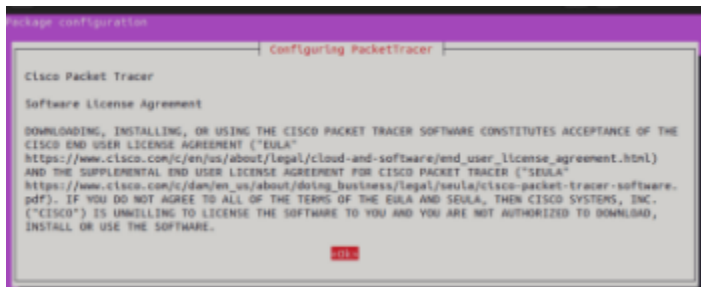


InRuntrack Réseau

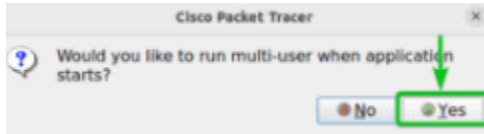
Commande pour installer Cisco Packet Tracer.

- sudo Apt update
- cd ~/Downloads
- ls -lh
- sudo apt install ./Packet_Tracer821_amd64_signed (1)
- sudo apt install -f ou sudo apt install --fix-broken
- sudo apt install ./Descargas/PacketTracer_
- Pour confirmer l' installation, appuyer sur Y et puis <Enter>.
- Une fois que vous voyez l'invite suivante, sélectionnez <OK> et appuyez sur <Entrée>



Pour accepter le CLUF/licence Packet Tracer, appuyer sur tab puis sélectionnez <Oui> et appuyez sur <Entrée>.





Exécution de Cisco Packet Tracer sur Ubuntu pour la première fois

Une fois Cisco Packet Tracer installé, vous pouvez le trouver dans le « Menu Application » d'Ubuntu 22.04 LTS.

Job 2/

→ Qu'est-ce qu'un réseau ?

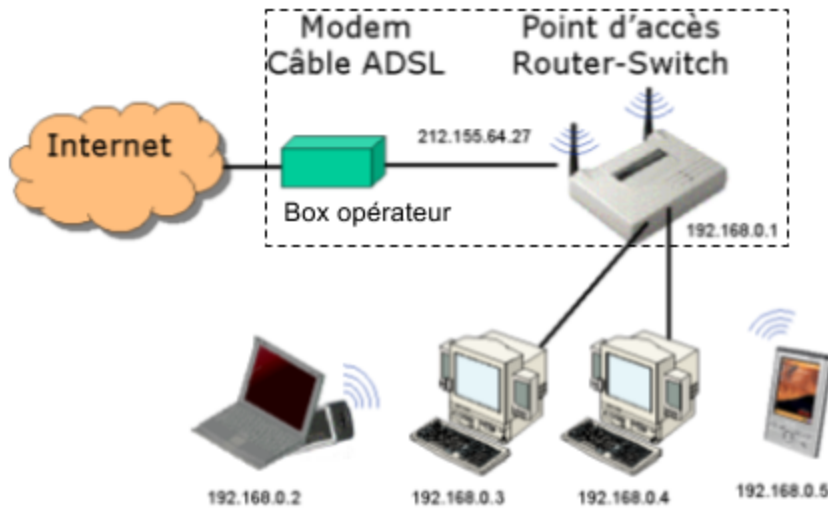
Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux.

→ À quoi sert un réseau informatique ?

Un **réseau informatique** sert à réseau informatique est la mise en relation de tous les postes ordinateurs d'une même société par le biais d'un serveur commun.

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

Pour créer un réseau, il faut un Switch qui permet de relier les machines entre elles. Pour relier les machines au Switch, il faut des câbles RJ45 ou des liaisons sans-fil. Pour relier votre réseau à Internet, il faut un routeur.



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.

J'ai choisi un câble croisé car il permet de connecter deux dispositifs du même type pour communiquer ensemble, comme un ordinateur à un autre ordinateur, ou un commutateur à un autre commutateur. Le câble de raccordement connecte deux dispositifs différents l'un à

l'autre, comme un ordinateur et un commutateur. Le câble peut aussi être choisi automatiquement en cliquant sur **Automatically Choose connection type**.

Job 4/

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP est votre numéro d'identification qui a été attribué à votre ordinateur connecté à un réseau Internet.

→ À quoi sert un IP ?

Il sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet. permet d'identifier chaque hôte connecté à un réseau informatique utilisant le protocole IP. Actuellement, elle est utilisée dans sa version 4, une version dans laquelle l'adresse IP est composée de **4 nombres** (4 octets) allant de **0 à 255**, séparés par des points. De ce fait, l'adresse IP la plus basse est **0.0.0.0** et la plus haute **255.255.255.255**, chacun de ces nombres correspond à un octet.

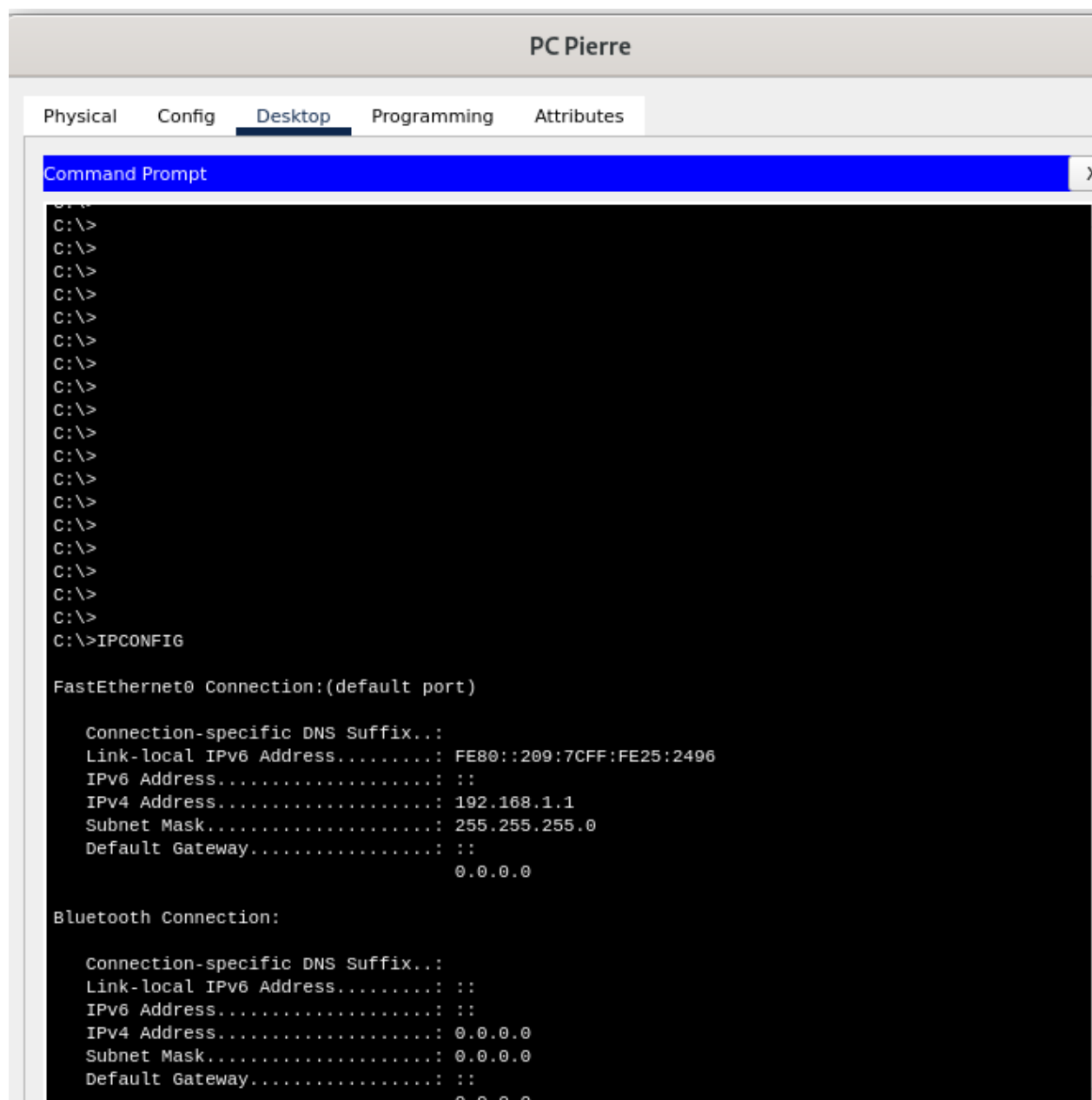
→ Qu'est-ce qu'une adresse MAC ?

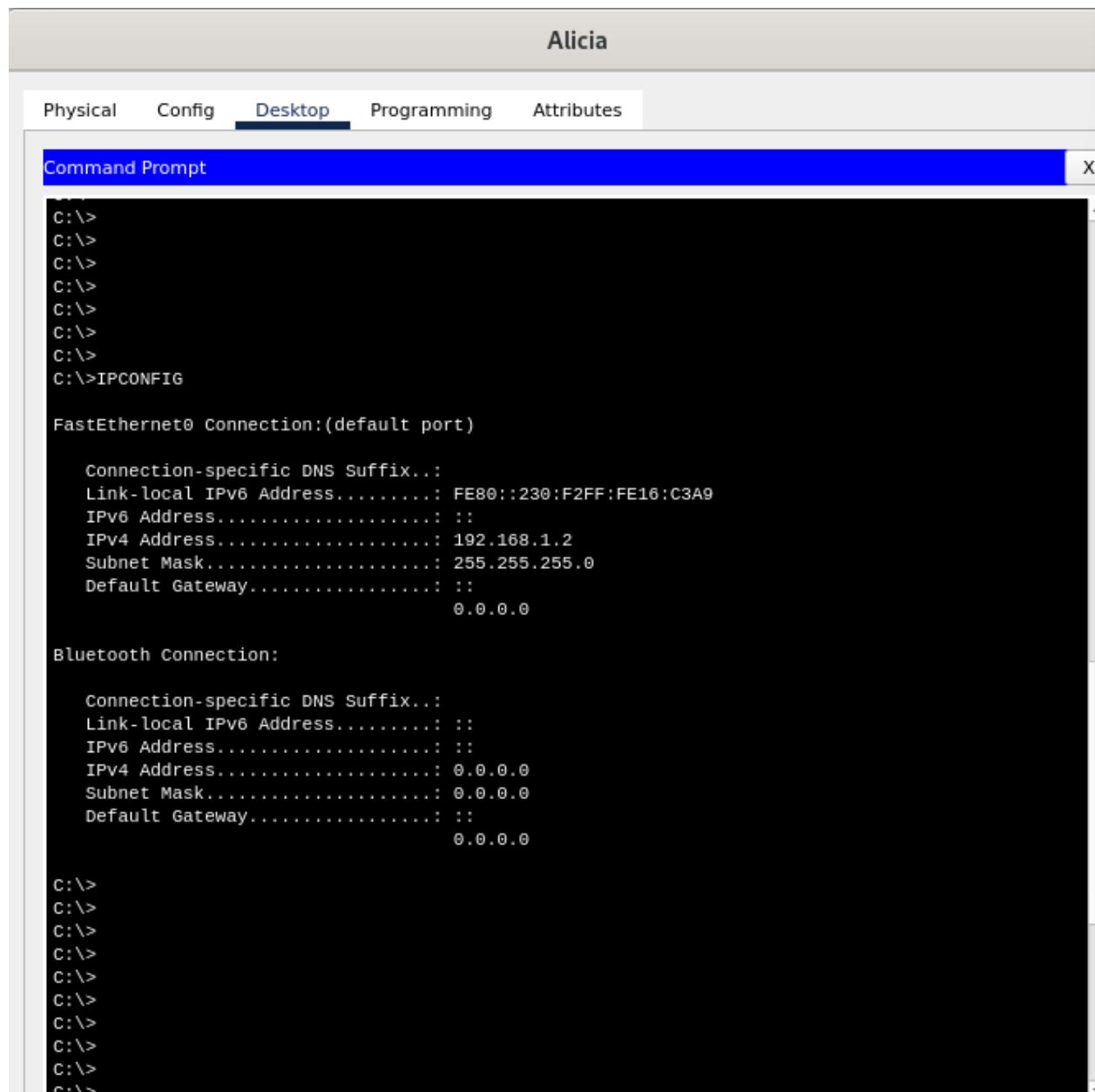
Une adresse MAC correspond à l'adresse physique d'un équipement réseau. Cette adresse est un identifiant, normalement unique, permettant d'identifier un équipement réseau par rapport à un autre.

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

Les adresses IP privées représentent toutes les adresses IP de classe A, B et C que l'on peut utiliser dans un réseau local (LAN) c'est-à-dire dans le réseau de votre entreprise ou dans le réseau domestique. De plus, les adresses IP privées ne peuvent pas être

192.168.1.2 et 192.168.1.1



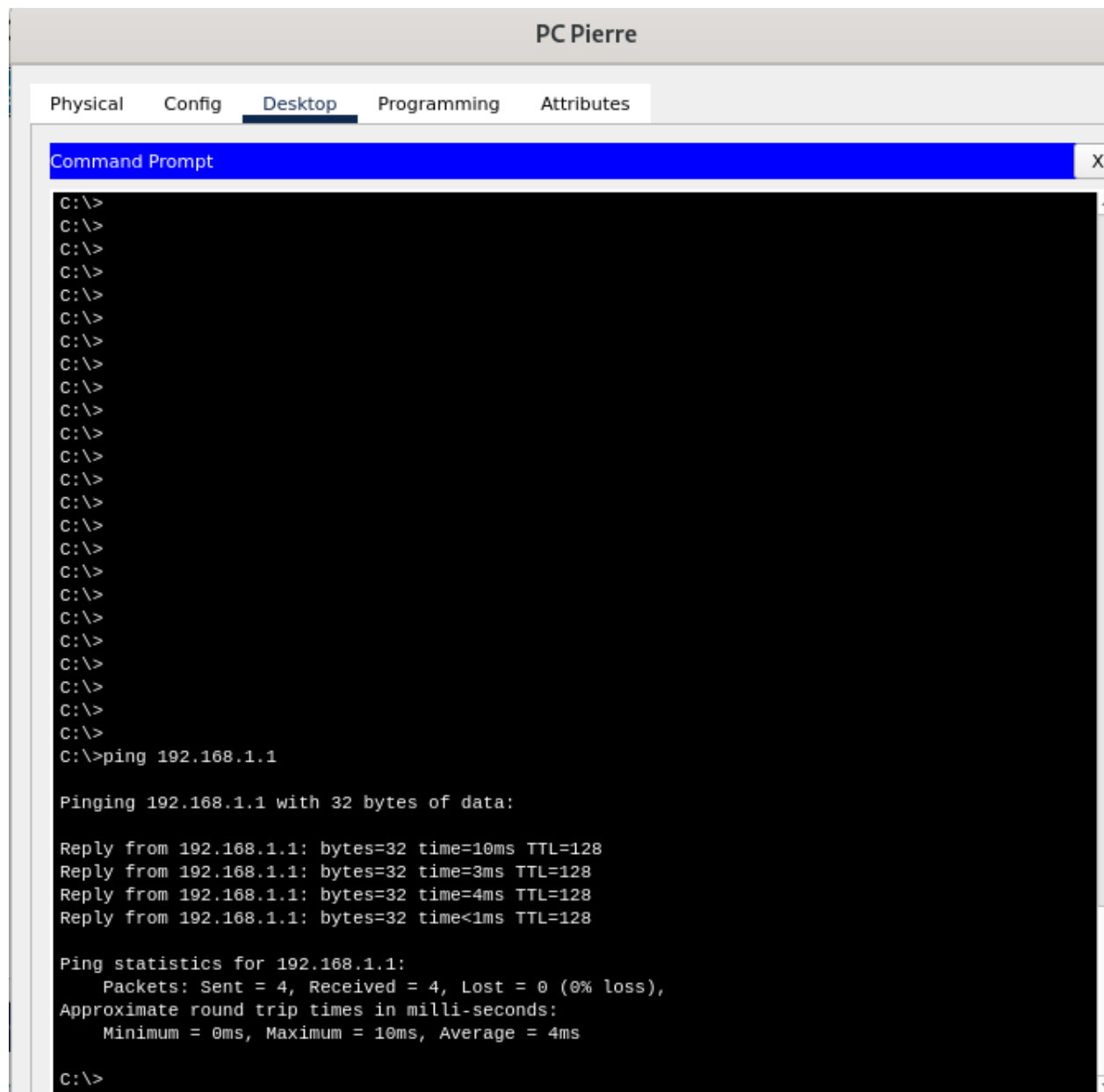


Job 5/

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

J'ai utilisé la commande ?

J'ai utilisé ping.



The screenshot shows a window titled "PC Pierre" with a tabbed interface. The "Desktop" tab is selected, displaying a "Command Prompt" window. The command prompt shows a series of "C:\>" prompts, followed by the command "C:\>ping 192.168.1.1". The output of the command is as follows:

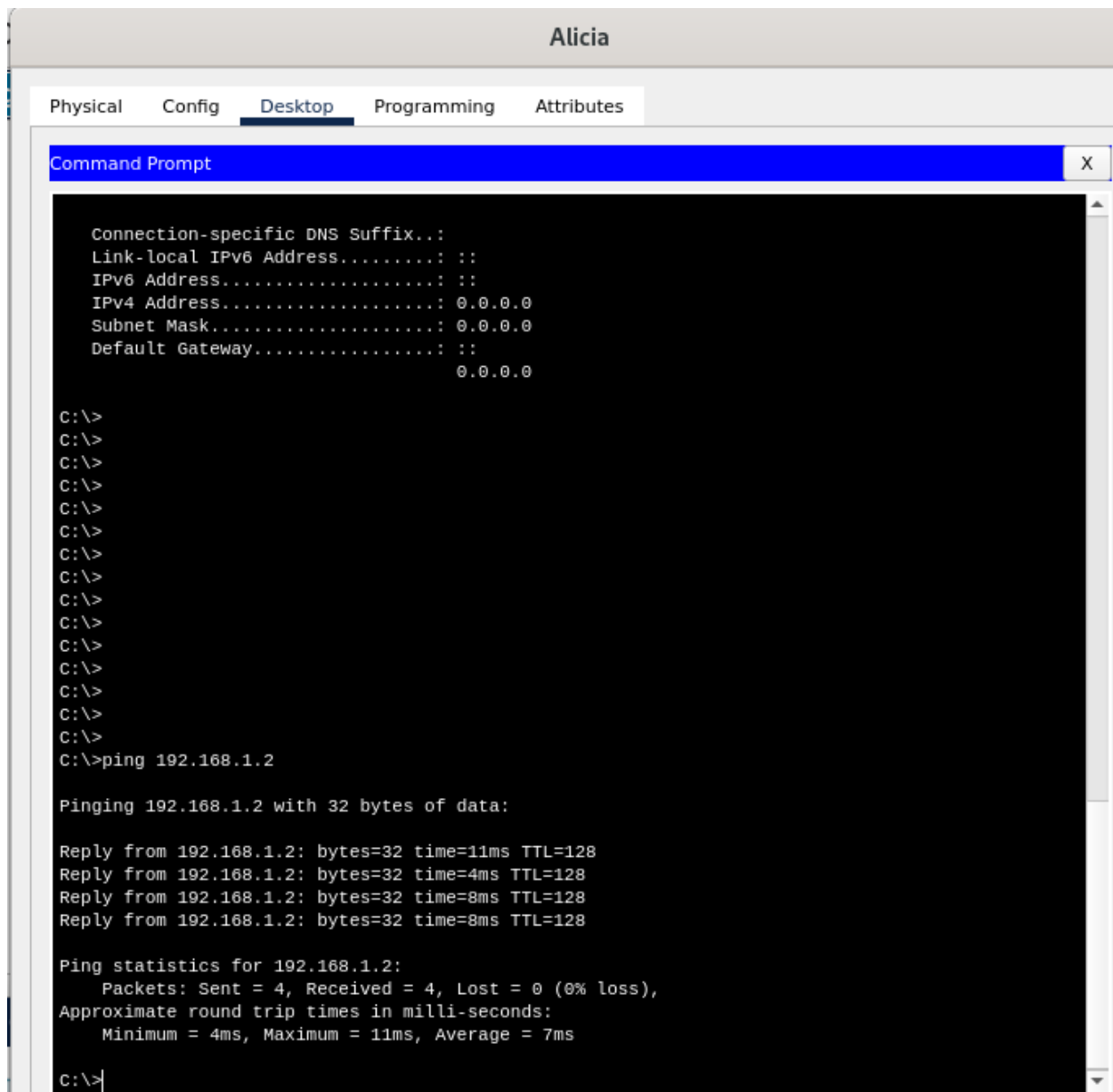
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

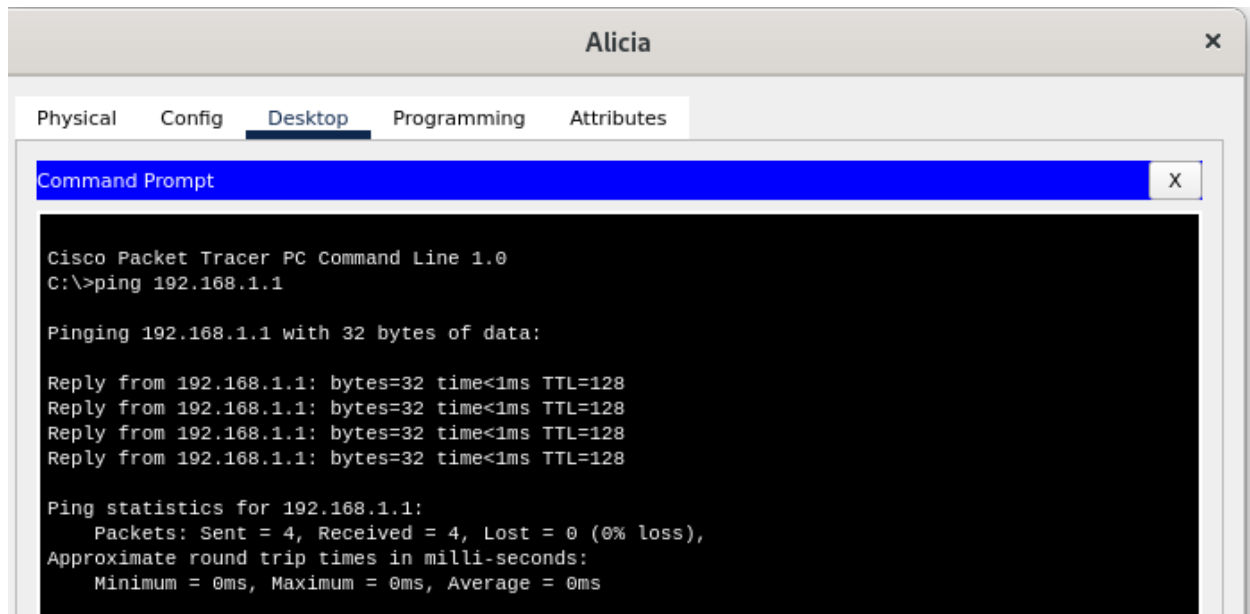
Reply from 192.168.1.1: bytes=32 time=10ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

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 = 10ms, Average = 4ms

C:\>
```



Job 6/



Pierre

```
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

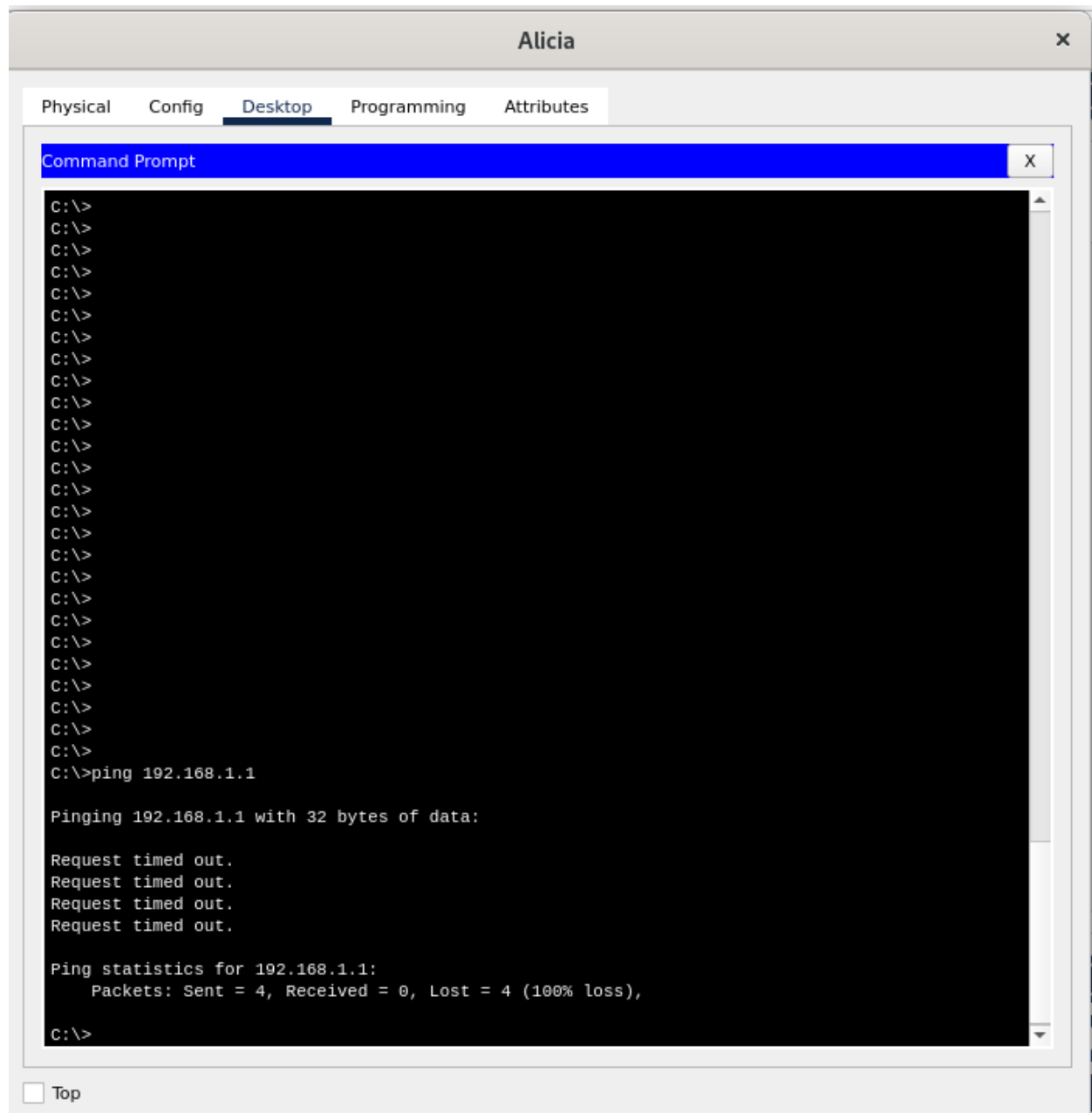
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Quelle est la commande permettant de Ping entre des PC ?

Ping et l'adresse ip de l'autre pc et inversement.

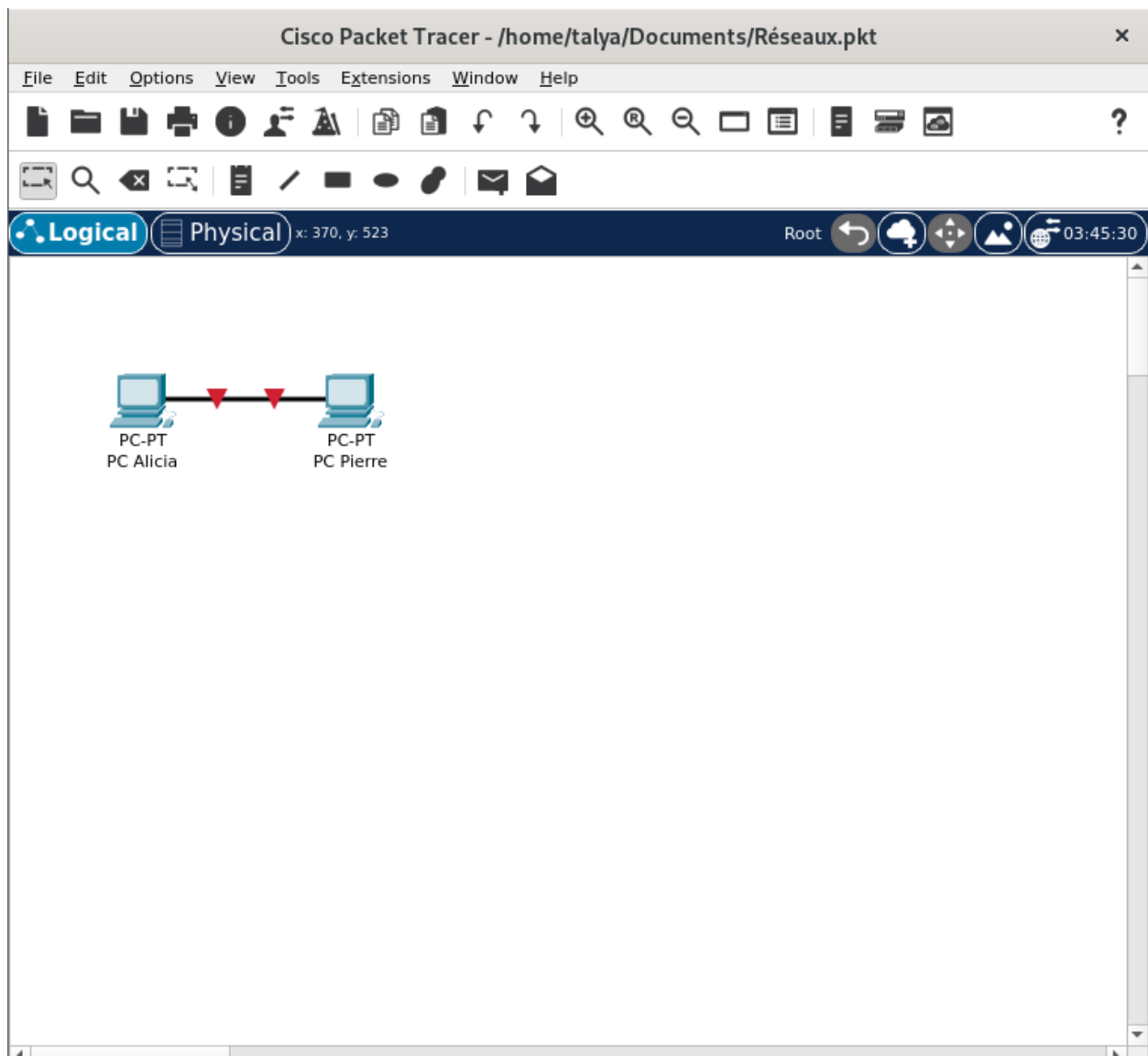
Job 7/



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

→ Expliquez pourquoi.

Le pc de pierre n'a pas reçu les paquets envoyés par Alicia car son pc était éteint. Le triangle aurait été vert si la connexion était établie.



Job 8/

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

Un Hub est un périphérique qui connecte plusieurs périphériques Ethernet sur un même réseau et les faire fonctionner ensemble en un seul réseau. Un Hub ne collecte pas d'informations. Tandis qu'un switch est un périphérique réseau qui effectue le même travail que le Hub mais qui est considéré comme un Hub plus intelligent car il collecte des informations sur les paquets de données qu'il reçoit et les transmet au seul réseau auquel il était destiné

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

Lorsqu'un hub reçoit des données, il transfère l'intégralité de celles-ci à tous les appareils connectés (ou hôtes) sur le mode du semi-duplex. **L'inconvénient c'est que tous les raccordements (ou ports) d'un hub fonctionnent à la même vitesse et se trouvent dans un même domaine de collision (regroupant tous les appareils connectés en réseau).** d'autres périphériques réseau, un hub ne permet pas de cibler ou d'exclure uniquement certains de ces récepteurs. En cas de transfert, tous les paquets sont invariablement transmis à l'ensemble des ordinateurs. Tous les appareils reçoivent donc le paquet de données en question, même si celui-ci ne leur est pas initialement destiné. Étant donné que tous les hôtes sont occupés par ce transfert, aucun autre appareil ne peut envoyer de données tant que ce processus est en cours. Les demandes simultanées sont donc traitées les unes après les autres. La technologie qui se cache derrière les hubs est donc considérée comme étant vulnérable et obsolète.

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

Le switch présente plusieurs avantages dans la gestion de votre parc informatique. Il contribue à la sécurité du réseau et à la protection des données échangées via le réseau. Il permet de connecter davantage de postes de travail sur le même réseau Ethernet. Le switch permet avant tout de répartir l'information de manière « intelligente » . Il contrôle la sécurité au maximum votre réseau pour éviter les intrusions. **L'inconvénient les boucles dans une topologie avec des switchs redondant, cela provoquerait :**

- **Des Tempêtes de broadcast** car Chaque boucle provoque des émissions de trames sans fin, ce qui ralentit fortement les performances du réseau.
- **Ça provoquerait aussi des Transmissions de paquets identiques** qui peuvent être livrées à la destination, alors qu'il en attend qu'une seul, cela provoque de nombreuses erreurs et donc des retransmissions...

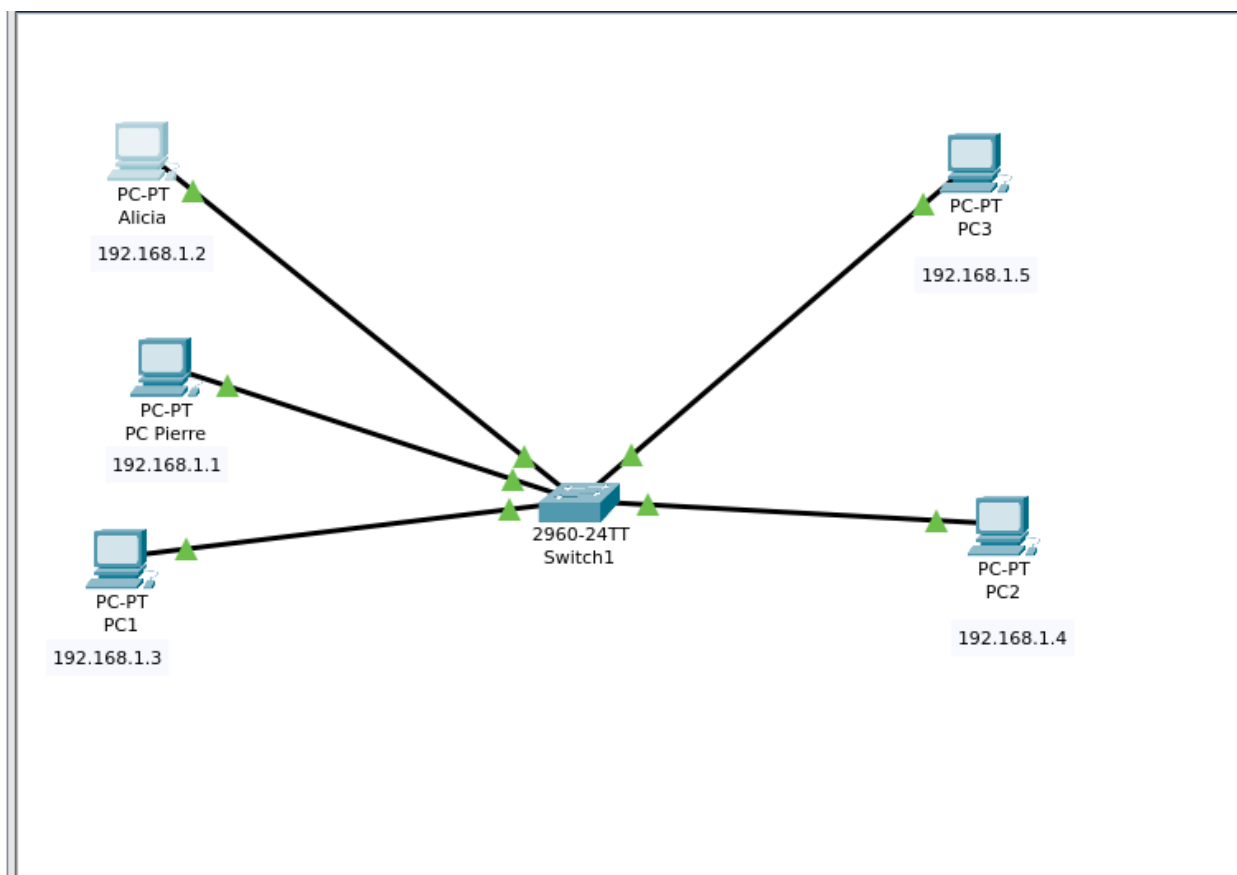
→ Comment un switch gère-t-il le trafic réseau ?

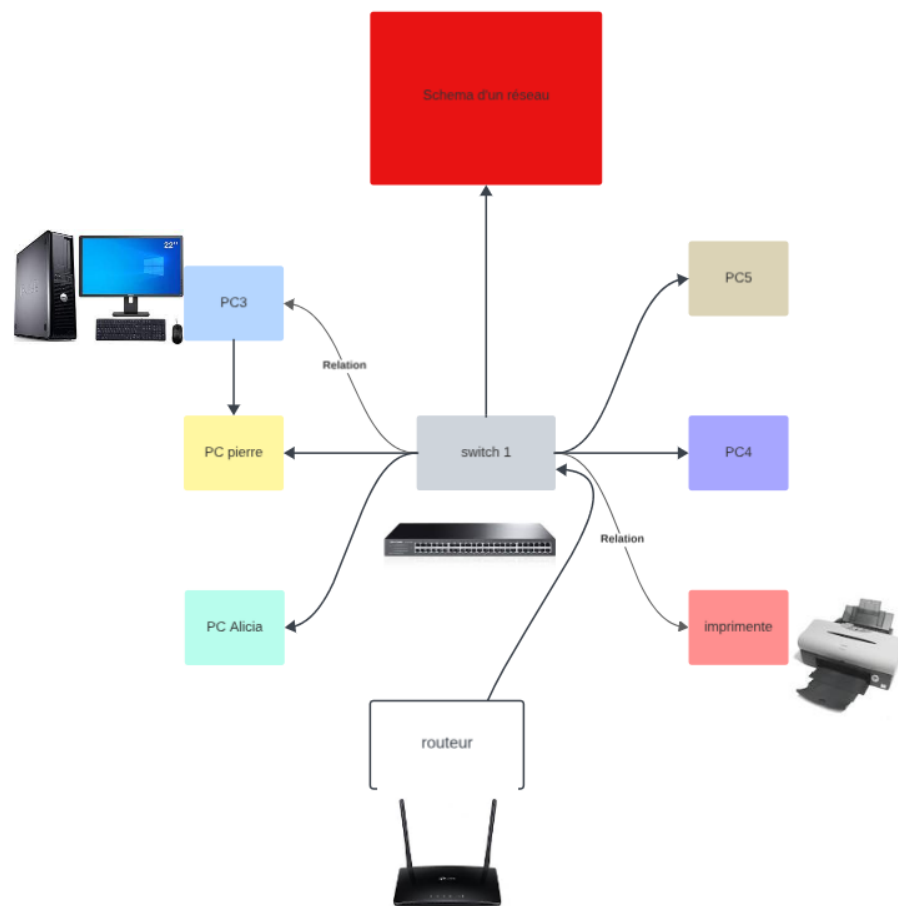
Un switch gère le trafic réseau en utilisant une fonctionne intelligemment avec les adresses MAC pour s'assurer que le trafic qui est envoyé entre les appareils aboutit au bon endroit. Pour ce faire, il surveille en permanence le trafic qui entre dans le commutateur à partir des appareils connectés.

Il apprend ensuite où les différentes adresses MAC de ces appareils sont connectées.

Pour ce faire, il examine le trafic qui arrive des ordinateurs pour lire l'adresse MAC source du trafic. Ainsi lorsqu'un paquet est envoyé d'un équipement à l'autre.

Un switch réseau sait sur quel port physique envoyer la trame.



Job 9/

J'ai choisi un switch ainsi que 5 pc avec une imprimante qui se connecte aussi au commutateur et un routeur.

10/

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

Les adresses IP statiques permettent aux dispositifs de réseau de conserver la même adresse IP en permanence. Un administrateur de réseau doit garder une trace de chaque dispositif attribué statiquement pour éviter de réutiliser la même adresse IP. Comme l'adresse IP statique requiert des configurations manuelles, elle peut créer des problèmes de réseau en cas d'utilisation sans une bonne maîtrise du protocole TCP/IP.

DHCP est un protocole permettant d'automatiser la tâche d'attribution des adresses IP. Le DHCP est avantageux pour les administrateurs de réseau car il supprime la tâche répétitive consistant à attribuer plusieurs adresses IP à chaque appareil du réseau. Cela peut ne prendre qu'une minute, mais lorsque vous configurez des centaines de périphériques réseau, cela peut devenir très fatigant. Les points d'accès sans fil utilisent également le DHCP afin que les administrateurs n'aient pas besoin de configurer eux-mêmes leurs appareils.

11/

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

L'adresse 10.0.0.0 a été choisie car elle appartient à la plage d'adresses réservée pour les réseaux privés de classe A. Les adresses de classe A sont généralement utilisées pour les grandes organisations qui nécessitent un grand nombre d'adresses IP. Elles

offrent une vaste plage d'adresses, ce qui permet de créer de nombreux sous-réseaux et d'héberger un grand nombre d'hôtes.

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

Il existe différents types d'adresses IP, tels que les adresses de classe A, B, C, D et E. Chaque classe a une plage d'adresses et une structure spécifique. Les adresses de classe A sont utilisées pour les réseaux très vastes, car elles permettent d'avoir un grand nombre d'adresses IP disponibles, les adresses de classe B sont utilisées pour les réseaux de taille moyenne, les adresses de classe C sont utilisées pour les réseaux plus petits, car elles offrent moins d'adresses disponibles que les classes A et B, les adresses de classe D sont réservées pour le multicasting, c'est-à-dire l'envoi de données à un groupe d'ordinateurs spécifique, Les adresses de classe E sont réservées à des fins expérimentales et ne sont pas utilisées pour les réseaux publics.

2. Cinq sous-réseaux de 30 hôtes :

- Adresse réseau : 10.0.0.16/27, 10.0.0.32/27, 10.0.0.48/27, 10.0.0.64/27, 10.0.0.80/27
- Plage d'adresses utilisables : de la première à l'avant-dernière adresse de chaque sous-réseau
- Broadcast : la dernière adresse de chaque sous-réseau

3. Cinq sous-réseaux de 120 hôtes :

- Adresse réseau : 10.0.0.96/25, 10.0.0.128/25, 10.0.0.160/25, 10.0.0.192/25, 10.0.0.224/25
- Plage d'adresses utilisables : de la première à l'avant-dernière adresse de chaque sous-réseau
- Broadcast : la dernière adresse de chaque sous-réseau

4. Cinq sous-réseaux de 160 hôtes :- Adresse réseau : 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24, 10.0.5.0/24

- Plage d'adresses utilisables : de la première à l'avant-dernière adresse de chaque sous-réseau

- Broadcast : la dernière adresse de chaque sous-réseau

12/

1. Physique	Transmet les bits bruts sur le support physique	Fibre optique, câble RJ45, Wi-Fi
2. Liaison de données	Gère l'accès au support physique et la détection d'erreurs	Ethernet, MAC
3. Réseau	Gère le routage des données à travers le réseau	IPv4, IPv6
4. Transport	Assure la fiabilité et le contrôle de flux des données	TCP, UDP
5. Session	Établit, gère et termine les connexions entre les applications	PPTP
6. Présentation	Gère la conversion, la compression et le chiffrement des données	SSL/TLS
7. Application 	Fournit des services de réseau aux applications utilisateurs	HTML, FTP

13/

→ Quelle est l'architecture de ce réseau ?

C'est Architecture en étoile.

→ Indiquer quelle est l'adresse IP du réseau ?

l'adresse IP du réseau est 192.168.10.0.

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

l'adresse de diffusion de ce réseau es 192.168.10.255.

14/ Convertissez les adresses IP suivantes en binaires :

145.32.59.24 en binaire est 10010001.00100000.00111011.00011000

200.42.129.16 en binaire est 11001000.00101010.10000001.00010000

14.82.19.54 en binaire est 00001110.01010010.00010011.00110110

15/

Définition:

Routage=Le routage est le processus de transmission de données entre différents réseaux informatiques. Il implique la sélection du meilleur chemin pour acheminer les

paquets de données d'une source à une destination, en utilisant des protocoles de routage tels que OSPF ou BGP.

Gateway=Une passerelle (gateway en anglais) est un dispositif qui permet de connecter des réseaux informatiques différents. Elle agit comme un point d'entrée ou de sortie pour les données entre ces réseaux, en traduisant les protocoles et en facilitant la communication entre eux.

Un VPN=Un VPN (Virtual Private Network) est un réseau privé virtuel qui permet de créer une connexion sécurisée et chiffrée entre un appareil et un réseau distant via Internet. Il permet de protéger la confidentialité des données en transit et de contourner les restrictions géographiques en masquant l'adresse IP réelle de l'utilisateur.

Le DNS = Le DNS (Domain Name System) est un système qui traduit les noms de domaine (comme exemple.com) en adresses IP numériques compréhensibles par les ordinateurs. Il agit comme un annuaire qui permet de localiser les serveurs correspondant aux noms de domaine et de faciliter la navigation sur Internet en utilisant des noms conviviaux plutôt que des adresses IP numériques.