

Contexte

L'objectif de cette runtrack est de comprendre le principe de fonctionnement des réseaux à la fois théoriquement en faisant différentes recherche et à la fois de manière pratique via le logiciel Cisco Packet Tracer qui est un logiciel de simulation de réseau informatique

Job 1

Pour l'installation de Cisco Packet Tracer il faut se rendre sur le site :

<https://www.netacad.com/fr/courses/packet-tracer> puis s'inscrire et renseigner ses informations un fois que cela est fait on descend en bas de page et dans la section "Ressources" on sélectionne "Packet Tracer" enfin on arrive sur une page où l'on a le mode d'emploi d'installation et d'utilisation du logiciel et en bas de page on a les prérequis pour utiliser cisco et le lien de téléchargement avec les différents système d'exploitation

Job 2

→ Qu'est-ce qu'un réseau ?

Un réseau est un ensemble de dispositifs ou de machines connectés qui communiquent entre eux.

→ À quoi sert un réseau informatique ?

Un réseau informatique permet la communication, le partage de ressources et l'accès à l'information entre des machines interconnectés.

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

Ordinateurs et périphériques : Utilisateurs du réseau.

Serveurs : Fournissent divers services réseau.

Routeurs : Acheminent le trafic entre différents réseaux, y compris Internet.

Switches : Relient les appareils sur un réseau local (LAN) et facilitent la communication.

Firewalls : Protègent le réseau en contrôlant le trafic entrant et sortant.

Câble réseau : Connecte physiquement tous les composants du réseau.

Points d'accès sans fil : Permettent la connexion Wi-Fi.

Modems : Transforment les signaux pour la transmission, notamment pour Internet.

Job 3

→ Comme vous avez pu le constater, il existe des câbles croisés, droits... Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

Avec cisco packer tracer on a la possibilité de relier les machines de manière automatique. On remarque que le câble placé automatiquement entre les deux PC est un câble croisé, on utilisera des câbles croisés pour lier des machines du même type et des câbles droits pour connecter des appareils de nature différentes.

Job 4

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP, IP qui veut dire Internet Protocol, est une série de chiffres qui identifie de manière unique un dispositif connecté à un réseau, lui permettant de communiquer avec d'autres dispositifs sur Internet ou sur un réseau local.

Remarque : Les adresses IP sont essentielles pour le routage des données sur Internet et la localisation des dispositifs dans un réseau.

→ À quoi sert un IP ?

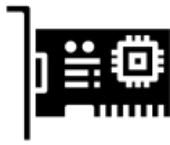
Une adresse IP sert à identifier une machine au sein d'un réseau, que ce soit sur Internet ou sur un réseau local. Cette identification permet le routage des données vers le bon destinataire et la communication entre les dispositifs au sein du réseau.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un identifiant unique associé à chaque carte réseau qui se trouve sur les ordinateurs, les imprimantes, les routeurs, et d'autres équipements réseau.

Remarque : Contrairement aux adresses IP, qui sont logiques et attribuées logiquement, les adresses MAC sont des identifiants matériels inscrits en usine sur chaque carte réseau.

exemple : Intel va avoir pour une carte réseau un identifiant du type



00:1A:2B:EF:45:3E

avec la partie en bleu correspondant à l'identifiant du constructeur et la partie en noir à celui de la carte réseau

De cette manière on peut différencier chaque carte réseau dans le monde, ce qui est essentiel pour le bon fonctionnement des réseaux locaux (LAN) et pour contrôler la communication entre les dispositifs au niveau matériel.

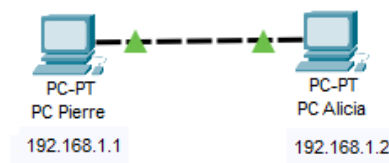
→ Qu'est-ce qu'une IP publique et privée ?

Une adresse IP publique est une adresse unique et routable qui identifie un dispositif ou un réseau sur Internet. Elles permettent aux dispositifs d'accéder à Internet et de recevoir des données en provenance d'autres dispositifs du monde entier.

Une adresse IP privée est utilisée pour identifier un dispositif au sein d'un réseau local (LAN) et n'est pas routable sur Internet. Les adresses IP privées sont généralement attribuées selon des plages spécifiques réservées à cet usage, telles que 192.168.0.0 à 192.168.255.255. Elles servent à permettre la communication au sein du réseau local, mais ne sont pas visibles depuis Internet.

→ Quelle est l'adresse de ce réseau ?

Il s'agit de l'adresse : **192.168.1.0**

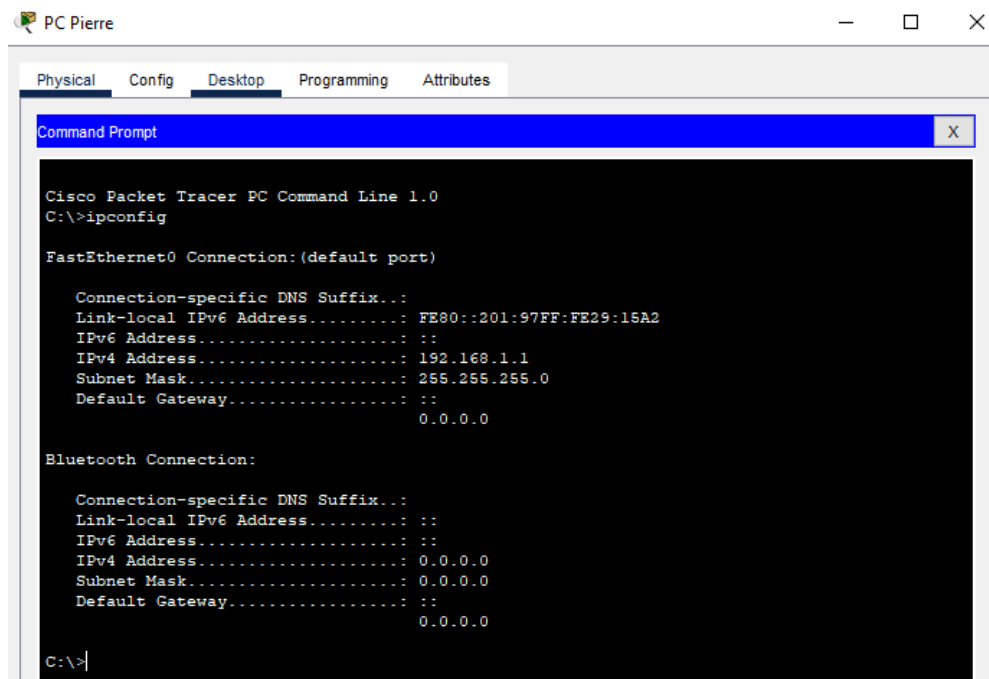


Job 5

→ Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?

On utilise dans le command prompt la commande suivante : **"ipconfig"**

PC Pierre



The screenshot shows a window titled "PC Pierre" with a "Command Prompt" window open. The command prompt displays the output of the "ipconfig" command. It shows details for the "FastEthernet0" and "Bluetooth" connections, including IPv4 and IPv6 addresses, subnet masks, and default gateways.

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

FastEthernet0 Connection: (default port)

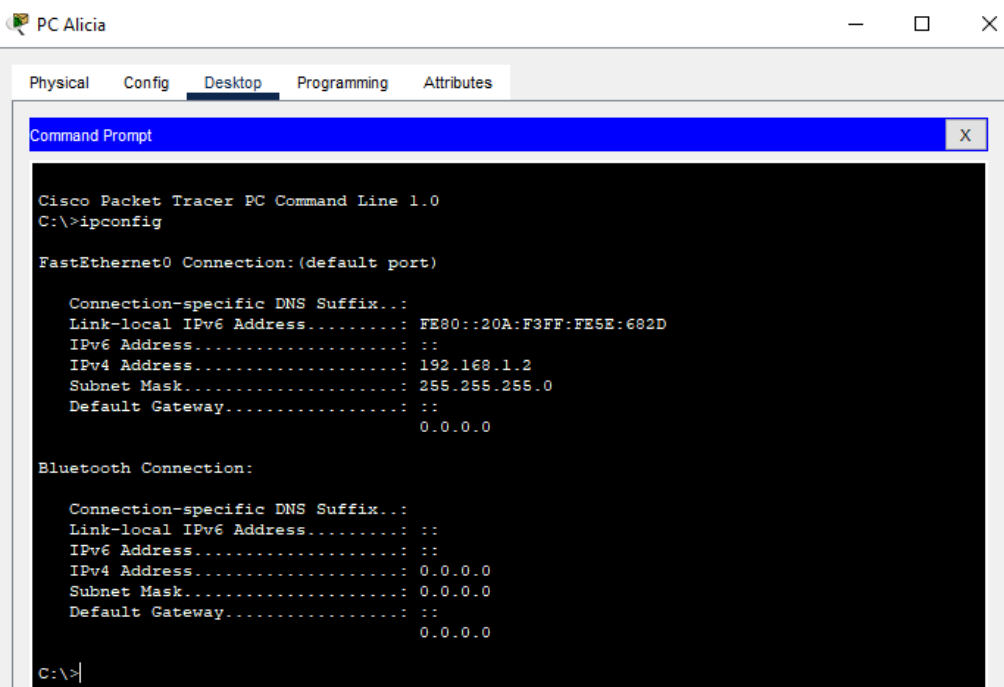
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:97FF:FE29:15A2
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>
```

PC Alicia



The screenshot shows a window titled "PC Alicia" with a "Command Prompt" window open. The command prompt displays the output of the "ipconfig" command. It shows details for the "FastEthernet0" and "Bluetooth" connections, including IPv4 and IPv6 addresses, subnet masks, and default gateways.

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

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20A:F3FF:FE5E:682D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>
```

Job 6

→ Quelle est la commande permettant de Ping entre des PC ?

On écrit la commande “**ping**” suivi de l’adresse du PC avec lequel on veut interagir dans notre cas on va écrire dans le command prompt depuis le PC Pierre la commande : **ping 192.168.1.2**

PC Pierre

```
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=12ms 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 = 12ms, Average = 3ms

C:\>|
```

On réalise la même commande depuis le PC Alicia avec cette fois l’adresse de PC Pierre **ping 192.168.1.1**

PC Alicia

```
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

C:\>|
```

Job 7

→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

PC Alicia

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

On comprend que le PC de Pierre n'a pas reçu les paquets envoyés par Alicia

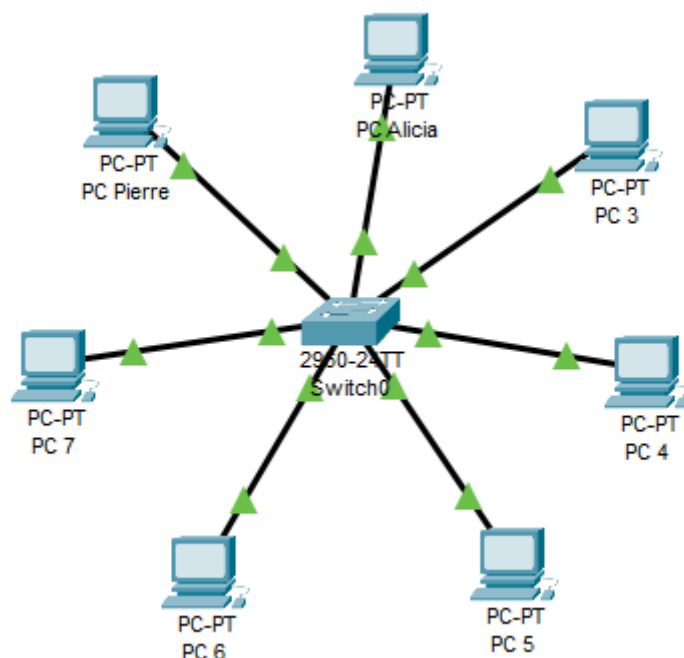
→ Expliquez pourquoi.

Les paquets envoyés par Alicia n'ont pas été reçus par Pierre car lorsqu'on éteint l'ordinateur de Pierre, il n'est pas en mesure de recevoir ou de traiter des données réseau.

Les paquets envoyés à cet ordinateur resteront en attente dans les routeurs et commutateurs du réseau jusqu'à ce que l'ordinateur soit à nouveau allumé et capable de les recevoir.

Or, les paquets réseau ont une durée de vie très courte c'est pour cela que on a sur la console "Request timed out" pour chaque paquet

Job 8



→ Quelle est la différence entre un hub et un switch ?

La principale différence entre un hub et un switch réside dans leur manière de gérer le trafic réseau. Un hub rediffuse les données à tous les dispositifs connectés, ce qui signifie que tous les dispositifs du réseau reçoivent toutes les données, même si elles ne sont pas destinées à eux, entraînant une utilisation inefficace de la bande passante.

En revanche, un switch examine l'adresse MAC des données et les transmet uniquement au dispositif de destination approprié, ce qui améliore l'efficacité du réseau en évitant la surcharge de trafic inutile.

→ Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

Un hub est un dispositif réseau qui fonctionne en transmettant les données reçues à tous les dispositifs connectés à lui, sans distinction. Lorsqu'un paquet de données arrive sur un port d'un hub, il est immédiatement répété sur tous les autres ports du hub, ce qui signifie que chaque dispositif du réseau reçoit toutes les données, qu'elles leur soient destinées ou non.

Les avantages d'un hub résident dans leur simplicité et leur coût relativement bas. Ils sont faciles à installer, généralement sans besoin de configuration complexe, et conviennent aux petits réseaux où le trafic est limité.

Cependant, les inconvénients des hubs sont significatifs. Le principal inconvénient est leur inefficacité. Puisque les données sont diffusées à tous les dispositifs, même si elles ne leur sont pas destinées, cela entraîne une utilisation inefficace de la bande passante.

→ Quels sont les avantages et inconvénients d'un switch ?

Les switches offrent plusieurs avantages significatifs dans la gestion des réseaux. Ils permettent une transmission de données plus efficace en envoyant les paquets uniquement vers les dispositifs destinataires, ce qui réduit la congestion du réseau et améliore les performances.

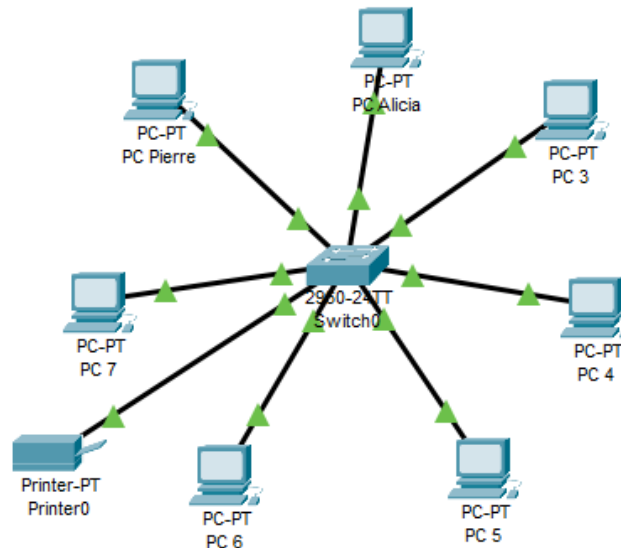
Cependant, le principal inconvénient est leur coût, car ils sont généralement plus chers que les hubs et leur configuration et la gestion des switches peuvent être plus complexes.

→ Comment un switch gère-t-il le trafic réseau ?

Un switch gère le trafic réseau en utilisant une approche plus intelligente et sélective que celle d'un hub, lorsqu'un dispositif est connecté au switch, ce dernier enregistre l'adresse MAC de ce dispositif dans une table et lorsqu'une donnée est reçue, le switch examine l'adresse MAC de destination pour déterminer sur quel port elle doit être transmise.

Au lieu de diffuser les données à tous les ports, comme le fait un hub, le switch envoie les données uniquement au port correspondant au dispositif de destination, réduisant ainsi la congestion du réseau et améliorant les performances.

Job 9



- ☐ Permet une meilleur vision permettant de prendre du recul
- ☐ Permet une facilité de compréhension
- ☐ Permet d'avoir une liberté de réflexion

Job 10

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

La principale différence entre une adresse IP statique et une adresse IP attribuée par DHCP réside dans la manière dont elles sont configurées et gérées.

Une adresse IP statique est configurée manuellement par un administrateur réseau, celui-ci choisit une adresse IP spécifique pour un dispositif et la configure dans les paramètres réseau de ce dispositif de manière permanente.

En revanche, une adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) est obtenue automatiquement auprès d'un serveur DHCP lors de sa première connexion au réseau, il envoie une demande au serveur DHCP, qui attribue une adresse IP disponible à ce dispositif.

Job 11

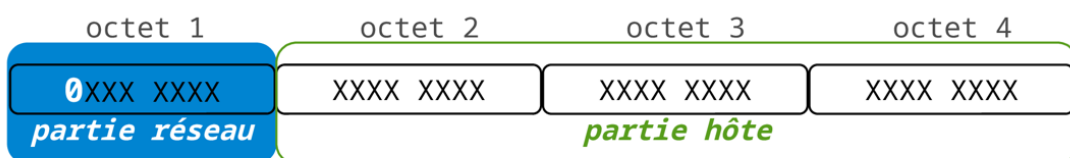
→ Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

On a choisi une adresse de classe A car les adresses de classe A offrent une grande flexibilité pour diviser votre réseau en sous-réseaux plus petits à mesure que votre réseau évolue. Cela peut être utile pour l'organisation et la gestion de votre infrastructure réseau

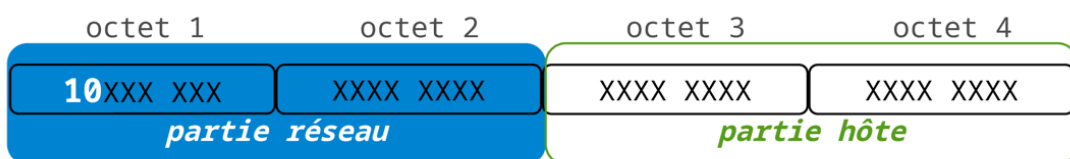
→ Quelle est la différence entre les différents types d'adresses ?

La principale différence réside dans leur utilisation en fonction de la taille du réseau.

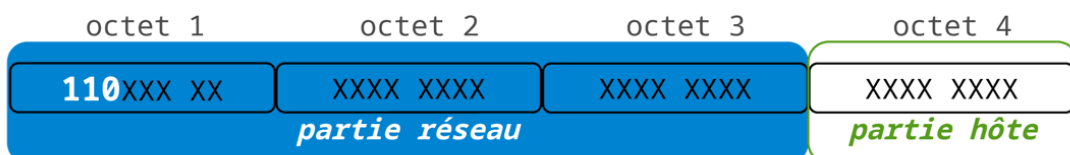
Classe A



Classe B



Classe C

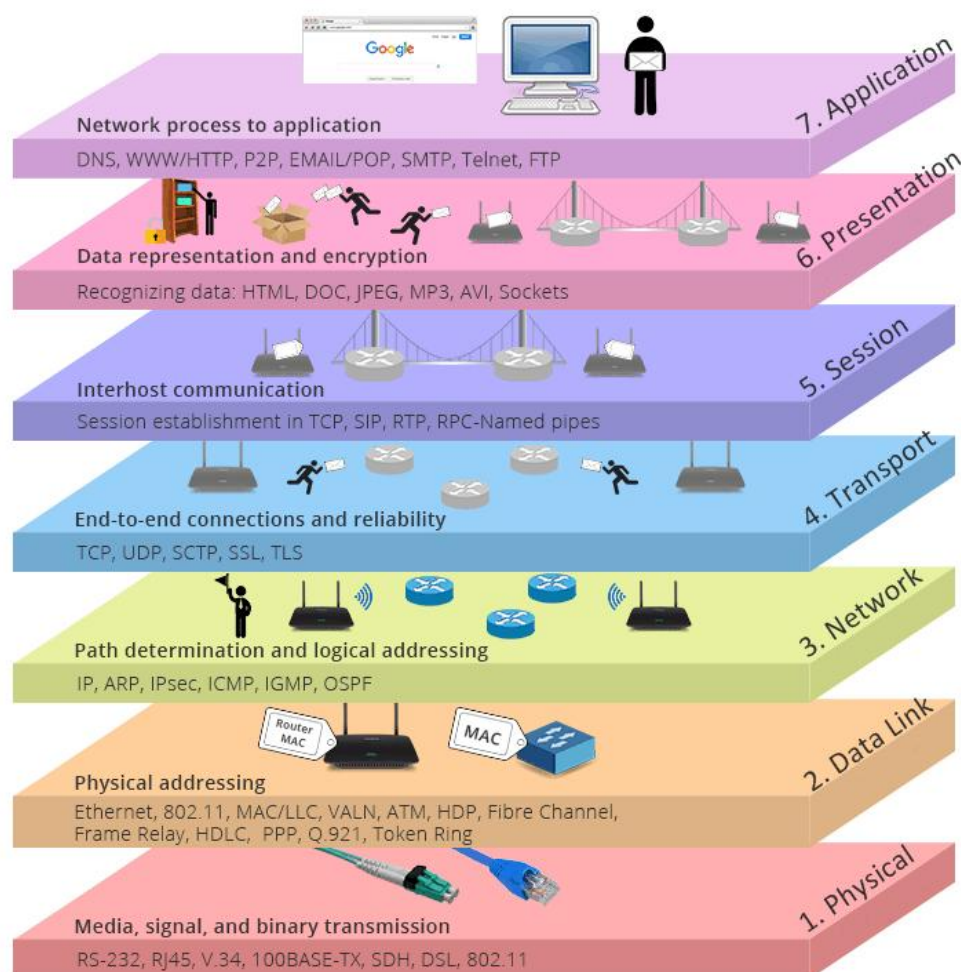


	Plan d'adressage	Masque de sous-réseau et nombre de bits
Sous-réseaux de 12 hôtes	10.0.0.0 à 10.0.0.15	255.255.255.240
Sous-réseaux de 30 hôtes	10.0.1.0 à 10.0.1.31	255.255.255.224
	10.0.2.0 à 10.0.2.31	
	10.0.3.0 à 10.0.3.31	
	10.0.4.0 à 10.0.4.31	
	10.0.5.0 à 10.0.5.31	
Sous-réseaux de 120 hôtes	10.0.6.0 à 10.0.6.128	255.255.255.128
	10.0.7.0 à 10.0.7.128	
	10.0.8.0 à 10.0.8.128	
	10.0.9.0 à 10.0.9.128	
	10.0.10.0 à 10.0.10.128	
Sous-réseaux de 160 hôtes	10.0.11.0 à 10.0.11.255	255.255.255.0
	10.0.12.0 à 10.0.12.255	
	10.0.13.0 à 10.0.13.255	
	10.0.14.0 à 10.0.14.255	
	10.0.15.0 à 10.0.15.255	

Job 12

Couche OSI	Description des rôles	Matériels/Protocoles
couche 7	Application	DNS, FTP, HTTP,..
couche 6	Présentation	SSL/TLS, HTML,..
couche 5	Session	SSL/TLS, PPTP,..
couche 4	Transport	TCP, UDP, SCTP,..
couche 3	Réseau	IPv4, IPv6, routeur,..
couche 2	Liaison de données	Ethernet, MAC, Wi-Fi, câble RJ45,..
couche 1	Physique	Fibre optique, câble RJ45,..

et en plus jolie



Job 13

→ Quelle est l'architecture de ce réseau ?

Il s'agit de l'architecture d'un réseau LAN puisque tous les dispositifs fonctionnent sur le même réseau.

→ Indiquer quelle est l'adresse IP du réseau ?

192.168.10.0

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

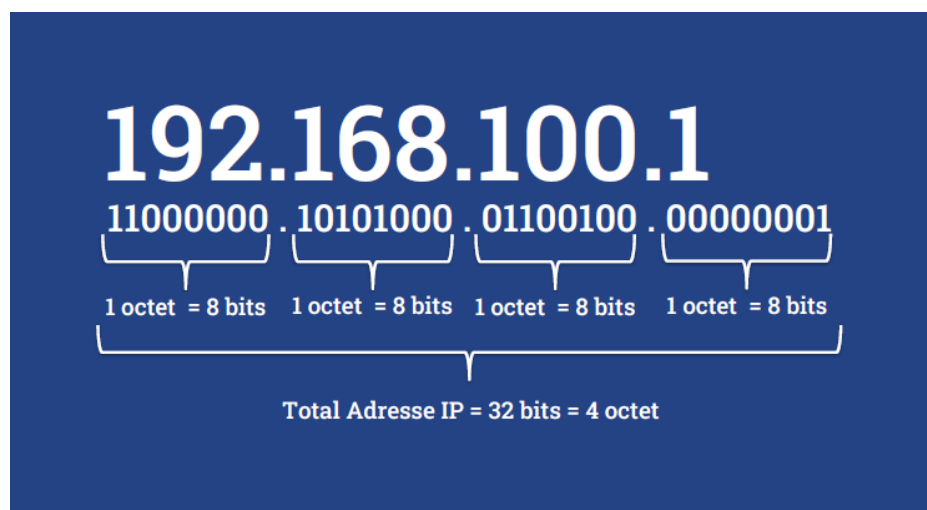
De 0 à 255 or l'adresse en 0 correspond à l'adresse du réseau et l'adresse en 255 correspond à l'adresse de diffusion du réseau ce qui laisse 254 adresses disponibles soit donc : 254 machines

→ Quelle est l'adresse de diffusion de ce réseau ?

192.168.10.255

Job 14

On peut soit le faire avec le calcul pour cela on doit comprendre le schéma d'une adresse IP (ici IPv4)



le reste c'est simplement des calculs que l'on peut faire sur feuille ou avec la calculatrice

l'autre méthode serait d'utiliser un convertisseur d'adresse IP en binaire ce qui est pratique une fois qu'on a compris le principe

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

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission des données d'un point à un autre à travers un réseau. Il implique la détermination du chemin optimal pour que les données atteignent leur destination en passant par différents dispositifs interconnectés tels que des routeurs.

→ Qu'est-ce qu'un gateway ?

gateway ou une passerelle en français, est un dispositif ou un logiciel qui interconnecte deux réseaux informatiques distincts et leur permet de communiquer entre eux, les passerelles permettent de traduire les différentes conventions de communication utilisées par ces réseaux. Par exemple, une passerelle peut connecter un réseau local (LAN) à Internet, ce qui permet aux dispositifs du LAN d'accéder à des ressources sur Internet ou de communiquer avec des réseaux distants.

→ Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network), ou Réseau Privé Virtuel en français, est une technologie qui permet de créer un tunnel de communication sécurisé sur Internet. Il est conçu pour protéger la confidentialité et la sécurité des données échangées entre un utilisateur ou un réseau local et un serveur distant. Les données sont chiffrées, ce qui rend difficile pour des tiers de les intercepter ou de les surveiller.

→ Qu'est-ce qu'un DNS ?

Un DNS, ou Domain Name System (Système de Noms de Domaine en français), est un système informatique utilisé sur internet pour convertir les noms de domaine conviviaux que les gens utilisent en adresses IP numériques, qui sont nécessaires pour localiser les serveurs et les ressources en ligne, pour faire plus simple, le DNS agit comme un annuaire pour l'Internet, en traduisant les noms de domaine en adresses IP, facilitant ainsi la navigation sur le web pour les utilisateurs.