Enam AKLI - Runtrack Réseau

JOB 2.

1. Un réseau est un ensemble interconnecté de dispositifs ou d'ordinateurs qui communiquent entre eux pour partager des informations, des ressources et des services. Ces dispositifs, appelés nœuds, peuvent être connectés par des câbles physiques (comme des câbles Ethernet) ou par des liaisons sans fil (comme le Wi-Fi). Les réseaux permettent aux utilisateurs d'accéder à des données, de partager des fichiers, d'imprimer, de communiquer via des courriels, des chats ou des visioconférences, et bien plus encore.

2.Un réseau informatique a plusieurs objectifs importants :

- **Partage de ressources**: Il permet le partage de fichiers, d'imprimantes, de connexions Internet, et d'autres ressources entre les ordinateurs connectés au réseau.

- **Communication**: Il facilite la communication entre les utilisateurs, que ce soit par le biais de courriels, de messagerie instantanée, de visioconférences, ou d'autres moyens.

- **Accès à distance**: Il permet l'accès à des ordinateurs ou des serveurs distants pour récupérer des données ou exécuter des applications à partir de n'importe où dans le monde.

- **Sécurité**: Il offre des moyens de sécuriser les données en transit et d'accéder aux ressources de manière contrôlée.

- **Économie**: Il permet de réduire les coûts en partageant des ressources plutôt qu'en en ayant une par utilisateur.

- **Redondance**: Il assure la disponibilité continue des services en cas de défaillance d'un nœud, grâce à la redondance.

3. Pour construire un réseau informatique, il va falloir de divers composants matériels, chacun ayant un rôle spécifique :

- **Ordinateurs/Dispositifs Clients**: Ce sont les ordinateurs ou dispositifs finaux utilisés par les utilisateurs pour accéder au réseau et aux ressources partagées.

- **Serveurs**: Les serveurs sont des ordinateurs puissants dédiés à des tâches spécifiques, comme le stockage de données, la gestion des utilisateurs, l'hébergement de sites web, et al .

- **Routeurs**: Les routeurs dirigent le trafic entre différentes parties du réseau et entre le réseau local et Internet. Ils prennent des décisions sur la meilleure route pour acheminer les données.

- **Switches**: Les commutateurs sont utilisés pour connecter plusieurs appareils au sein d'un réseau local (LAN). Ils transmettent les données uniquement aux appareils qui en ont besoin, améliorant ainsi l'efficacité du réseau.

- **Modems**: Les modems sont utilisés pour se connecter à Internet via une ligne à large bande (comme DSL, câble ou fibre optique). Ils convertissent le signal numérique de l'ordinateur en signal analogique pour la transmission sur la ligne, et vice versa.

- **Câbles et Connecteurs**: Les câbles Ethernet et les connecteurs RJ-45 sont couramment utilisés pour relier les dispositifs au réseau. Les câbles à fibre optique sont utilisés pour les réseaux à haut débit.

- **Points d'accès Wi-Fi**: Ils permettent aux appareils sans fil de se connecter au réseau.

- **Firewalls**: Les pare-feu assurent la sécurité du réseau en filtrant le trafic entrant et sortant, en bloquant les menaces potentielles.

- **Serveurs de fichiers et de stockage en réseau**: Ils stockent des données partagées accessibles à partir de différents appareils du réseau.

- **Imprimantes réseau**: Elles permettent l'impression depuis n'importe quel ordinateur du réseau.

- **Systèmes de sauvegarde en réseau**: Ils assurent la sauvegarde des données importantes du réseau.

JOB 3

Jái choisi un câble croisé pour permettre une connectivité directe et une communication entre deux PC sans avoir besoin d'un périphérique réseau intermédiaire, tel qu'un commutateur ou un routeur. Voici pourquoi un câble croisé est choisi à cette fin:

1. **Les Câbles Croisés Échangent les Broches de Transmission et de Réception :** Lorsque vous souhaitez connecter directement deux périphériques similaires, tels que deux ordinateurs ou deux commutateurs, vous avez besoin d'un moyen pour que les signaux de transmission d'un appareil se connectent aux broches de réception de l'autre appareil, et vice versa. Un câble croisé réalise cela en échangeant les broches de transmission et de réception à une extrémité du câble.

2. **Communication Directe :** En utilisant un câble croisé, les deux appareils connectés peuvent communiquer directement entre eux sans avoir besoin d'un dispositif intermédiaire tel qu'un commutateur réseau. Cela est utile pour des tâches telles que le transfert de fichiers entre deux ordinateurs, la configuration d'un petit réseau peer-to-peer ou le dépannage réseau.

JOB 4

1. Une adresse IP (Internet Protocol) est une série de numéros qui identifie de manière unique un périphérique connecté à un réseau informatique. Elle est utilisée pour acheminer les données vers et depuis cet appareil sur Internet ou sur un réseau local. Il existe deux versions principales d'adresses IP : IPv4 (Internet Protocol version 4) et IPv6 (Internet Protocol version 6).

2. Une adresse IP sert à identifier et à localiser un périphérique ou un hôte sur un réseau. Elle permet le routage des données, de sorte que les informations puissent être envoyées du point A au point B sur un réseau. Les adresses IP sont essentielles pour que les dispositifs puissent communiquer et échanger des données sur Internet ou au sein d'un réseau local.

3. Une adresse MAC (Media Access Control) est une adresse physique unique attribuée à chaque carte réseau, adaptateur réseau ou interface réseau d'un périphérique. Contrairement aux adresses IP, les adresses MAC ne changent généralement pas et sont gravées dans le matériel du périphérique. Elles sont utilisées au niveau de la couche de liaison de données du modèle OSI pour identifier les périphériques sur un réseau local.

4. **Adresse IP Publique :** Une adresse IP publique est une adresse attribuée à un périphérique qui est directement accessible depuis Internet. Elle est généralement utilisée pour identifier un réseau ou un routeur sur Internet. Les serveurs Web, les services de messagerie et d'autres ressources accessibles publiquement ont des adresses IP publiques.

Adresse IP Privée : Une adresse IP privée est utilisée à l'intérieur d'un réseau local pour identifier les périphériques au sein de ce réseau. Ces adresses ne sont pas routables sur Internet, ce qui signifie qu'elles ne sont pas directement accessibles depuis l'extérieur du réseau local. Les adresses IP privées sont utilisées pour gérer les dispositifs en interne.

5. L'adresse de ce réseau est 192.168.1.0, car c'est la partie commune aux adresses IP de PC Pierre (192.168.1.1) et de PC Alicia (192.168.1.2) lorsque l'on considère le masque de sous-réseau 255.255.255.0. Cette adresse représente le réseau auquel ces deux ordinateurs sont connectés.

JOB 5

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::210:11FF:FE65:DBBE
   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:\>
```

➔ **ipconfig**

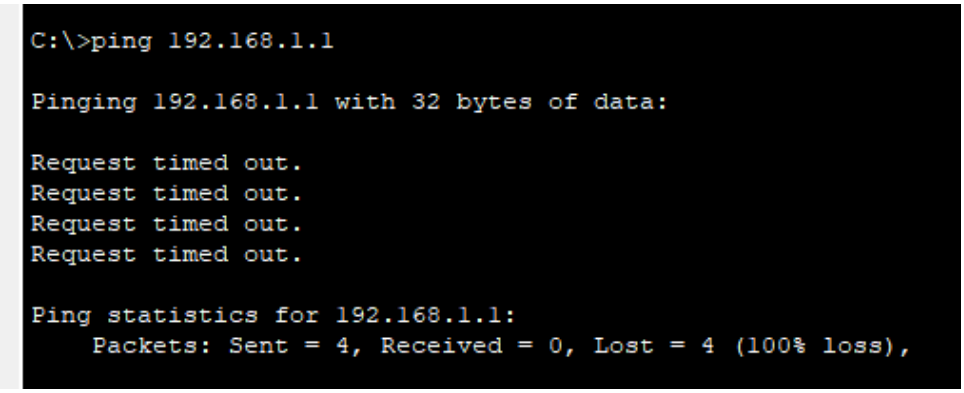
JOB 6.

```
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=4ms 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 = 4ms, Average = 1ms
```

➔ La commande pour effectuer un "ping" entre des PC dans un réseau est la suivante :

ping [adresse IP ou nom d'hôte]

JOB 7:



Non, il ne pourra pas recevoir les paquets envoyés par Alicia lorsque celle-ci utilise la commande `ping`. Lorsqu'un ordinateur est éteint, son interface réseau est désactivée, ce qui signifie qu'il n'est pas en mesure de répondre aux requêtes réseau, y compris aux demandes de ping.

Par conséquent, si le PC de Pierre est éteint, la commande `ping` d'Alicia aboutira généralement à une absence de réponse (timeout) avec un message indiquant que les paquets n'ont pas pu être atteints ou qu'ils sont perdus. Cela est dû au fait que le PC de Pierre n'est pas actif sur le réseau pour répondre aux requêtes ICMP (Internet Control Message Protocol) générées par la commande `ping`.

Job 8

Les hubs et les switches sont des dispositifs utilisés dans les réseaux informatiques pour connecter plusieurs appareils ensemble, mais ils fonctionnent de manière différente et ont des avantages et des inconvénients distincts.

1. **Différence entre un hub et un switch:**

- Un hub est un dispositif de couche 1 du modèle OSI (couche physique). Il transmet simplement les données reçues sur tous les ports à tous les appareils connectés, sans prendre en compte la destination.

- Un switch est un dispositif de couche 2 du modèle OSI (couche liaison de données). Il analyse les adresses MAC des données entrantes et les transmet uniquement au port où se trouve l'appareil de destination, ce qui permet une communication plus efficace dans le réseau.

2. **Fonctionnement et avantages/inconvénients d'un hub:**

- **Fonctionnement :** Un hub répète simplement les signaux qu'il reçoit sur un port à tous les autres ports.

- **Avantages :**

  - Simplicité : Les hubs sont simples et peu coûteux.

  - Facilité d'installation : Ils ne nécessitent généralement aucune configuration.

- **Inconvénients :**

- Collision de paquets : Les données émises par un appareil peuvent entrer en collision avec celles d'autres appareils, provoquant des collisions de paquets et une utilisation inefficace de la bande passante.

- Faible sécurité : Les données sont transmises à tous les appareils, ce qui signifie qu'elles peuvent être interceptées par d'autres appareils du réseau.

3. **Avantages et inconvénients d'un switch:**

- **Avantages :**

- Efficacité : Les switches dirigent les données uniquement vers les appareils concernés, évitant ainsi les collisions de paquets.

- Sécurité accrue: Les données sont isolées, ce qui les rend plus difficiles à intercepter.

- Haute performance: Les switches offrent des performances supérieures en termes de vitesse et de capacité de gestion du trafic.

- **Inconvénients :**

- Coût : Les switches sont généralement plus coûteux que les hubs.

- Configuration: Certains switches nécessitent une configuration, bien que de nombreux modèles grand public soient plug-and-play.

4. **Fonctionnement d'un switch pour la gestion du trafic :**

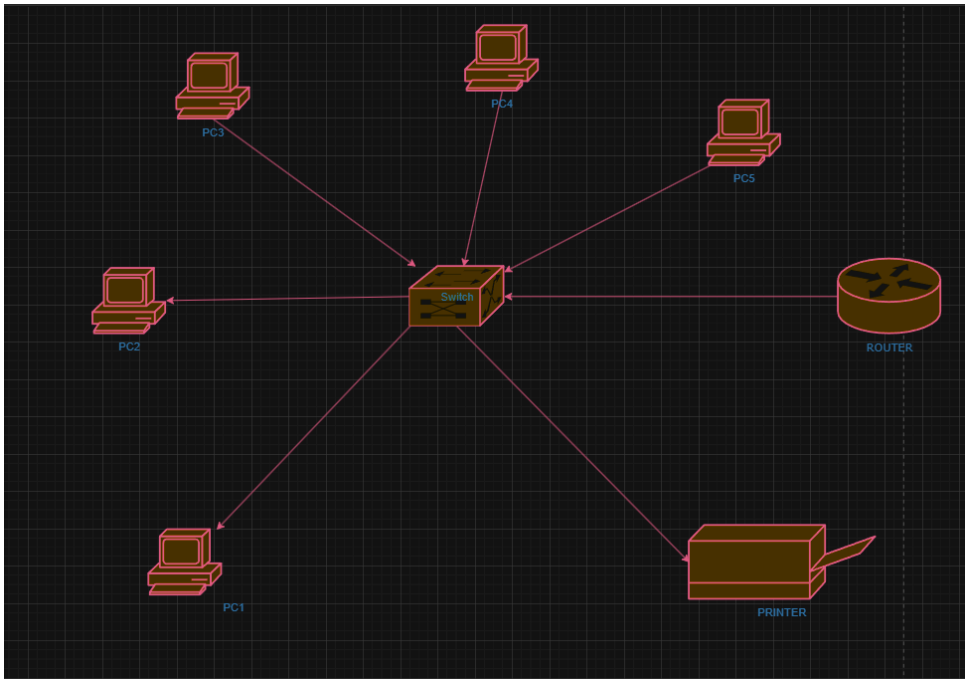
- Lorsqu'un switch reçoit des données, il examine l'adresse MAC de destination dans le cadre (frame) pour déterminer à quel port la transmission doit être dirigée.

- Le switch maintient une table d'adresses MAC pour associer chaque adresse MAC à un port spécifique.

- Une fois que l'adresse MAC de destination est identifiée, le switch transmet la transmission uniquement au port correspondant à cet appareil, minimisant ainsi la diffusion de données inutiles sur le réseau.

En résumé, les switches sont généralement préférés aux hubs dans les réseaux modernes en raison de leur efficacité, de leur sécurité accrue et de leur capacité à gérer le trafic de manière plus intelligente. Les hubs sont devenus obsolètes dans la plupart des applications en raison de leurs limitations en termes de performances et de sécurité.

JOB 9:



1. **Visualisation claire de la topologie :** Un schéma de réseau offre une représentation visuelle claire de la topologie du réseau, montrant comment les appareils sont interconnectés. Cela permet aux administrateurs réseau de comprendre rapidement la structure du réseau, y compris la disposition physique des appareils, les connexions entre les commutateurs, routeurs, pare-feu, serveurs, etc. Une visualisation claire facilite le dépannage des problèmes, l'ajout de nouveaux appareils et la planification de la croissance du réseau.

2. **Dépannage plus efficace :** Lorsqu'un problème survient dans un réseau, un schéma de réseau bien documenté permet aux administrateurs de localiser plus rapidement la source du problème. Ils peuvent suivre les connexions entre les appareils et les commutateurs, vérifier les configurations et identifier les points de défaillance potentiels. Cela réduit le temps d'arrêt du réseau et accélère la résolution des problèmes.

3. **Planification et expansion facilitées :** Un schéma de réseau aide les administrateurs à planifier la croissance du réseau et l'ajout de nouveaux appareils. Ils peuvent identifier les emplacements où de nouveaux commutateurs ou routeurs sont nécessaires, estimer la capacité requise, et prévoir l'ajout de nouvelles sous-réseaux ou segments de réseau. Cela garantit une expansion du réseau plus fluide et évite les problèmes liés à une croissance non planifiée.

Job 10:

La principale différence entre une adresse IP statique et une adresse IP attribuée par DHCP réside dans la manière dont les adresses IP sont configurées et attribuées aux appareils sur un réseau :

1. **Adresse IP statique :**

- **Attribution manuelle :** L'administrateur réseau configure manuellement chaque appareil avec une adresse IP spécifique, ainsi qu'une passerelle par défaut, un masque de sous-réseau et des serveurs DNS. Chaque appareil conserve cette adresse IP jusqu'à ce qu'elle soit modifiée manuellement.

- **Stabilité :** Les adresses IP statiques restent inchangées tant que l'administrateur réseau ne les modifie pas. Cela signifie que l'appareil aura toujours la même adresse IP, ce qui peut être important pour les serveurs ou les appareils nécessitant une adresse IP constante.

- **Gestion:** La gestion des adresses IP statiques peut devenir complexe à mesure que le réseau s'agrandit, car chaque appareil doit être configuré individuellement.

2. **Adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) :**

- **Attribution automatique :** Le serveur DHCP attribue dynamiquement des adresses IP aux appareils du réseau lorsque ceux-ci se connectent. Les appareils n'ont pas besoin d'être configurés manuellement.

- **Dynamisme :** Les adresses IP attribuées par DHCP peuvent varier chaque fois qu'un appareil se connecte au réseau. Cependant, le serveur DHCP peut être configuré pour attribuer la même adresse IP à un appareil spécifique (appelé "réservation DHCP").

- **Simplicité de gestion:** DHCP simplifie la gestion des adresses IP dans les réseaux de grande taille, car l'administrateur n'a pas besoin de configurer chaque appareil individuellement. De plus, le serveur DHCP peut gérer la distribution d'adresses IP, la mise à jour des informations réseau, etc.

En résumé, une adresse IP statique est configurée manuellement sur chaque appareil et reste constante, tandis qu'une adresse IP attribuée par DHCP est attribuée automatiquement par un serveur DHCP et peut varier. L'utilisation d'adresses IP statiques est courante pour les serveurs, les périphériques réseau critiques, tandis que DHCP est souvent utilisé pour simplifier la gestion des adresses IP dans les réseaux d'entreprise.

Job 11

1. 1 sous-réseau de 12 hôtes:

11111111.11111111.11111111.11110000

255.255.255.240/28

16 Utilisateurs

10.0.0.0 -----> Gateway

10.0.0.1 - 10.0.0.14 Pool d'addresses

10.0.0.15 -----> Broadcast

2. 5 sous-réseaux de 30 hôtes:

11111111.11111111.11111111.11100000

255.255.255.224/27

32 Utilisateurs

a. 10.0.0.16 -----> Gateway

10.0.0.17 - 10.0.0.46 Pool d'addresses

10.0.0.47 -----> Broadcast

b. 10.0.0.48 -----> Gateway

10.0.0.49 - 10.0.0.78 pool d'addresses

10.0.0.79 ----> Broadcast

c. 10.0.0.80 -----> Gateway

10.0.0.81 - 10.0.0.110 pool d'addresses

10.0.0.111 ----> Broadcast

d. 10.0.0.112 -----> Gateway

10.0.0.113 - 10.0.0.142 pool d'addresses

10.0.0.143----> Broadcast

e. 10.0.0.144 -----> Gateway

10.0.0.145 - 10.0.0.174 pool d'addresses

10.0.0.175 ----> Broadcast

3. 5 sous-réseaux de 120 hôtes

11111111.11111111.11111111.10000000

255.255.255.128/25

128 Utilisateurs

a. 10.0.0.176 -----> Gateway

10.0.0.177 - 10.0.0.254 pool d'addresses

10.0.0.255----> Broadcast

b. 10.0.1.0 -----> Gateway

10.0.1.1 - 10.0.1.126 pool d'addresses

10.0.1.127----> Broadcast

c. 10.0.1.128 -----> Gateway

10.0.1.129 - 10.0.1.254 pool d'addresses

10.0.1.255----> Broadcast

d. 10.0.2.0 -----> Gateway

10.0.2.1 - 10.0.2.126 pool d'addresses

10.0.2.127----> Broadcast

e. 10.0.2.128 -----> Gateway

10.0.2.129 - 10.0.2.254 pool d'addresses

10.0.2.255----> Broadcast

4. 5 sous-réseaux de 160 hôtes

11111111.11111111.11111111.00000000

255.255.255.0/24

256 Utilisateurs

a. 10.0.3.0 -----> Gateway

10.0.3.1 - 10.0.3.254 pool d'addresses

10.0.3.255----> Broadcast

b. 10.0.4.0 -----> Gateway

10.0.4.1 - 10.0.4.254 pool d'addresses

10.0.4.255----> Broadcast

c. 10.0.5.0 -----> Gateway

10.0.5.1 - 10.0.1.254 pool d'addresses

10.0.5.255----> Broadcast

d. 10.0.6.0 -----> Gateway

10.0.6.1 - 10.0.2.254 pool d'addresses

10.0.6.255----> Broadcast

e. 10.0.7.0 -----> Gateway

10.0.7.1 - 10.0.7.254 pool d'addresses

10.0.7.255----> Broadcast

L'adresse IP de classe A 10.0.0.0 a été choisie parce qu'elle offre une grande plage d'adresses IP, ce qui permet de créer de nombreux sous-réseaux tout en conservant un espace d'adressage suffisant. De plus, elle fait partie de la plage d'adresses IP privées, ce qui la rend appropriée pour une utilisation dans un réseau privé interne.

Classe A: Les adresses de classe A sont généralement utilisées pour les grands réseaux, car elles offrent un grand nombre d'adresses IP. Le premier octet est réservé pour le réseau, ce qui signifie que les adresses de classe A ont un format comme 1.0.0.0 à 126.0.0.0.

Classe B: Les adresses de classe B conviennent aux réseaux de taille moyenne. Le premier et le deuxième octet sont réservés pour le réseau, ce qui donne des adresses de classe B comme 128.0.0.0 à 191.255.0.0.

Classe C: Les adresses de classe C sont utilisées pour les petits réseaux. Les trois premiers octets sont réservés pour le réseau, ce qui signifie que les adresses de classe C ont un format comme 192.0.0.0 à 223.255.255.0.

Classe D et E: Les adresses de classe D (224.0.0.0 à 239.255.255.255) sont réservées pour la multidiffusion, tandis que les adresses de classe E (240.0.0.0 à 255.255.255.255) sont réservées à des fins expérimentales et de recherche.

Le sous-réseautage permet de subdiviser davantage les adresses IP de ces classes en sous-réseaux plus petits, en fonction des besoins spécifiques du réseau.

JOB 12

Couche OSI	Description et rôle	Matériels/Protocoles associés
Couche 7 - Application	Cette couche est responsable de l'interaction directe avec les applications et les services utilisateurs. Elle fournit des interfaces pour les logiciels d'application afin d'accéder au réseau.	FTP, HTTP, HTML, SSL/TLS
Couche 6 - Présentation	La couche de présentation s'occupe de la traduction, de la compression et du cryptage des données. Elle garantit que les données sont présentées de manière compréhensible à l'application.	SSL/TLS, Compression de données
Couche 5 - Session	La couche de session établit, gère et termine les sessions de communication entre les applications. Elle assure le contrôle de dialogues et la synchronisation.	PPTP, NetBIOS, RPC

Couche 4 - Transport	Cette couche assure le transport fiable des données d'un point à un autre. Elle divise les données en segments, les numérote et gère les erreurs de transmission.	TCP, UDP
Couche 3 - Réseau	La couche réseau est responsable du routage des données à travers le réseau. Elle prend des décisions de routage basées sur les adresses logiques (comme les adresses IP).	IPv4, IPv6, routeur
Couche 2 - Liaison de données	La couche liaison de données gère l'accès au support physique (câble, fibre optique) et la transmission des trames sur le réseau local. Elle identifie les périphériques sur le réseau avec des adresses MAC.	Ethernet, Wi-Fi, MAC
Couche 1 - Physique	La couche physique est responsable de la transmission des bits bruts sur le support physique. Elle gère la conversion entre les signaux électriques, optiques ou radio.	Fibre optique, câble RJ45

JOB 13

L'adresse IP du réseau est 192.168.10.0 avec un masque de sous-réseau 255.255.255.0.

1. **Architecture du réseau :** Le réseau utilise une architecture en étoile. Dans cette topologie, tous les périphériques, y compris les PC et les serveurs, sont connectés à un point central ou à un concentrateur. Dans ce cas précis, les adresses IP des PC (PC0, PC1, PC2, PC3) ainsi que des serveurs (Serveur 1 et Serveur 2) sont tous situées dans la même plage d'adresses IP (192.168.10.x) avec un masque de sous-réseau commun (255.255.255.0).

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

3. **Nombre de machines:** Avec un masque de sous-réseau de 255.255.255.0, il est possible de connecter jusqu'à 254 machines au réseau. Cela exclut l'adresse réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255), laissant 254 adresses IP utilisables pour les hôtes.

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

En résumé, le réseau utilise l'adressage IPv4 avec une architecture de sous-réseau de classe C, l'adresse IP du réseau est 192.168.10.0, il peut prendre en charge jusqu'à 254 machines, et l'adresse de diffusion est 192.168.10.255.

JOB 14

145.32.59.24 en binaire : 10010001.00100000.00111011.00011000

200.42.129.16 en binaire : 11001000.00101010.10000001.00010000

14.82.19.54 en binaire : 00001110.01010010.00010011.00110110

JOB 15

1. **Le routage :** Le routage est le processus par lequel les données sont dirigées à travers un réseau informatique d'un point d'origine à une destination. Il consiste à déterminer le chemin optimal pour le transfert des paquets de données d'un réseau à un autre, en utilisant des routeurs qui prennent des décisions basées sur des informations contenues dans les en-têtes de paquets.

2. **Un gateway:** Un gateway, est un dispositif matériel ou logiciel qui relie deux réseaux informatiques différents, permettant ainsi la communication entre eux. Il agit comme une interface de transition entre les réseaux, facilitant le routage des données entre eux.

3. **Un VPN (Virtual Private Network) :** Un VPN est un réseau privé virtuel qui utilise une connexion sécurisée pour permettre à des utilisateurs ou à des réseaux distants de se connecter à un réseau privé, souvent via Internet. Les VPN sont utilisés pour sécuriser les communications en chiffrant les données transitant entre les points d'extrémité, garantissant ainsi la confidentialité et la sécurité des informations échangées.

4. **Un DNS (Domain Name System):** Le DNS est un système de noms de domaine qui traduit les noms de domaine conviviaux pour les humains (comme www.exemple.com) en adresses IP numériques compréhensibles par les ordinateurs. Il sert de répertoire permettant de résoudre les noms de domaine en adresses IP, ce qui facilite la navigation sur Internet et l'accès à des ressources en ligne en utilisant des noms de domaine plutôt que des adresses IP numériques. Le DNS est essentiel pour l'ensemble du fonctionnement d'Internet.