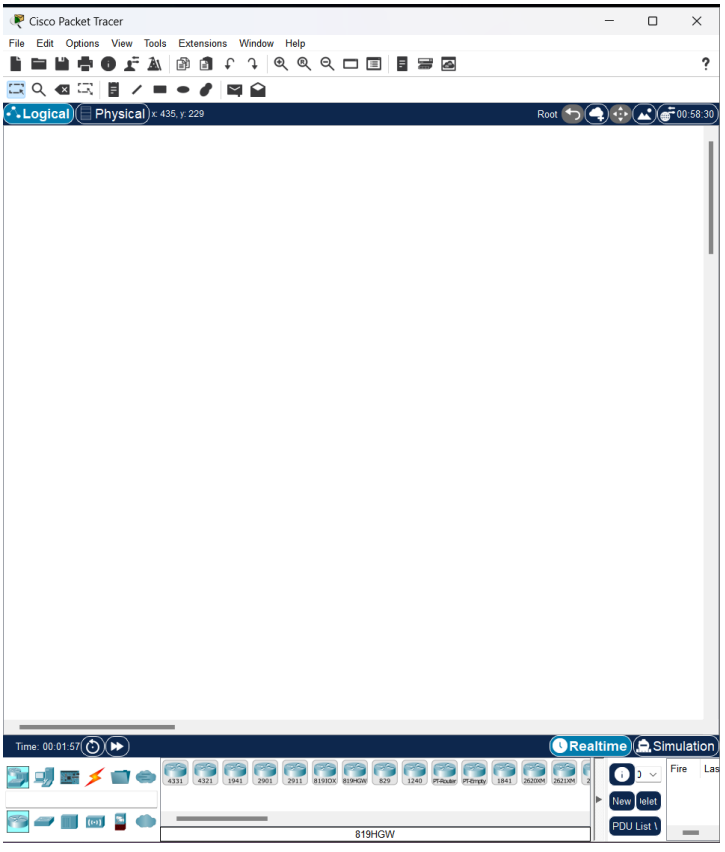
La Plateforme

Runtrack Réseau

Pourquoi les administrateurs réseau aiment-ils les oiseaux ? Parce qu'ils ont des protocoles de migration bien définis !

Job 1:

Pour commencer à utiliser **Cisco Packet Tracer**, j'ai suivi une procédure d'installation simple. J'ai tout d'abord téléchargé le logiciel depuis le site officiel de Cisco Networking Academy en m'identifiant avec mon compte Cisco. Une fois le téléchargement terminé, j'ai ouvert le fichier d'installation. Là, j'ai suivi les étapes de l'assistant d'installation en optant pour les paramètres par défaut, à moins que j'aie des besoins particuliers. Une fois l'installation terminée, j'ai lancé Packet Tracer, et j'ai été immédiatement prêt à concevoir, configurer et dépanner des réseaux informatiques.



Job 2:

1.Un réseau:

Un réseau est une infrastructure qui permet à plusieurs dispositifs de communiquer entre eux. Il se compose de composants matériels (matériel réseau) et de logiciels (protocoles de communication) qui facilitent la transmission d'échange d'informations entre les différents appareils connectés.

2.Un réseau informatique:

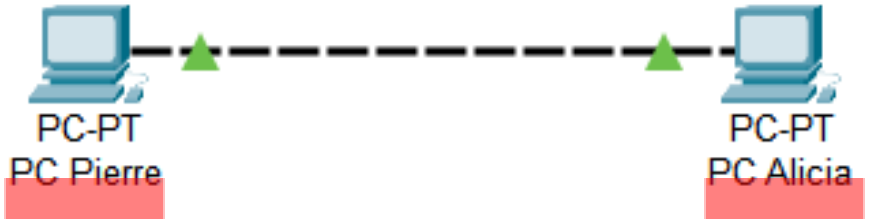
Un réseau informatique connecte des appareils pour partager des ressources et faciliter la communication. Il permet d'accéder à Internet, centraliser des données, effectuer des sauvegardes et automatiser des processus. Les composants clés incluent des routeurs, des commutateurs, des pare-feu, des câbles Ethernet, des points d'accès Wi-Fi et des serveurs.

3.Construire un réseau:

Pour construire un réseau, vous avez besoin de ces composants essentiels :

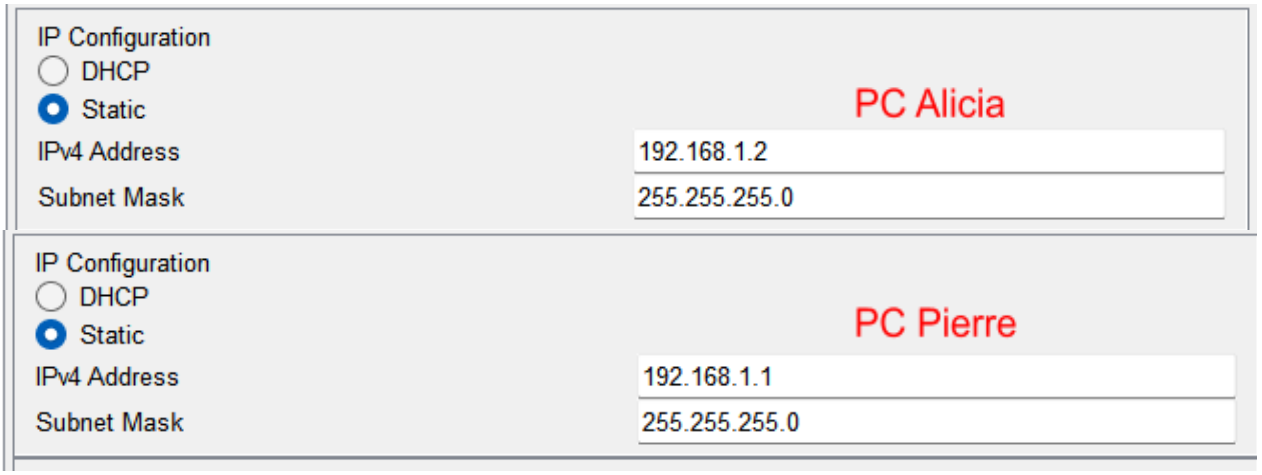
- Routeur : relie le réseau local à Internet et gère les adresses IP.
- Commutateur (Switch) : Connecte les appareils du réseau local et facilite la communication.
- Pare-feu (Firewall) : Sécurise le réseau en contrôlant le trafic et en bloquant les menaces
- Modem : Permet la connexion à Internet en convertissant les signaux.
- Câbles Ethernet : Connectent les dispositifs physiquement.
- Point d'accès sans fil (WAP) : Étend la connectivité sans fil.
- Serveur : Fournit des services spécifiques aux autres dispositifs du réseau, comme le stockage et la messagerie.

Job 3:



Dans ce schéma, j'ai créé un réseau local (LAN) rudimentaire en utilisant l'outil Packet Tracer. J'ai positionné deux ordinateurs de bureau dans mon espace de travail virtuel et les ai connectés en utilisant un câble Ethernet, établissant ainsi une liaison directe entre eux.
j'ai choisie un câble copper cross-over pour relier les deux ordinateurs car c'est utilisé pour connecter directement deux périphériques de réseau de même type, sans avoir besoin d'un équipement intermédiaire tel qu'un routeur ou un commutateur. Les câbles crossover sont câblés de manière à croiser les broches à chaque extrémité, permettant ainsi une communication directe entre les deux périphériques.

Job 4:



1. Une adresse IP (Internet Protocol) est une série de numéros qui identifie de manière unique un périphérique sur un réseau, lui permettant de communiquer avec d'autres périphériques. Les adresses IP sont essentielles pour le routage des données sur Internet et les réseaux locaux.

2. Une adresse IP sert à identifier un périphérique dans un réseau et à lui permettre d'envoyer et de recevoir des données au sein de ce réseau ou sur Internet. Elle fonctionne comme l'équivalent d'une adresse postale pour les ordinateurs et les appareils connectés, leur permettant de se localiser mutuellement et d'échanger des informations.

3. Une adresse MAC (Media Access Control) est un identifiant unique attribué à chaque carte réseau ou adaptateur réseau. Contrairement à une adresse IP, une adresse MAC est fixe et ne change pas. Elle est utilisée pour identifier un périphérique au sein d'un réseau local.

4. Une adresse IP publique est une adresse utilisée pour identifier un périphérique sur Internet, accessible depuis n'importe où dans le monde. En revanche, une adresse IP privée est utilisée pour identifier un périphérique dans un réseau local, tel qu'un réseau domestique, et n'est généralement pas accessible directement depuis Internet. Les adresses IP privées sont utilisées pour router le trafic à l'intérieur du réseau local, tandis que les adresses IP publiques sont utilisées pour le trafic entre les réseaux sur Internet.

5. L'adresse du réseau pour PC Pierre et PC Alicia est 192.168.1.0. Lorsqu'on configure des adresses IP pour un réseau local, l'adresse du réseau est déterminée en utilisant les bits du masque de sous-réseau. Dans ce cas, avec un masque de sous-réseau de 255.255.255.0, les trois premiers octets (192.168.1) définissent l'adresse du réseau, tandis que le dernier octet (0) est réservé pour les adresses spécifiques aux appareils du réseau.

Job 5:

La ligne de commande utilisée pour vérifier l'Id des machines est: ipconfig

```
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:FE8D:74A6
   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:\>
```

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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:70FF:FE28:6D33
   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:\>
```

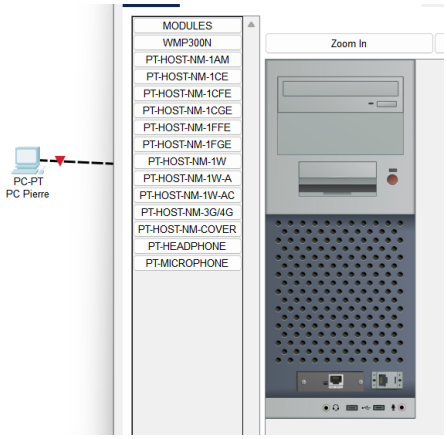
Job 6:

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::209:7CFF:FE93:1B72
   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:\>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
```

```
FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:47FF:FEA5:8ADC
   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:\>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
```

la commande utilisée est ping <adresse IP ou nom d'hôte >

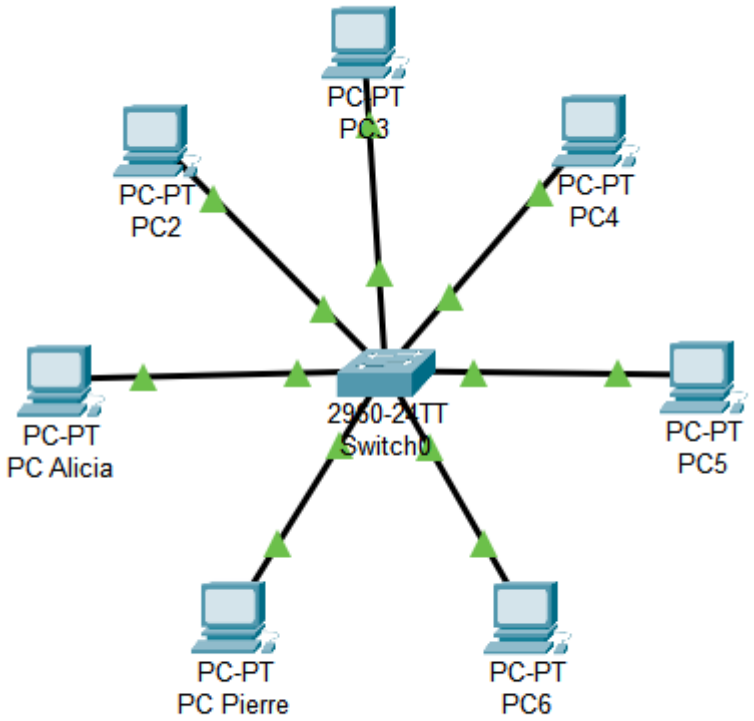
Job 7:




```
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),
```

Le protocole ICMP (Internet Control Message Protocol) utilisé par la commande ping est conçu pour envoyer des paquets d'écho (ping) à une adresse IP spécifique et attendre une réponse de l'ordinateur cible. Si l'ordinateur cible (PC de Pierre) est éteint, il ne peut pas recevoir ni répondre aux paquets ICMP.
Par conséquent, la commande ping d'Alicia n'obtiendrait aucune réponse, ce qui se traduirait par un "hôte de destination inaccessible" ou un nombre élevé de paquets perdus.

Job 8:



1. Différence entre un hub et un switch :

- Un hub est un dispositif de couche 1 (physique) du modèle OSI, qui agit comme un répéteur, diffusant tout le trafic qu'il reçoit à tous les ports. Il ne prend pas en compte les adresses MAC.
- Un switch est un dispositif de couche 2 (liaison de données) qui examine les adresses MAC pour déterminer où diriger le trafic. Il maintient une table de correspondance entre les adresses MAC des dispositifs connectés à ses ports.

2. Fonctionnement d' un hub :

- Un hub répète simplement les signaux qu'il reçoit sur un port à tous les autres ports.
- Avantages : Il est simple et peu coûteux, mais en général obsolète.
- Inconvénients : Il génère beaucoup de trafic inutile et peut entraîner des collisions sur un réseau Ethernet, réduisant l'efficacité.

3. Avantages et inconvénients d'un switch :

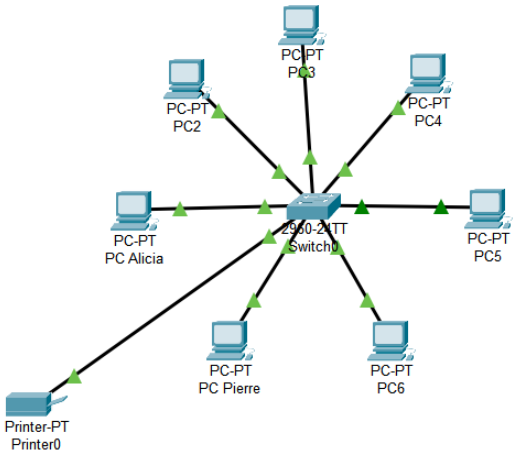
- Avantages :
  - Il permet une commutation intelligente du trafic, envoyant les données uniquement vers le port du destinataire, ce qui améliore les performances et réduit le trafic inutile.
  - Il peut isoler les ports, améliorant la sécurité.
  - Il prend en charge des fonctionnalités avancées comme la qualité de service (QoS) et la surveillance du trafic.

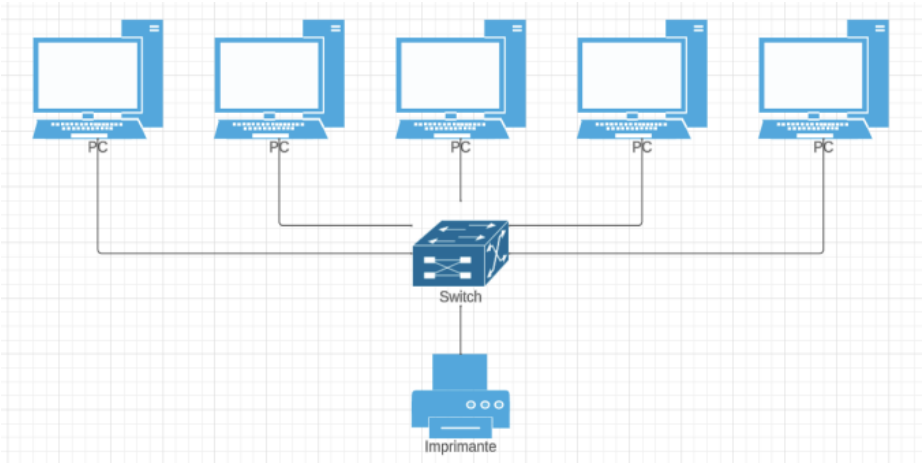
- Inconvénients :
  - Il est plus coûteux qu'un hub.
  - Les switchs non gérés ont des fonctionnalités limitées par rapport aux switchs gérés.

4. Comment un switch gère le trafic réseau :

- Un switch examine les trames Ethernet entrantes pour extraire les adresses MAC source et de destination.
- Il consulte sa table MAC (table d'adresses) pour déterminer sur quel port se trouve l'adresse MAC de destination.
- Il envoie ensuite la trame uniquement vers ce port spécifique.
- Il apprend continuellement les adresses MAC en surveillant le trafic, mettant à jour sa table MAC en conséquence.
- Cela permet au switch de réduire la congestion du réseau en envoyant du trafic uniquement vers les ports nécessaires et d'améliorer les performances globales du réseau.

Job 9:

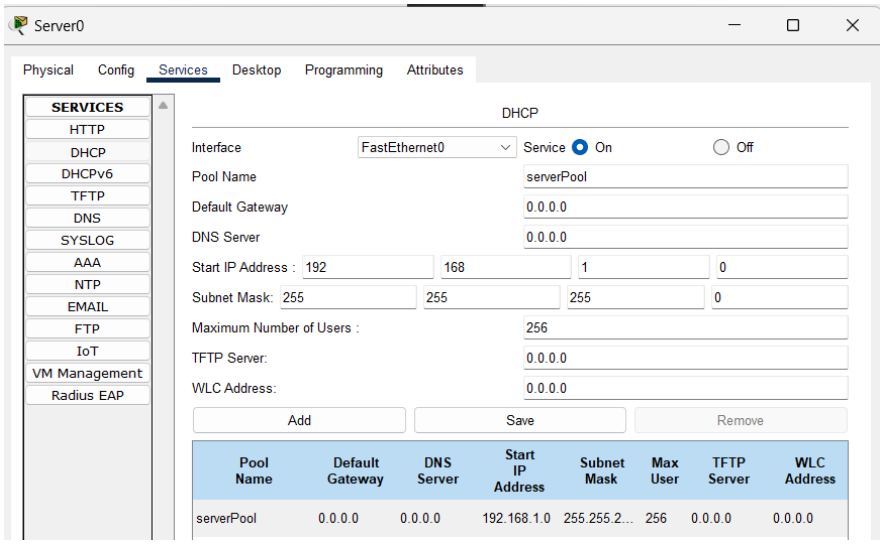


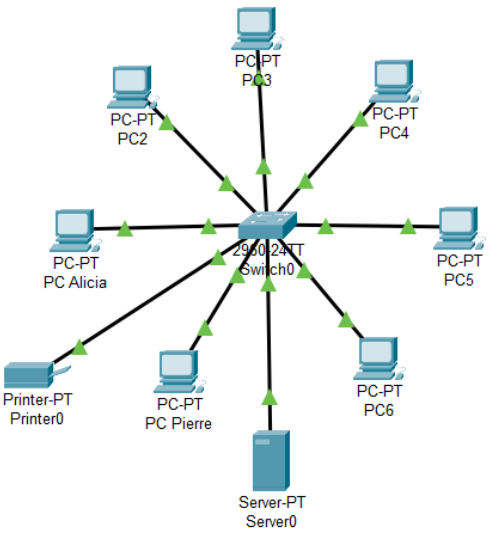


Avantages d'avoir un schéma de réseau :

- Documentation claire : Un schéma de réseau fournit une documentation visuelle claire de la topologie de votre réseau, ce qui facilite la compréhension de sa configuration.
- Dépannage plus facile : En cas de problèmes de connectivité ou de configuration, un schéma de réseau peut être un outil précieux pour identifier rapidement les sources des problèmes.
- Planification et expansion simplifiées : Vous pouvez utiliser un schéma de réseau pour planifier des mises à jour, des ajouts de périphériques, ou des expansions de réseau, en vous assurant qu'ils s'intègrent correctement dans la configuration existante.

Job 10:





Une adresse IP est un identifiant unique pour les appareils sur un réseau. La principale différence entre une adresse IP statique et une attribuée par le DHCP réside dans leur configuration et leur gestion. **Une adresse IP statique** est définie manuellement par un administrateur réseau ou un utilisateur et reste constante, sauf si elle est modifiée manuellement. Elle est généralement utilisée pour les appareils qui nécessitent une adresse IP constante, comme les serveurs ou les imprimantes réseau. En revanche, **une adresse IP attribuée par le DHCP** est gérée de manière dynamique par un serveur DHCP dans le réseau. Lorsqu'un appareil se connecte au réseau, le serveur DHCP attribue automatiquement une adresse IP. Ces adresses IP attribuées dynamiquement peuvent changer à chaque connexion en fonction des adresses disponibles dans le pool DHCP. Cette méthode est couramment utilisée pour les appareils clients tels que les ordinateurs de bureau et les appareils mobiles, afin de simplifier la gestion des adresses IP et garantir une utilisation efficace de celles-ci.

Job 11:

	Plage d'adresse	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	

1. L'attribution de l'adresse IP 10.0.0.0 en tant qu'adresse de classe A s'explique par sa capacité intrinsèque à répondre aux besoins de réseaux de grande envergure. Les adresses de classe A se caractérisent par une vaste plage d'adresses, ce qui les rend idéales pour la création d'un grand nombre de sous-réseaux et la prise en charge d'un grand nombre d'hôtes. Dans ce cas , l'utilisation de cette adresse de classe A se justifie pleinement, car elle permet de subdiviser le réseau en 21 sous-réseaux, certains d'entre eux pouvant accueillir un nombre significatif d'hôtes. Cette approche offre une flexibilité et une évolutivité essentielles pour les réseaux complexes, répondant ainsi aux besoins en matière de gestion et de croissance de l'infrastructure réseau.

2. Les différents types d'adresses IP (A, B, C, etc.) sont définis par leur classe, qui détermine la plage d'adresses disponibles et le nombre d'hôtes pouvant être pris en charge. Les classes d'adresses sont réparties comme suit :
   - Classe A : Conçue pour les réseaux de grande envergure, avec un octet d'adresse réseau et trois octets d'adresse hôte. Elle peut prendre en charge un grand nombre d'hôtes.
   - Classe B : Conçue pour les réseaux de taille moyenne, avec deux octets d'adresse réseau et deux octets d'adresse hôte. Elle peut prendre en charge un nombre moyen d'hôtes.
   - Classe C : Conçue pour les réseaux de petite taille, avec trois octets d'adresse réseau et un octet d'adresse hôte. Elle peut prendre en charge un petit nombre d'hôtes.
   - Classe D (multicast) et Classe E (réservée) ne sont pas couramment utilisées pour l'adressage des hôtes.

Job 12:

Couche OSI	Description	Exemples de Matériels, Protocoles et Technologies
Couche 7 - Application	Interface utilisateur, services d'application et interaction avec les applications.	HTML,FTP,SSL/TLS,PPTP
Couche 6 - Présentation	Gestion de la présentation des données, cryptage, compression, conversion de formats.	SSL/TLS, HTML, JPEG, GIF
Couche 5 - Session	Établissement, gestion et terminaison des sessions de communication.	NetBIOS, API RESTful, WebSocket
Couche 4 - Transport	Assure le transport fiable des données, contrôle du flux, segmentation et réassemblage.	TCP, UDP
Couche 3 - Réseau	Routage des données à travers le réseau, gestion de sous-réseaux.	IPv4, IPv6, routeur, sous-réseaux, IPsec
Couche 2 - Liaison de données	Gestion de l'accès au support physique, adresses MAC.	Ethernet, Wi-Fi, câble RJ45, commutateur, adresse MAC
Couche 1 - Physique	Transfert de bits bruts sur le support physique, spécifications de câblage.	Fibre optique, câble RJ45, câble coaxial, hubs, répéteurs

Job 13:

1. Architecture du réseau :
   Le réseau utilise l'adresse IP 192.168.10.0/24 avec un masque de sous-réseau 255.255.255.0. Cela indique un réseau de classe C avec un masque de sous-réseau par défaut.

2. Adresse IP du réseau :
   L'adresse IP du réseau est 192.168.10.0.

3. Nombre de machines pouvant être connectées au réseau :
   Avec un masque de sous-réseau de 255.255.255.0 , il y a 256 adresses IP possibles au total. Cependant, deux adresses IP sont réservées : l'adresse du réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255). Il reste 254 adresses IP pour les PCs et serveurs qui peuvent être branchées sur ce réseau.

4. Adresse de diffusion du réseau :
   L'adresse de diffusion de ce réseau est 192.168.10.255. Elle est utilisée pour envoyer des données à toutes les machines du réseau en même temps.

Job 14:

les adresses IP en binaires :

145.32.59.24 (IPv4) Binary :

10010001.00100000.00111011.00011000

200.42.129.16 (IPv4) Binary :

11001000.00101010.10000001.00010000

14.82.19.54 (IPv4) Binary :

00001110.01010010.00010011.00110110

Job 15:

1. le routage :

   Le routage est le processus de transmission de données d'un point à un autre à travers un réseau. Il s'agit de déterminer la meilleure trajectoire ou chemin pour faire parvenir les données de l'expéditeur au destinataire. Les routeurs, qui sont des dispositifs réseau, sont responsables du routage en analysant les adresses IP des données et en choisissant la voie optimale pour les faire circuler à travers le réseau.

2. Un gateway :

   Une gateway, ou passerelle en français, est un dispositif matériel ou logiciel qui permet de relier deux réseaux informatiques hétérogènes. Les gateways sont essentielles pour permettre la communication entre différents types de réseaux, tels que la connexion d'un réseau local (LAN) à Internet, la conversion de protocoles de communication, ou la mise en place de passerelles entre des réseaux sans fil et filaires. Elles jouent un rôle de traducteur et de médiateur entre les différents réseaux.

3. Un VPN :

Un VPN, ou Réseau Privé Virtuel en français, est un service de sécurité qui permet de créer une connexion cryptée et sécurisée sur Internet. Il est utilisé pour protéger la confidentialité des données, l'anonymat de l'utilisateur et pour établir des connexions sécurisées sur des réseaux publics, comme Internet. Un VPN permet de masquer l'adresse IP de l'utilisateur, rendant ainsi sa navigation plus confidentielle, tout en chiffrant les données qui transitent entre son appareil et le serveur VPN.

4. Un DNS :

   Le DNS, ou Système de Noms de Domaine, est un protocole fondamental pour le fonctionnement d'Internet. Il est utilisé pour traduire les noms de domaine en adresses IP numériques que les ordinateurs peuvent comprendre. Les serveurs DNS sont responsables de cette traduction, permettant aux utilisateurs d'accéder à des sites web en utilisant des noms de domaine conviviaux, au lieu de se souvenir d'adresses IP numériques complexes. Le DNS joue un rôle crucial dans la navigation sur Internet en aidant à trouver des ressources en ligne.