresse physique d'un équipement réseau. Cette adresse est un identifiant, normalement unique, permettant d'identifier un équipement réseau par rapport à un autre.

Par exemple, chaque ordinateur a sa propre adresse MAC.

IV. Qu'est-ce qu'une IP publique et privée ?

Les adresses IP privées s'utilisent dans un réseau interne. Elles permettent à vos appareils périphériques de communiquer avec votre routeur. De fait, chacun de vos appareils connectés à votre réseau privé pourra reconnaître les autres et ils pourront échanger entre eux. Vous pouvez définir manuellement ces adresses IP ou bien laisser votre routeur (protocole DHCP) le faire pour vous.

Les adresses IP publiques, quant à elles, s'utilisent en dehors de votre réseau privé. C'est votre fournisseur d'accès qui vous l'attribue et c'est grâce à elles que votre réseau (qu'il soit domestique ou professionnel) va pouvoir communiquer avec les autres appareils en réseau du monde. Ce sont ces adresses IP qui vont vous permettre d'accéder à différents sites internet ou encore recevoir des e-mails, par exemple.

V. Quelle est l'adresse de ce réseau ?

Sachant que l'ip du PC de Pierre est 192.168.1.1 et le masque de sous réseau est 255.255.255.0, pour trouver l'adresse du réseau nous transformons l'adresse et le masque en binaire puis nous appliquons le **ET** logique.

Adresse IP en binaire	1100 0000	1010 1000	0000 0001	0000 0001
Masque de sous réseau en binaire	1111 1111	1111 1111	1111 1111	0000 0000
Adresse & Masque	1100 0000	1010 1000	0000 0001	0000 0000
Résultat en décimal	192	168	1	0

On retrouve donc l'adresse du réseau : **192.168.1.0**.

Job 05:

Vérification des adresses IP:

I. Quelle ligne de commande avez-vous utilisée pour vérifier l'ip des machines ?

Afin de voir l'ip des machines nous utilisons la commande **ipconfig** dans la console de commandes de l'ordinateur.

Ici nous voyons bien que l'ip du PC de Pierre (première capture) est **192.168.1.1** et que celle du PC d' Alicia est **192.168.1.2**.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:63FF:FE84:8E00
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        0.0.0.0
```

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2D0:FFFF:FE55:87C6
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::
                        0.0.0.0
```

Job 06:

Communication entre deux ordinateurs:

I. Quelle est la commande permettant de Ping entre des PC ?

Pour pouvoir ping deux ordinateurs on doit utiliser la commande **ping**.

Nous observons que les paquets sont reçus pour les deux ordinateurs.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Job 07:

Eteignons l'ordinateur de Pierre:

I. Comment l'éteindre?

Pour éteindre le PC de Pierre nous appuyons sur le bouton rouge de démarrage sur Cisco Packet Tracer.



II. Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ? Pourquoi?


Si on éteint le PC de Pierre, celui-ci ne pourra pas recevoir les paquets envoyés par Alicia et ne pourra donc pas les renvoyer à son tour, les paquets seront alors perdus et nous recevrons la réponse "Request timed out.". Cela signifie que les paquets ont dépassé un temps défini pour les recevoir.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
```



En effet un PC éteint ne peut pas recevoir de paquets parce que l'ordinateur ne sera donc pas connecté au réseau.

Job 08:

Connexion entre 5 ordinateurs :

On ne peut pas brancher plusieurs câbles sur les ordinateurs normaux car ils n'ont qu'une prise pour le câble. Pour connecter plus d'ordinateurs nous devons alors utiliser soit un hub soit un switch.

I. Quelle est la différence entre un hub et un switch ?

La grande différence entre le hub et le switch est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée tandis que le switch effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

II. Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

Un hub est souvent utilisé pour connecter des segments d'un réseau local (LAN). Un hub contient plusieurs ports. Lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local puissent accéder à tous les paquets. Le hub sert comme point de connexion commun pour les périphériques d'un réseau.

Son inconvénient majeur est donc sa bande passante partagée (plus il y a de postes connectés, moins il y a de débit). Le réseau peut également être rapidement saturé en cas de branchement en boucle, c'est-à-dire le branchement des deux extrémités d'un même câble sur deux ports de cet élément.

III. Quels sont les avantages et inconvénients d'un switch ?

Le principal avantage des switch est qu'ils permettent une vitesse de transfert de données plus élevée que celle des hubs.

Un autre avantage du switch est qu'il offre une plus grande sécurité. Ils sont conçus pour envoyer des paquets de données uniquement aux appareils qui les demandent, ce qui signifie que les données ne sont pas envoyées à tous les appareils connectés, ce qui peut constituer une faille de sécurité.

L'un des principaux inconvénients est qu'ils peuvent être plus chers que les hubs. À mesure que la technologie progresse, les prix ont baissé, mais les commutateurs peuvent néanmoins être plus chers que les hubs.

IV. Comment un switch gère-t-il le trafic réseau ?

Les switch utilisent une technique appelée commutation pour envoyer des données directement au périphérique de destination, permettant ainsi des vitesses de transfert de données plus élevées.

V. Testons notre réseau

```
C:\>
ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=3ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128 [

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Nous observons bel et bien que nos différentes machines communiquent entre elles.

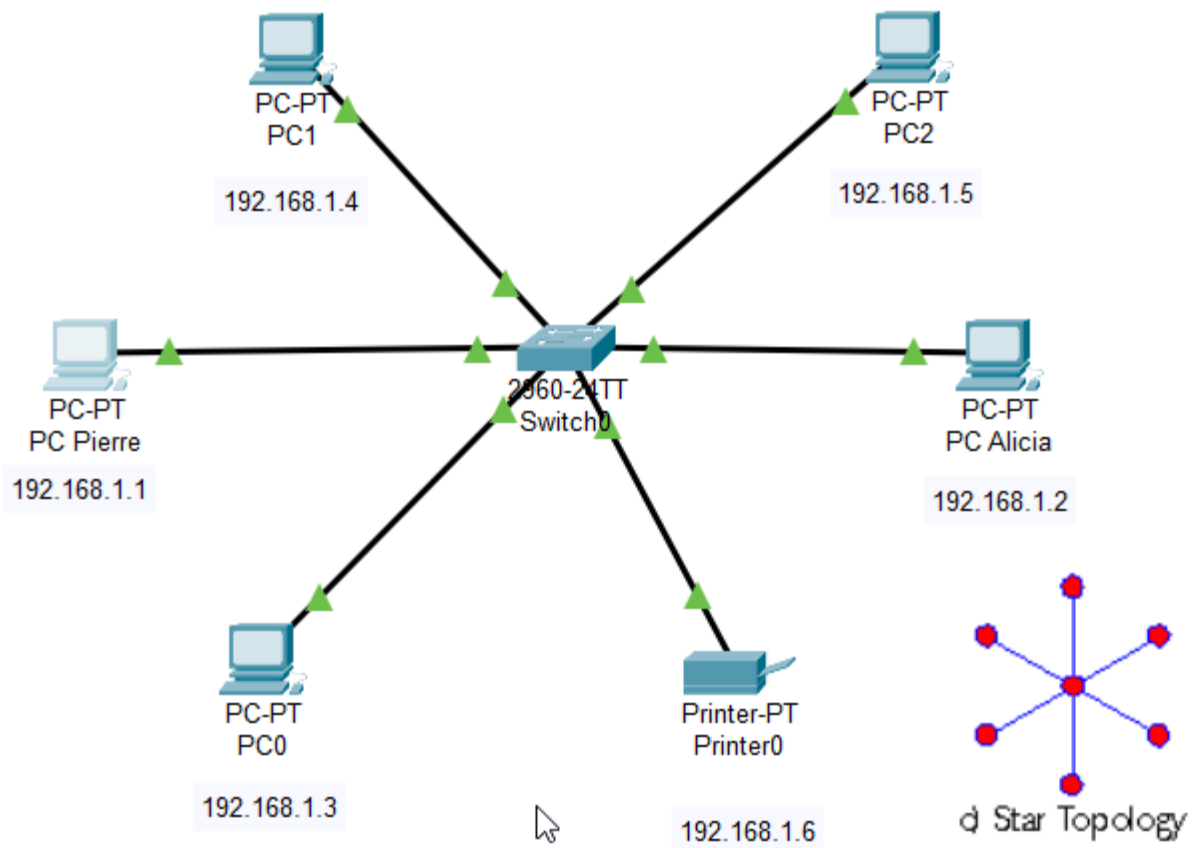
Par ailleurs, nous pouvons vérifier les ordinateurs avec lesquels nous avons communiqué grâce à la commande **arp -a**.

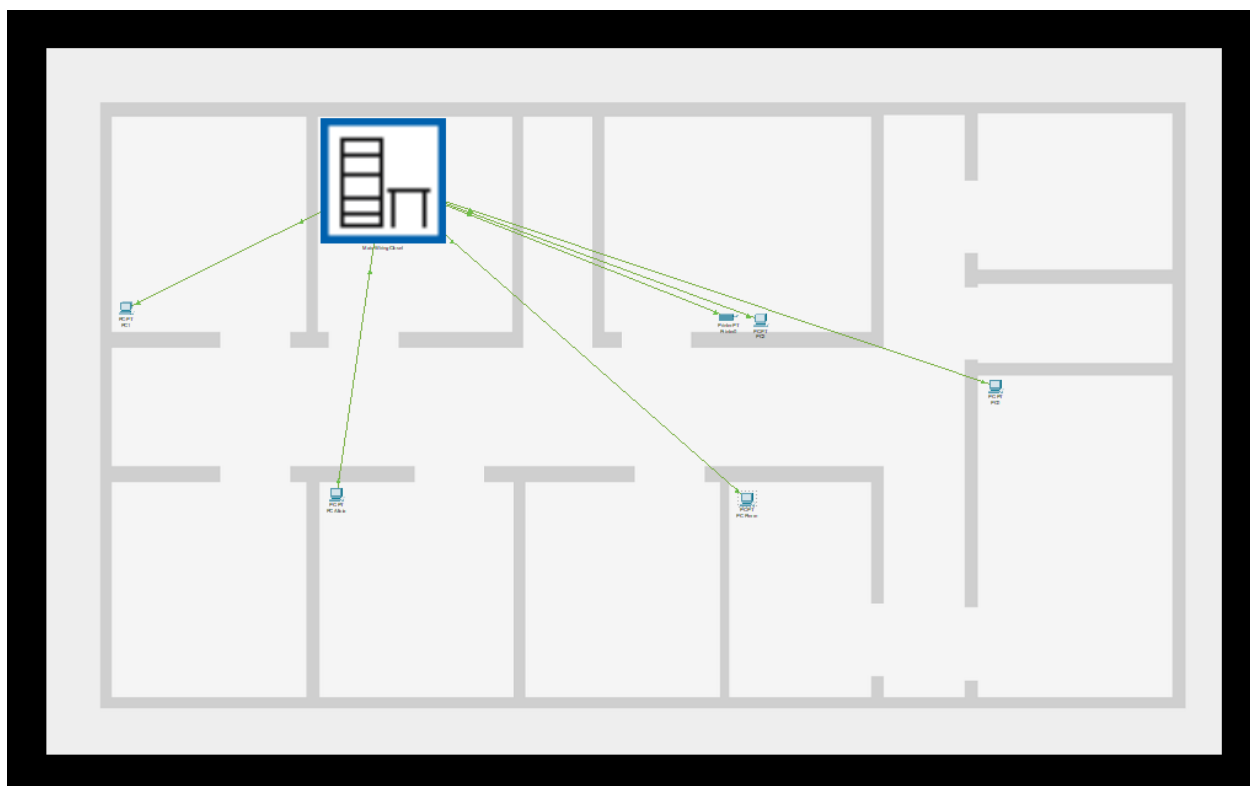
```
C:\>arp -a

Internet Address      Physical Address      Type
192.168.1.2           00d0.ff55.87c6        dynamic
192.168.1.3           0009.7ce0.1032        dynamic
192.168.1.4           0040.0b2a.b7d5        dynamic
192.168.1.5           0001.97d3.c219        dynamic
192.168.1.6           0001.966d.b0dc        dynamic
```

Job 09:

Ajoutons une imprimante:





Grâce à ce schéma nous pouvons observer graphiquement que notre réseau est un réseau étoile. Tous les ordinateurs et imprimantes sont connectés à un même switch qui gère la communication entre eux.

Les avantages d'utiliser un schéma sont :

Faciliter la visualisation. Nous pouvons en effet voir les ip de chaque hôte ainsi que les liaisons avec les autres appareils. Nous pouvons aussi schématiser l'emplacement physique.

La flexibilité et la modifiabilité peuvent modifier aisément notre configuration. De plus, si un réseau est déjà en place cela peut permettre une évolution de celui-ci en l'améliorant avant de procéder à la vraie modification.

L'avantage de cisco est que nous pouvons simuler une vraie interaction dans notre réseau et vérifier que tout fonctionne correctement.

Job 10:

Serveur DHCP:

VI. Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

Une adresse IP statique et une adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) sont deux méthodes de configuration des adresses IP pour les appareils sur un réseau.

L'Adresse IP statique est manuellement attribuée à un appareil et restera la même, même au redémarrage de l'appareil. Les adresses IP statiques sont stables et restent les mêmes, ce qui peut être utile pour les serveurs, les équipements réseau critiques et les appareils nécessitant une adresse IP constante pour des raisons de connectivité. Leur inconvénient est qu' elle doit être configurée à la main, ce qui peut être une tâche fastidieuse sur des grands réseaux et laisse place à l'erreur humaine.

L'Adresse IP attribuée par DHCP est une adresse IP dite dynamique, c'est-à-dire qu'elle est attribuée automatiquement par un serveur DHCP à un appareil lors de sa connexion au réseau. Le serveur DHCP attribue une adresse IP, un masque de sous-réseau, une passerelle par défaut et d'autres paramètres réseau. L'avantage est que les adresses IP attribuées par DHCP sont temporaires et peuvent être réutilisées une fois qu' un appareil se déconnecte du réseau. Cela permet une gestion efficace des adresses IP, en particulier dans les réseaux de grande taille.

Job 11:

Adressage:

Nombre d'hôtes minimum	Nombre d'adresses	Gateway	Plage d'adresses	Bits	Masque en binaire	Masque de sous réseau	Adresse de diffusion
12 hôtes	16 dont 14 utilisables	10.0.0.0	10.0.0.1-10.0.0.14	4	1111 1111.1111 1111.1111 1111.1111 0000	255.255.255.240 / 28	10.1.0.15
30 hôtes	32 dont 30 utilisables	10.0.0.16	10.0.0.17 - 10.0.0.46	5	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.47
30 hôtes		10.0.0.48	10.0.0.49 - 10.0.0.78				10.0.0.79
30 hôtes		10.0.0.80	10.0.0.81 - 10.0.0.110				10.0.0.111
30 hôtes		10.0.0.112	10.0.0.113 - 10.0.0.142				10.0.0.143
30 hôtes		10.0.0.144	10.0.0.145 - 10.0.0.174				10.0.0.175
120 hôtes	128 dont 126 utilisables	10.0.0.176	10.0.0.177 - 10.0.0.255, 10.0.1.0 - 10.0.1.46	7	1111 1111.1111 1111.1111 1111.1000 0000	255.255.255.128 / 25	10.0.1.47
120 hôtes		10.0.1.48	10.0.1.49 - 10.0.1.174				10.0.1.175
120 hôtes		10.0.1.176	10.0.1.177 - 10.0.1.255, 10.0.2.0 - 10.0.2.46				10.0.2.47
120 hôtes		10.0.2.48	10.0.2.49 - 10.0.2.174				10.0.2.175
120 hôtes		10.0.2.176	10.0.2.177 - 10.0.2.255, 10.0.3.0 - 10.0.3.46				10.0.3.47
160 hôtes	256 dont 254 utilisables	10.0.3.48	10.0.3.49 - 10.0.3.255 10.0.4.0 - 10.0.4.46	8	1111 1111.1111 1111.1111 1111.0000 0000	255.255.255.0 / 24	10.0.4.47
160 hôtes		10.0.4.48	10.0.4.49 - 10.0.4.255, 10.0.5.0 - 10.0.5.46				10.0.5.47
160 hôtes		10.0.5.48	10.0.5.49 - 10.0.5.255, 10.0.6.0 - 10.0.6.46				10.0.6.47
160 hôtes		10.0.6.48	10.0.6.49 - 10.0.6.255, 10.0.7.0 - 10.0.7.46				10.0.7.47
160 hôtes		10.0.7.48	10.0.7.49 - 10.0.7.255, 10.0.8.0 - 10.0.8.46				10.0.8.47

VII. Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

Nous avons choisi une adresse de classe A pour être sûrs que nous pouvons créer tous les sous-réseaux demandés. Nous aurions tout de même pu utiliser une adresse de classe B.

VIII. Quelle est la différence entre les différents types d'adresses ?

Les différents types d'adresses sont pour les adresses publiques :

- Classe A : **0.0.0.0 à 126.255.255.255**
- Classe B : **128.0.0.0 à 191.255.255.255**
- Classe C : **192.0.0.0 à 223.255.255.255**
- Classe D : **224.0.0.0 à 239.255.255.255** (adresses de multicast).
- Classe E : **240.0.0.0 à 255.255.255.255** (adresses réservées par l'IETF)

Pour les adresses privées :

- 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**

Job 12:

Modèle OSI:

Couche 7	La couche d'application	FTP, HTML,	Communique directement avec l'utilisateur
Couche 6	La couche de présentation	PPTP,	Prépare les données pour qu'elles puissent être affichées à l'utilisateur.
Couche 5	La couche session	SSL TSL, FTP,	Crée une session, qui est unique à l'utilisateur et l'identifie sur le serveur distant. La session doit être ouverte suffisamment longtemps pour que les données soient transférées
Couche 4	La couche de transport	TCP, UDP	La couche transport est chargée de prendre les données et de les décomposer en petits morceaux. Lorsque des données sont transférées sur un réseau, elles ne sont pas transférées en un seul paquet.
Couche 3	La couche réseau	IPv4, IPv6	Décompose les données sur l'appareil de l'expéditeur et de les réassembler sur l'appareil du destinataire lorsque la



			transmission s'effectue sur deux réseaux différents.
Couche 2	La couche de liaison de données	MAC,	Facilite la communication entre différents réseaux, mais la couche liaison de données est responsable du transfert des informations sur le même réseau
Couche 1	La couche physique	Ethernet, fibre optique, Wi-Fi, routeur,cable RJ45.	Comme son nom l'indique, la couche physique est responsable de l'équipement qui facilite le transfert des données, comme les câbles et les routeurs installés sur le réseau.

Job 13:

Réseau La Plateforme:

I. Quelle est l'architecture de ce réseau ?

La topologie de ce réseau est un réseau en étoile. Le réseau possède un point central commun à tous les appareils. Ce point central est souvent un switch ou un hub (commutateur ou concentrateur en français)

II. Indiquer quelle est l'adresse IP du réseau ?

Adresse IP en binaire	1100 0000	1010 1000	0000 1010	0000 0110
Masque de sous réseau en binaire	1111 1111	1111 1111	1111 1111	0000 0000
Adresse & Masque	1100 0000	1010 1000	0000 1010	0000 0000
Résultat en décimal	192	168	10	0

L'adresse IP du réseau est donc **192.168.10.0**.

III. Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?

Sur ce réseau on peut brancher jusqu'à **254 hôtes** car le 0 est réservé à l'adresse du réseau et 255 à l'adresse de diffusion. Néanmoins ce seul switch ne pourra pas accueillir ces 254 hôtes car il ne possède pas suffisamment de fentes.

IV. Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion est **192.168.10.255**.

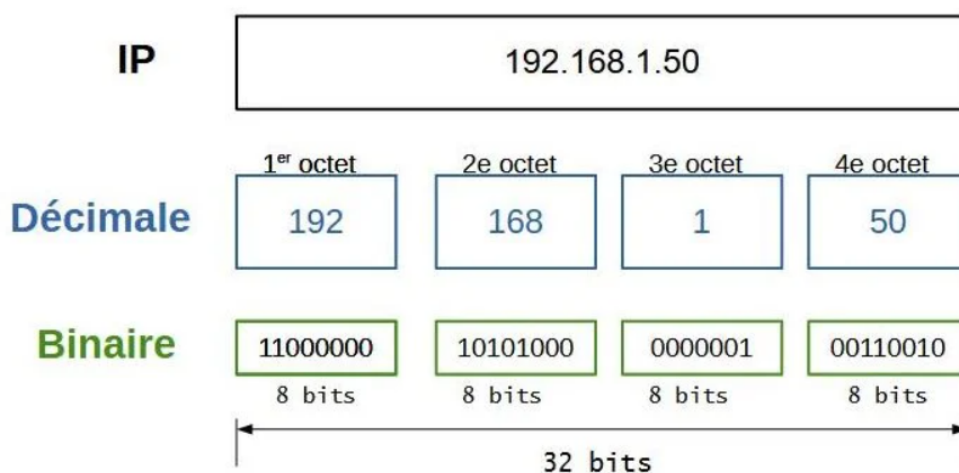
Job 14:

Conversion d'adresses IP en binaire:

I. Introduction

Afin de convertir des adresses IP en binaire nous utiliserons une table de conversion.

Nous devons d'abord savoir que chaque partie divisée par le point est un chiffre codé sur 8 bit (1 octet) et que nous avons 4 parties Donc notre adresse IP sera codée sur 32 bit soit 4 octets.



8e bit	7e bit	6e bit	5e bit	4e bit	3e bit	2e bit	1e bit
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

J'ai réalisé un programme python qui transforme une adresse IP (sous forme de string) et la transforme en binaire. Voici le code :

```
def decimalToBinary(number):
    binaryReversedString = ''
    while number > 0:
        print(number % 2)
        binaryReversedString += str(number % 2)
        number //= 2
    while len(binaryReversedString) < 8:
        binaryReversedString += '0'
    return binaryReversedString[::-1]

def ipToBinary (ip):
    splittedIP = ip.split(".")
    binaryString = ''
    for i in range(len(splittedIP)):
        if i == 0:
            binaryString += decimalToBinary(int(splittedIP[0]))
        else:
            binaryString += '.' + decimalToBinary(int(splittedIP[i]))
    return binaryString
```

J' ai utilisé la méthode euclidienne trouvée sur un cours de maths.

- 145.32.59.24

10010001.00100000.00111011.00011000

- 200.42.129.16

11001000.00101010.10000001.00010000

- 14.82.19.54

00001110.01010010.00010011.00110110

Job 15:

Questions:

I. Qu'est-ce que le routage ?

Le routage consiste à choisir la voie à emprunter dans un réseau. Un réseau informatique se compose de plusieurs appareils, appelés nœuds, qui sont connectés par des chemins ou des liaisons. Lorsque deux nœuds dans un réseau interconnecté veulent communiquer, il existe de nombreuses options de chemins par lesquels cette communication peut s'effectuer.

II. Qu'est-ce qu'un gateway ?

Une passerelle, ou gateway en anglais, représente un point dans un réseau qui sert de point d'entrée vers un autre réseau utilisant un protocole distinct.

III. Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel, établit une connexion réseau privée entre des dispositifs via Internet. Les VPN sont utilisés pour sécuriser et anonymiser la transmission de données sur des réseaux publics.

IV. Qu'est-ce qu'un DNS ?

DNS signifie Domain Name System, ou Système de Nom de Domaine en français. C'est un protocole qui permet aux utilisateurs d'accéder à un site web sans avoir à saisir son adresse IP. Au lieu de cela, il envoie une demande à un serveur pour obtenir l'adresse IP correspondante.