

Job02 :

Qu'est-ce qu'un réseau ?

Un réseau est un ensemble d'éléments interconnectés qui communiquent entre eux pour partager des informations, des ressources ou des services. Ces éléments peuvent être des ordinateurs, des périphériques, des serveurs, des routeurs, des commutateurs, des câbles, des antennes, etc. Les réseaux permettent la transmission de données, de signaux ou de ressources d'un point à un autre, que ce soit localement (dans une même pièce ou un même bâtiment) ou à l'échelle mondiale, via Internet.

À quoi sert un réseau informatique ?

Un réseau informatique sert à accomplir plusieurs objectifs, tels que :

- **Partage de ressources** : Les utilisateurs peuvent partager des fichiers, des imprimantes, des scanners et d'autres périphériques.
- **Communication** : Les réseaux permettent la communication entre les utilisateurs, que ce soit par le biais de courriers électroniques, de messagerie instantanée ou de visioconférences.
- **Accès à Internet** : Un réseau offre une connexion à Internet, permettant l'accès à des informations, des services en ligne et des applications.
- **Sauvegarde et stockage centralisés** : Les données peuvent être stockées et sauvegardées de manière centralisée sur un serveur.
- **Sécurité** : Les réseaux permettent de mettre en place des mesures de sécurité pour protéger les données et les systèmes.

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

- **Ordinateurs** : Les appareils qui se connectent au réseau, tels que les ordinateurs de bureau, les ordinateurs portables, et les serveurs.
- **Routeur** : L'appareil central qui relie le réseau local au reste du monde (comme Internet). Il dirige le trafic.
- **Commutateur (Switch)** : Utilisé pour connecter les ordinateurs au sein du réseau local (LAN) et acheminer les données entre eux.
- **Câbles Ethernet** : Utilisés pour connecter les ordinateurs, le routeur et le commutateur.
- **Cartes réseau** : Installées dans les ordinateurs pour les connecter physiquement au réseau.
- **Point d'accès sans fil (AP)** : Pour permettre aux dispositifs de se connecter au réseau sans fil (Wi-Fi).

Ces composants de base sont essentiels pour un réseau informatique simple. Vous pouvez ensuite ajouter des éléments supplémentaires en fonction de vos besoins spécifiques, comme des imprimantes réseau, des serveurs, des pare-feu, etc.

Job03 :

**Quels câbles avez-vous choisis pour relier les deux ordinateurs ?
Expliquez votre choix.**

Le câble que j'ai choisi est le A.C.C.T (Automatically Choose Connection Type), car il est le plus simple à se connecter pour une personne lambda.

Job04 :

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

- Une adresse IP (Internet Protocol) est une série unique de numéros attribués à chaque appareil connecté à un réseau informatique. Elle permet d'identifier cet appareil sur le réseau et de le localiser.

2. À quoi sert une adresse IP ?

- Les adresses IP servent à deux fonctions principales : l'identification des appareils sur un réseau et le routage des données. Elles permettent aux appareils de communiquer entre eux en envoyant et recevant des données sur le réseau.

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

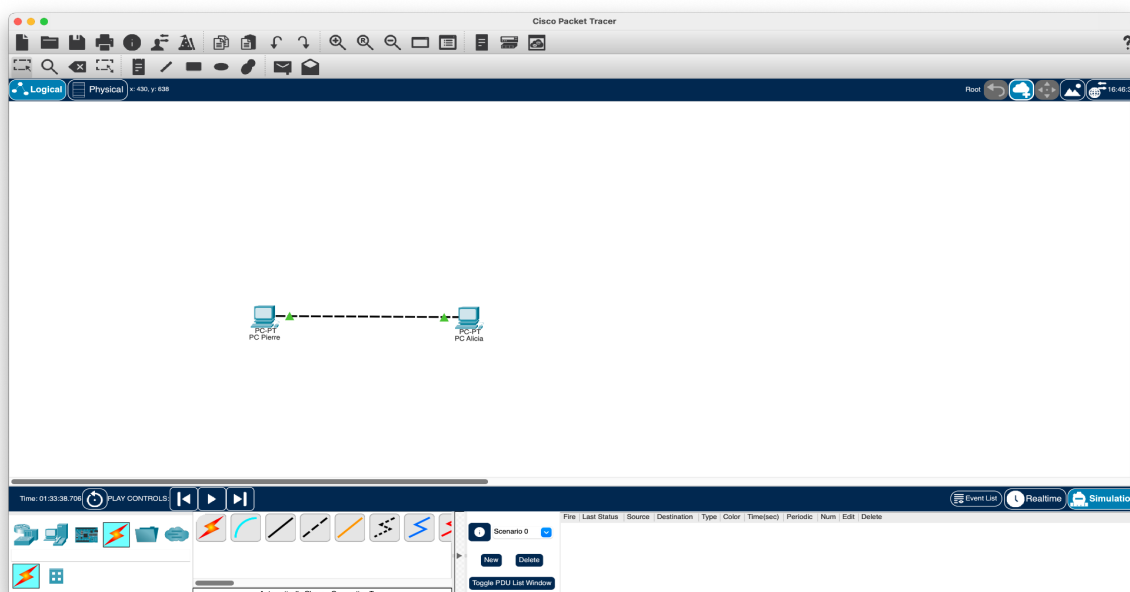
- Une adresse MAC (Media Access Control) est une adresse matérielle unique attribuée à une carte réseau d'un dispositif. Contrairement aux adresses IP, les adresses MAC sont généralement permanentes et servent à identifier de manière unique chaque carte réseau dans le monde. Elles sont utilisées au niveau local pour la communication dans un réseau local (LAN).

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

- Une adresse IP publique est l'adresse attribuée à un dispositif directement connecté à Internet. Elle est visible et identifiable sur Internet. Les adresses IP privées sont utilisées à l'intérieur d'un réseau local pour identifier les appareils au sein de ce réseau. Elles ne sont pas directement visibles sur Internet, car elles sont traduites en une adresse IP publique par le routeur lorsqu'un appareil du réseau local accède à Internet. Les adresses IP privées sont définies par des plages spécifiques (par exemple, 192.168.0.0 à 192.168.255.255).

5. Quelle est l'adresse de ce réseau ?

- Vous n'avez pas spécifié le réseau en question, donc je ne peux pas fournir une adresse IP sans cette information. Chaque réseau a une adresse IP unique ou une plage d'adresses IP qui lui est assignée, en fonction de sa configuration et de sa localisation. Si vous avez une adresse IP spécifique en tête, je peux vous aider à la comprendre, mais j'aurais besoin de plus de détails sur le réseau en question.

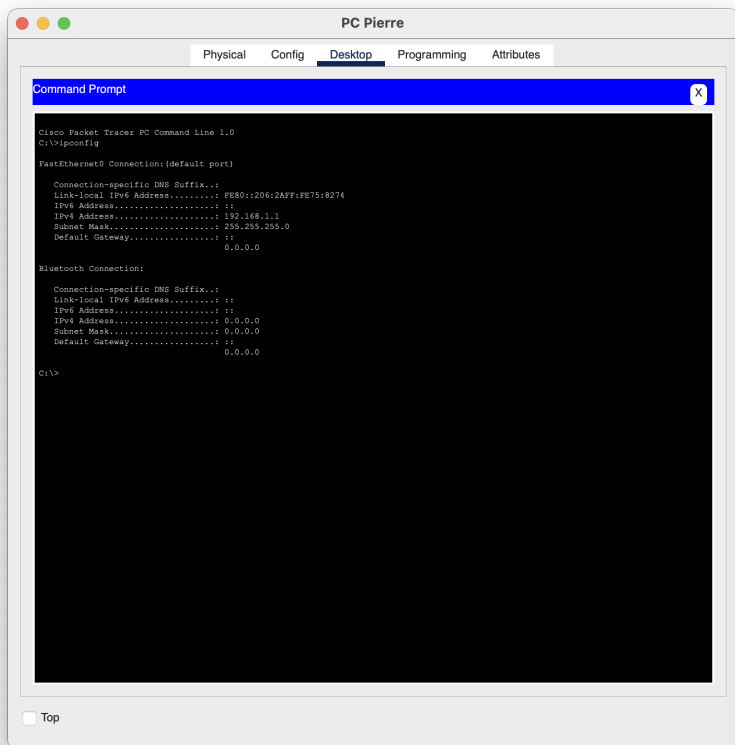


Job05 :

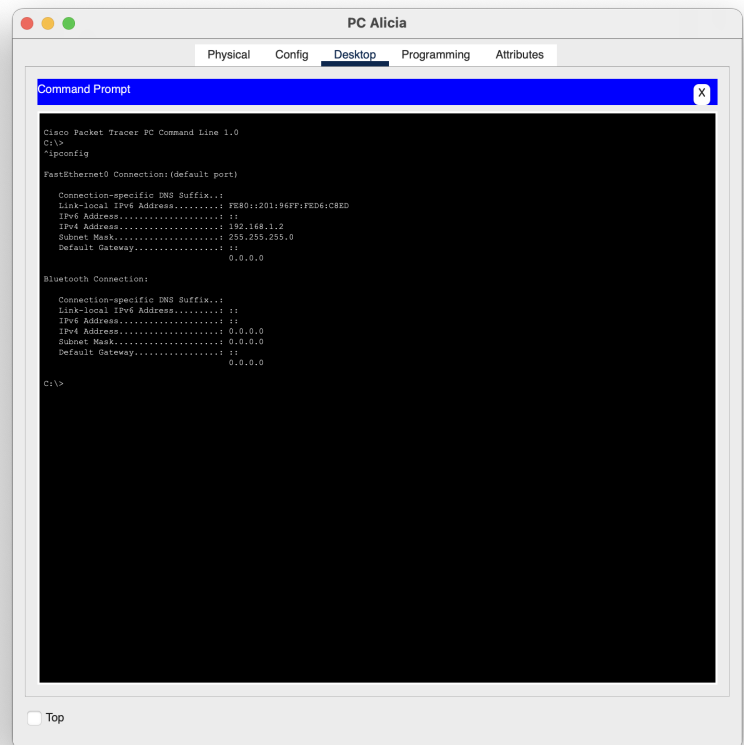
- Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?

La commande est *ipconfig*.

PIERRE



ALICIA

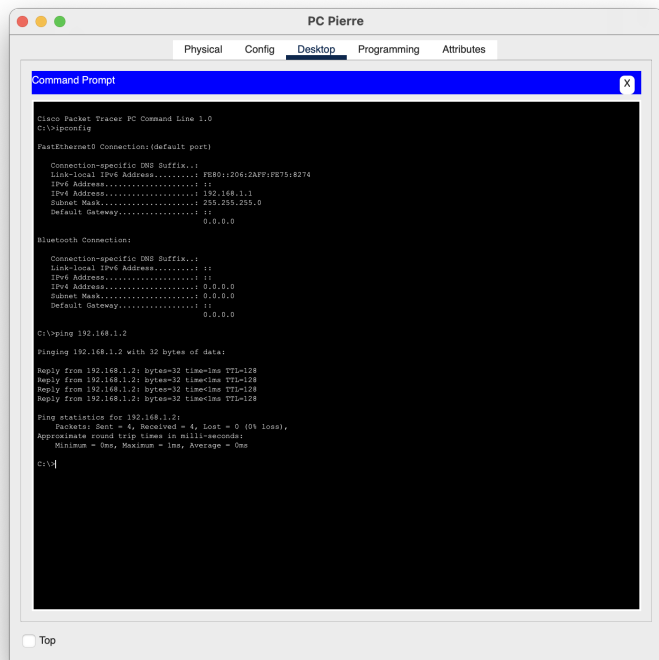


Job06 :

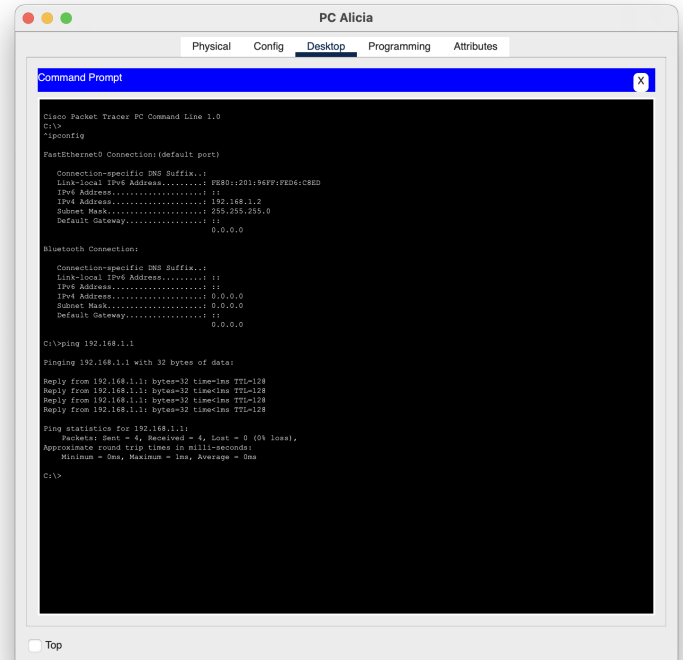
- Quelle est la commande permettant de Ping entre des PC ?

La commande est *ping*.

PIERRE



ALICIA

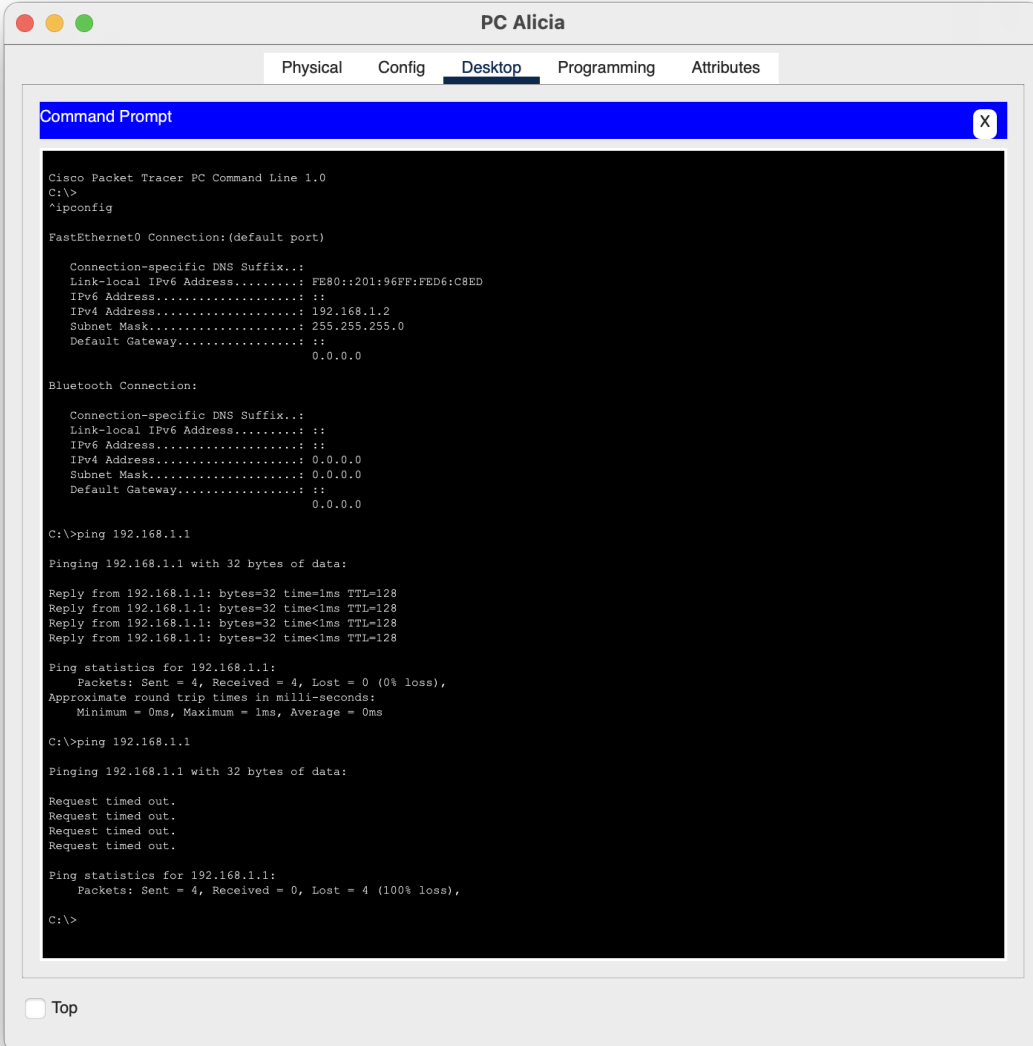


Job07 :

**Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?
Expliquez pourquoi.**

Non, le PC de Pierre n'a probablement pas reçu les paquets envoyés par Alicia, car il était éteint au moment de l'envoi des paquets. Cette absence de réponse est attendue lorsque le PC cible est hors tension.

Il est important de noter que pour que les paquets ICMP soient reçus avec succès, le PC cible doit être en ligne et fonctionnel, prêt à répondre aux requêtes réseau.



The screenshot shows the 'PC Alicia' window with the 'Desktop' tab selected. Inside is a 'Command Prompt' window titled 'Cisco Packet Tracer PC Command Line 1.0'. The user has entered the following commands and received the following output:

```
C:\>
^ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:96FF:FED6:C8ED
    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 . . . . .: 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 = 1ms, Average = 0ms

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:\>
```

At the bottom left of the Command Prompt window, there is a checkbox labeled 'Top' which is currently unchecked.

Job08 :

➤ **Quelle est la différence entre un hub et un switch ?**

- Un hub est un dispositif qui répète tout le trafic sur tous ses ports, manquant d'efficacité et de sécurité. Il est peu utilisé dans les réseaux modernes.

- Un switch est plus avancé, acheminant le trafic uniquement vers le port de destination en fonction des adresses MAC, améliorant l'efficacité et la sécurité. Les switches sont largement utilisés pour améliorer les performances dans les réseaux locaux (LAN).

➤ **Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?**

Fonctionnement d'un hub :

Un hub est un dispositif réseau de couche 1 (couche physique) qui fonctionne de manière très simple. Lorsqu'il reçoit des données sur un port, il les répète simultanément sur tous les autres ports. En d'autres termes, il agit comme un répéteur de signal. Les données envoyées à un port d'un hub sont copiées et diffusées à tous les autres ports du hub, quelle que soit la destination réelle des données.

Avantages d'un hub :

1. Simplicité : Les hubs sont très simples à mettre en place et à utiliser. Ils ne nécessitent aucune configuration complexe.
2. Coût : Les hubs sont généralement moins chers que les commutateurs, ce qui peut en faire une option économique pour de petites installations.

Inconvénients d'un hub :

1. Inefficacité : Les hubs sont inefficaces, car ils répètent tout le trafic à tous les ports, ce qui peut entraîner une congestion du réseau. Tous les appareils connectés voient le trafic de tous les autres appareils, même s'ils ne sont pas la cible du trafic, ce qui entraîne une utilisation inutile de la bande passante.
2. Manque de sécurité : Étant donné que toutes les données sont diffusées à tous les ports, les hubs ne fournissent aucune isolation du trafic. Cela signifie que n'importe quel appareil connecté au hub peut potentiellement intercepter le trafic destiné à un autre appareil, ce qui pose un risque pour la sécurité.
3. Obsolescence : En raison de leur inefficacité et de leur manque de sécurité, les hubs sont devenus obsolètes dans les réseaux modernes. Ils ont été largement remplacés par des commutateurs qui offrent des performances et une sécurité supérieures.

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

Avantages d'un switch :

- **Efficacité** : Les switches acheminent le trafic uniquement vers le port de destination, améliorant l'efficacité et l'utilisation de la bande passante.
- **Isolation du trafic** : Le trafic entre les ports est isolé, améliorant la sécurité et la confidentialité des données.
- **Performance** : Les switches offrent des performances élevées pour des réseaux rapides et fiables.
- **Sécurité** : Ils renforcent la sécurité en empêchant la surveillance non autorisée du trafic.
- **Évolutivité** : Les switches permettent la création de réseaux plus vastes en interconnectant plusieurs d'entre eux.

Inconvénients d'un switch :

- **Coût** : Les switches sont généralement plus chers que les hubs.
- **Complexité de configuration** : Ils peuvent nécessiter une configuration plus avancée.
- **Maintenance** : Les switches demandent une gestion et une maintenance plus attentives.
- **Surchargé** : Dans des réseaux très chargés, les switches peuvent devenir surchargés, entraînant des latences.

En somme, les switches offrent une meilleure efficacité, sécurité et performance que les hubs, mais ils peuvent être plus coûteux et nécessiter une configuration et une maintenance plus avancées. Le choix dépend des besoins spécifiques de votre réseau et de votre budget, bien que les switches soient souvent préférés dans les réseaux modernes pour leurs avantages significatifs.

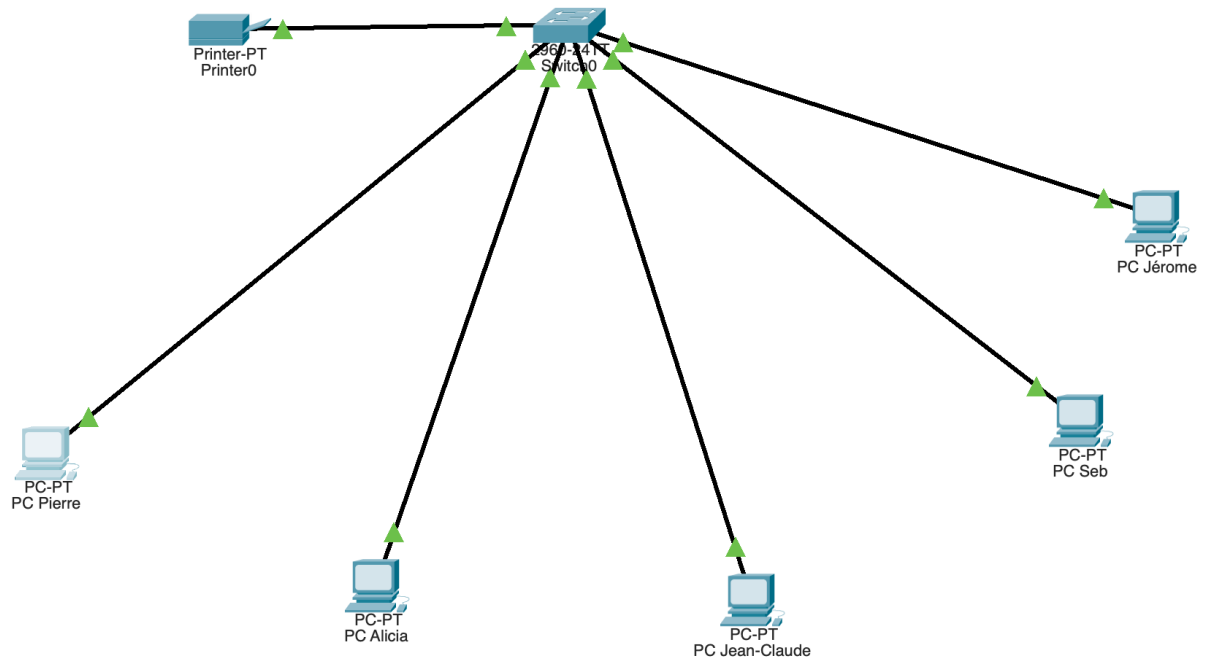
➤ Comment un switch gère-t-il le trafic réseau ?

1. **Apprentissage des adresses MAC** : Le switch crée une table de correspondance (table MAC) en enregistrant les adresses MAC des appareils connectés à ses ports.
2. **Réception des trames** : Lorsqu'une trame Ethernet est reçue, le switch examine l'adresse MAC de destination dans l'en-tête de la trame.
3. **Consultation de la table MAC** : Le switch vérifie si l'adresse MAC de destination est répertoriée dans sa table MAC pour déterminer le port de destination.
4. **Acheminement de la trame** : Si l'adresse MAC de destination est trouvée, le switch envoie la trame uniquement vers le port correspondant à cet appareil. Sinon, il diffuse la trame sur tous les ports, sauf celui sur lequel la trame a été reçue.
5. **Mise à jour de la table MAC** : Le switch met à jour sa table MAC en enregistrant les adresses MAC source des trames et en associant ces adresses aux ports correspondants.
6. **Expiration des entrées** : Les entrées obsolètes dans la table MAC sont supprimées après un certain temps.

En utilisant ces informations, le switch isole le trafic, améliore l'efficacité et renforce la sécurité dans un réseau local (LAN).

Job09 :

Schéma du réseau :



1. **Visualisation de la topologie :** Un schéma de réseau vous permet de visualiser clairement la topologie de votre réseau, c'est-à-dire comment les appareils, les commutateurs, les routeurs, les serveurs, etc., sont connectés les uns aux autres. Cela facilite la compréhension de la structure de votre réseau.
2. **Dépannage facilité :** En cas de problème ou de panne sur le réseau, un schéma bien documenté peut être un outil précieux pour le dépannage. Vous pouvez rapidement identifier les connexions, les composants ou les chemins potentiellement problématiques.
3. **Planification et amélioration du réseau :** Un schéma de réseau vous permet de planifier des améliorations ou des mises à niveau en identifiant les zones de congestion, les points faibles et les opportunités d'optimisation. Cela vous aide à prendre des décisions éclairées pour améliorer les performances et la sécurité du réseau.

Job10 :

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

Adresse IP Statique :

- Configurée manuellement par l'administrateur.
- Reste constante tant que l'administrateur ne la modifie pas.
- Stable et prévisible.
- Configuration individuelle de chaque appareil.
- Adaptée aux serveurs et appareils nécessitant des adresses IP permanentes.

Adresse IP attribuée par DHCP :

- Attribuée automatiquement par un serveur DHCP au moment de la connexion.
- Peut changer à chaque connexion ou après expiration du bail.
- Configuration automatique des paramètres réseau.
- Gestion centralisée via un serveur DHCP.
- Adaptée aux réseaux dynamiques avec des appareils se connectant et se déconnectant fréquemment.

Job11 :

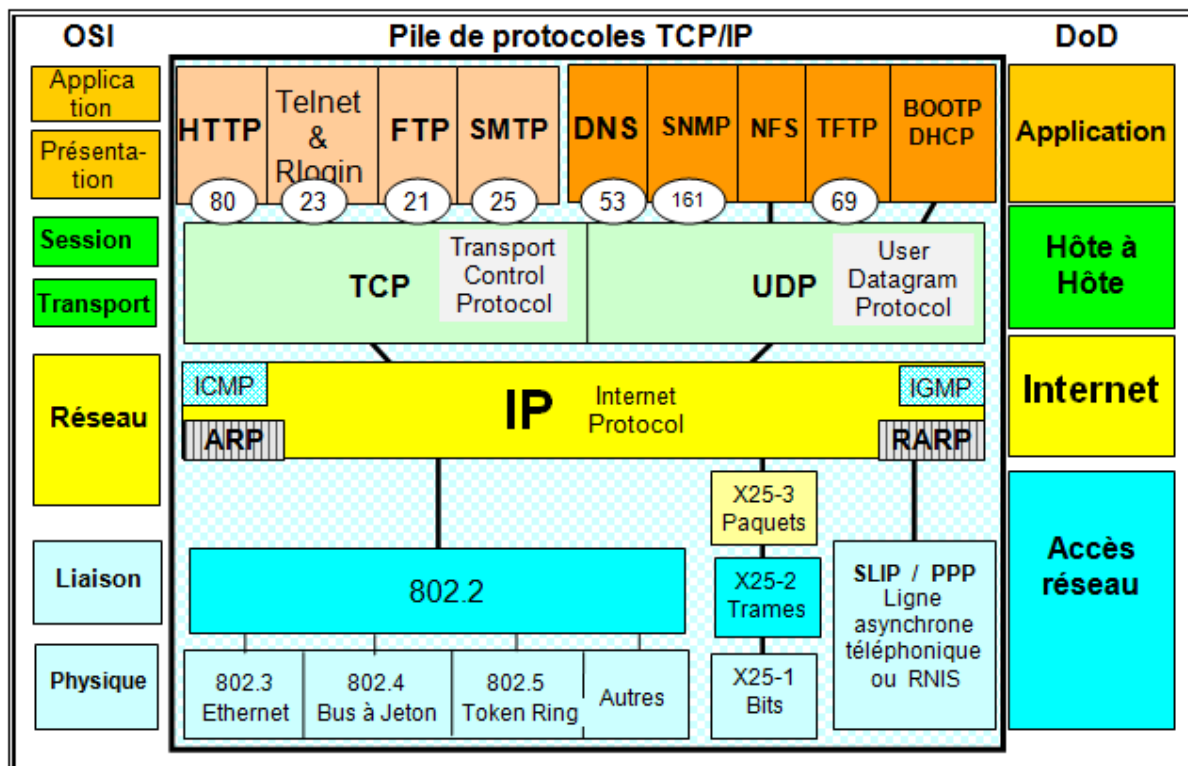
- **Pourquoi a-t-on choisi une adresse de classe A (10.0.0.0) ?**

L'adresse de classe A a une grande plage d'adresses disponibles, ce qui est nécessaire pour créer de nombreux sous-réseaux. Dans ce cas, une adresse de classe A est suffisante pour répondre à vos besoins en termes de sous-réseaux et d'hôtes.

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

Les classes d'adresses (A, B, C, D, E) déterminent la plage d'adresses disponibles dans un réseau. Les adresses de classe A ont un préfixe de réseau de 8 bits, ce qui signifie qu'elles peuvent être utilisées pour un grand nombre de sous-réseaux avec un grand nombre d'hôtes. Les autres classes ont des préfixes de réseau de différentes tailles, ce qui limite le nombre d'adresses de réseau et d'hôtes possibles. Les sous-réseaux sont créés en empruntant des bits d'adresse d'hôte pour les répartir en sous-réseaux plus petits. La taille des sous-réseaux et le nombre d'hôtes possibles varient en fonction de la classe de l'adresse et du nombre de bits empruntés pour l'adressage du sous-réseau.

Job12 :



Description des sept couches du modèle OSI et comment elles se rapportent aux composants et protocoles mentionnés :

1. Couche 7 (Application) : Cette couche est la plus proche de l'utilisateur. Elle fournit des interfaces pour les applications utilisateur et les services de communication. Les composants associés à cette couche sont ceux qui interagissent directement avec l'utilisateur, tels qu'HTML (pour les pages web), FTP (pour le transfert de fichiers) et PPTP (pour les tunnels VPN).

2. Couche 6 (Présentation) : La couche de présentation gère la traduction, la compression et le chiffrement des données. SSL/TLS est un protocole couramment utilisé pour le chiffrement des données dans cette couche.

3. Couche 5 (Session) : Cette couche est responsable de l'établissement, de la gestion et de la fin des sessions de communication entre les applications. Elle ne dispose pas de composants spécifiques mentionnés dans votre liste.

4. Couche 4 (Transport) : La couche de transport assure le contrôle de bout en bout de la communication. Elle garantit que les données sont correctement livrées et peut retransmettre les données en cas de perte. TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) sont les protocoles couramment utilisés à cette couche.

5. Couche 3 (Réseau) : La couche réseau gère le routage des données entre différents réseaux et sous-réseaux. Elle effectue la résolution des adresses IP en adresses MAC pour le transfert de données. Les protocoles IPv4 et IPv6, ainsi que les routeurs, sont associés à cette couche.

6. Couche 2 (Liaison de données) : Cette couche assure la liaison de données au sein d'un réseau local. Elle gère les adresses MAC et la détection d'erreurs. Les composants associés comprennent Ethernet, les cartes réseau (NIC), les commutateurs, le Wi-Fi, les câbles RJ45 et la fibre optique.

7. Couche 1 (Physique) : La couche physique gère les aspects matériels de la communication, tels que les signaux électriques, les câbles et les supports physiques. Les composants associés sont les câbles (comme le RJ45 et la fibre optique) et les équipements matériels.

Chaque couche joue un rôle spécifique dans le processus de communication, allant des aspects les plus proches de l'utilisateur aux aspects physiques du réseau. Les protocoles et composants sont utilisés à différentes couches pour assurer une communication efficace.

Job13 :

1. Architecture du réseau : Le réseau est configuré en utilisant une adresse IP de la classe C (192.168.10.X) avec un masque de sous-réseau de 255.255.255.0, ce qui signifie que le réseau est un réseau de classe C.

2. Adresse IP du réseau : L'adresse IP du réseau est la première adresse de la plage d'adresses IP, c'est-à-dire 192.168.10.0.

3. Nombre de machines sur le réseau : Avec un masque de sous-réseau de 255.255.255.0 (ou /24 en notation CIDR), vous avez 8 bits pour les adresses d'hôtes. Cela signifie qu'il y a $2^8 - 2$ adresses IP disponibles pour les machines, car 2 adresses sont réservées (l'adresse réseau et l'adresse de diffusion). Donc, le nombre de machines possibles est $2^8 - 2 = 256 - 2 = 254$.

4. Adresse de diffusion du réseau : L'adresse de diffusion pour ce réseau est la dernière adresse de la plage d'adresses IP, c'est-à-dire 192.168.10.255.

Donc, pour résumer :

- Architecture du réseau : Classe C (192.168.10.X)
- Adresse IP du réseau : 192.168.10.0
- Nombre de machines possibles : 254
- Adresse de diffusion : 192.168.10.255

Le réseau est capable de prendre en charge jusqu'à 254 machines, et l'adresse de diffusion permet de diffuser des données à toutes les machines du réseau.

Job14 :

Voici les adresses IP que vous avez fournies en binaire :

➤ **1. 145.32.59.24 en binaire :**

- 145 s'écrit en binaire : 10010001
- 32 s'écrit en binaire : 00100000
- 59 s'écrit en binaire : 00111011
- 24 s'écrit en binaire : 00011000

L'adresse IP 145.32.59.24 en binaire est donc : 10010001.00100000.00111011.00011000

➤ **2. 200.42.129.16 en binaire :**

- 200 s'écrit en binaire : 11001000
- 42 s'écrit en binaire : 00101010
- 129 s'écrit en binaire : 10000001
- 16 s'écrit en binaire : 00010000

L'adresse IP 200.42.129.16 en binaire est donc : 11001000.00101010.10000001.00010000

➤ **3. 14.82.19.54 en binaire :**

- 14 s'écrit en binaire : 00001110
- 82 s'écrit en binaire : 01010010
- 19 s'écrit en binaire : 00010011
- 54 s'écrit en binaire : 00110110

L'adresse IP 14.82.19.54 en binaire est donc : 00001110.01010010.00010011.00110110

Job15 :

Bien sûr, je vais répondre attentivement à ces questions :

1. Qu'est-ce que le routage ? : Le routage est le processus de détermination du chemin optimal pour acheminer des données d'un point à un autre au sein d'un réseau ou entre différents réseaux. Les routeurs sont les dispositifs principaux qui prennent en charge cette fonction. Ils examinent les adresses de destination des paquets de données et décident de la meilleure manière de les transmettre vers leur destination en fonction de la topologie du réseau et des règles de routage configurées.

2. Qu'est-ce qu'un gateway (passerelle) ? : Une passerelle (gateway) est un dispositif ou un logiciel qui relie deux réseaux distincts, permettant la communication entre eux. Elle agit comme une interface d'interconnexion entre des réseaux ayant des protocoles ou des architectures différents. Par exemple, une passerelle peut relier un réseau local (LAN) à Internet ou un réseau local à un réseau privé virtuel (VPN).

3. Qu'est-ce qu'un VPN (Virtual Private Network) ? : Un VPN (Virtual Private Network) est une technologie qui permet de créer un réseau privé virtuel sécurisé au-dessus d'un réseau public, tel qu'Internet. Il permet aux utilisateurs de transmettre des données de manière cryptée, ce qui renforce la sécurité et la confidentialité des communications. Les VPN sont couramment utilisés pour établir des connexions sécurisées à distance, pour accéder à des ressources réseau privées, ou pour contourner les restrictions géographiques sur Internet.

4. Qu'est-ce qu'un DNS (Domain Name System) ? : Le DNS (Domain Name System) est un système qui permet de traduire les noms de domaine (par exemple, www.exemple.com) en adresses IP compréhensibles par les ordinateurs. Il s'agit d'un élément clé d'Internet, car il simplifie la manière dont les utilisateurs accèdent aux sites web. Le DNS fonctionne en associant des noms de domaine à des adresses IP, ce qui facilite la navigation sur Internet en remplaçant des adresses IP numériques par des noms de domaine conviviaux.