

Runtrack Réseau

job 2

→ Qu'est-ce qu'un réseau ?

Un réseau se compose d'un groupe d'appareil connecté entre eux qui permet l'échange d'informations.

→ À quoi sert un réseau informatique ?

Un réseau informatique sert à accomplir plusieurs tâches essentielles, notamment, il permet la communication, le partage de ressources, l'accès à Internet, la centralisation des données ainsi que la gestion des ressources

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

Pour construire un réseau, vous aurez besoin de divers composants matériels, chacun ayant une fonction spécifique. Voici les principaux éléments d'un réseau informatique :

Ordinateurs/Dispositifs Clients : Ce sont les appareils utilisés par les utilisateurs pour accéder au réseau. Ils peuvent être des ordinateurs de bureau, des ordinateurs portables, des smartphones, des tablettes, etc.

Serveurs : Les serveurs sont des ordinateurs puissants conçus pour fournir des services, tels que le stockage de données, l'hébergement de sites web, la messagerie électronique, etc.

Commutateurs (Switches) : Les commutateurs sont des dispositifs de réseau utilisés pour relier et gérer la communication entre les dispositifs clients. Ils acheminent les données vers les destinataires appropriés.

Routeurs : Les routeurs relient différents réseaux (par exemple, le réseau local à Internet) et acheminent le trafic entre eux. Ils sont essentiels pour l'accès à Internet.

Firewalls : Les pare-feu sont des dispositifs de sécurité qui protègent le réseau contre les menaces en filtrant le trafic entrant et sortant.

Câbles et Connexions : Les câbles Ethernet et les connexions sans fil (Wi-Fi) permettent aux dispositifs de réseau de communiquer entre eux.

Périphériques réseau : Cela inclut des dispositifs tels que les imprimantes réseau, les scanners, les points d'accès Wi-Fi et les caméras IP qui peuvent être partagés sur le réseau.

Serveurs de Stockage : Les serveurs de stockage centralisent et gèrent les données partagées, permettant aux utilisateurs d'y accéder.

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

Modems : Les modems sont nécessaires pour établir une connexion Internet, convertissant les signaux entre le réseau local et le fournisseur de services Internet.

Câblage structuré : Les câbles Ethernet sont installés de manière organisée dans les locaux pour connecter les dispositifs réseau.

job 3

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

J'ai choisi le Câble Ethernet croisé car il est utilisé pour relier deux récepteurs ensemble sans passer par un réseau internet ou un commutateur ou un routeur.

job 4

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est un identifiant numérique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication.

→ À quoi sert un IP ?

Les adresses IP servent à deux fonctions principales, l'Identification et la Localisation

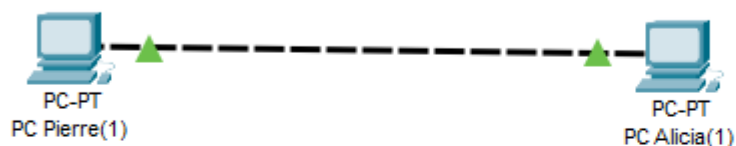
→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un identifiant physique unique attribué à chaque carte réseau d'un dispositif. Contrairement à l'adresse IP, qui peut être configurée ou modifiée par l'utilisateur, l'adresse MAC est intégrée dans le matériel du dispositif et est permanente.

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

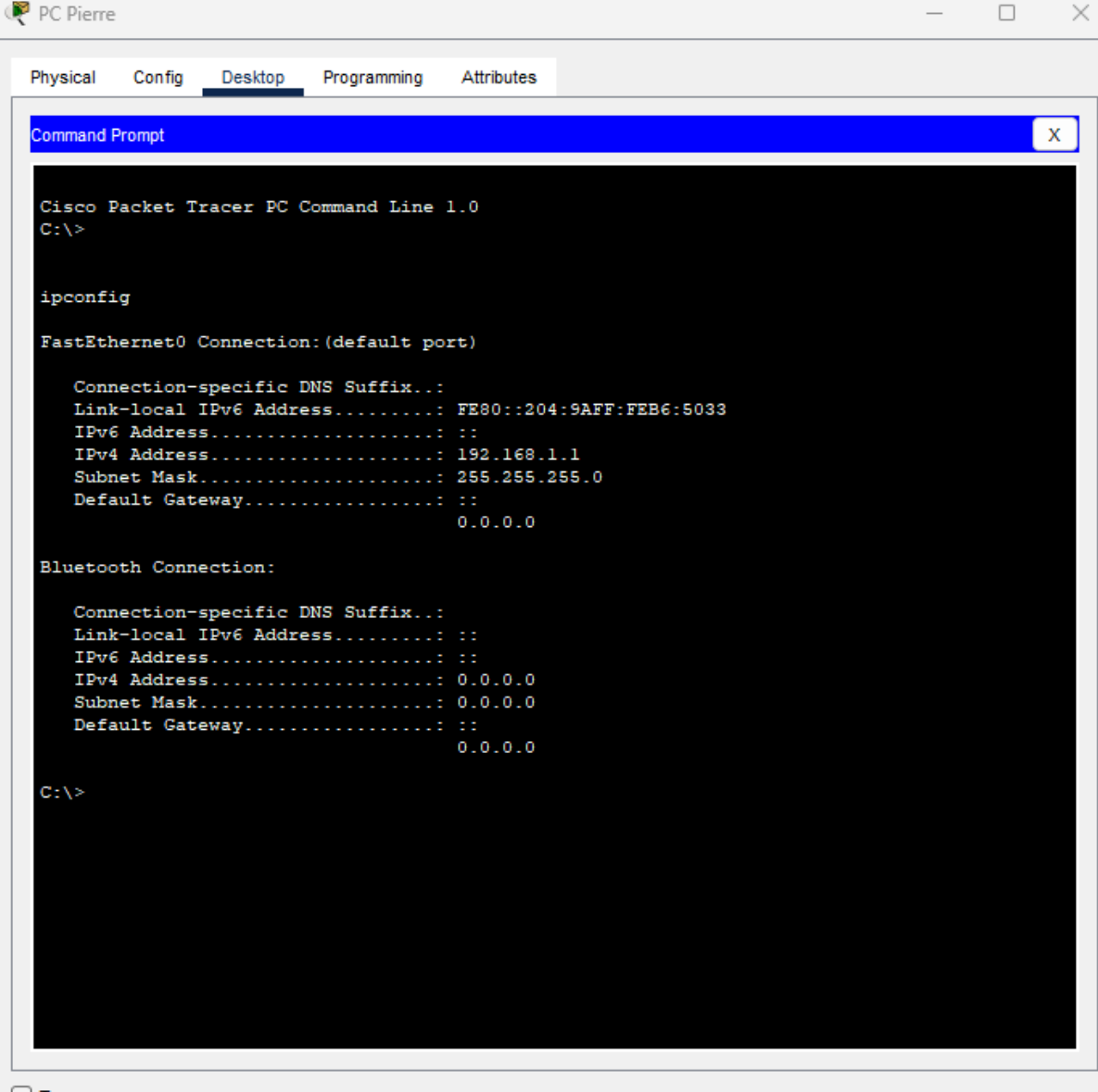
Une adresse IP publique est une adresse attribuée à un routeur ou un dispositif qui est directement connecté à Internet. Elle est utilisée pour identifier ce dispositif sur Internet de manière globale et est généralement visible depuis n'importe quel point d'Internet.

Une adresse IP privée est une adresse attribuée à un dispositif sur un réseau local privé, tel qu'un réseau domestique ou un réseau d'entreprise. Ces adresses sont généralement invisibles depuis Internet et sont utilisées pour acheminer le trafic localement au sein du réseau privé.



job 5

→ Quelle ligne de commande avez-vous utilisée pour vérifier l'IP des machines ?
J'ai utilisé la commande ipconfig



The screenshot shows a window titled "PC Pierre" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a "Command Prompt" window. The Command Prompt shows the output of the "ipconfig" command, which displays network configuration details for both FastEthernet0 and Bluetooth connections. The FastEthernet0 connection shows an IPv4 address of 192.168.1.1 and a subnet mask of 255.255.255.0. The Bluetooth connection shows all fields as empty or 0.0.0.0.

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

ipconfig

FastEthernet0 Connection: (default port)

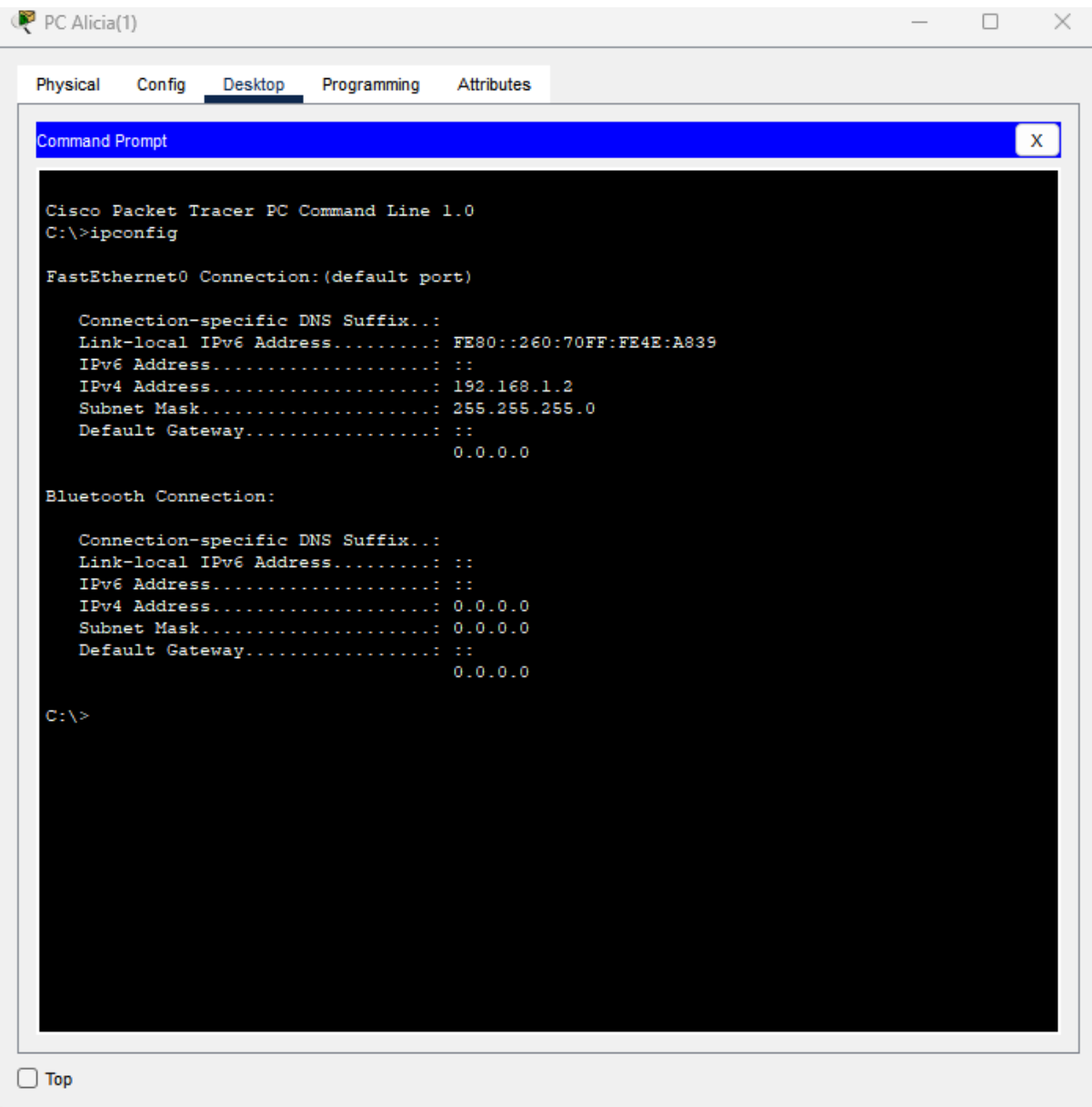
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::204:9AFF:FEB6:5033
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

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

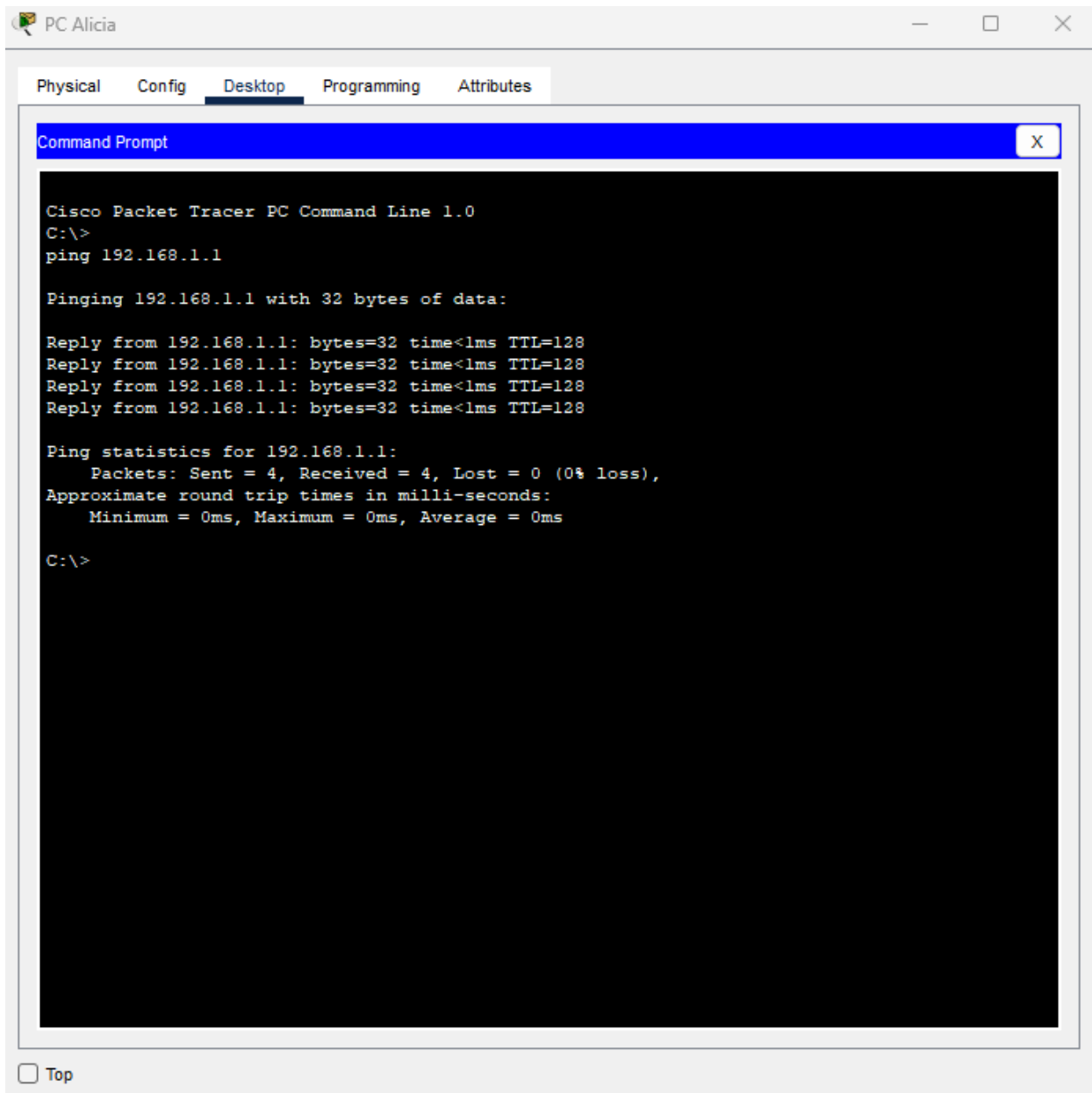
C:\>
```

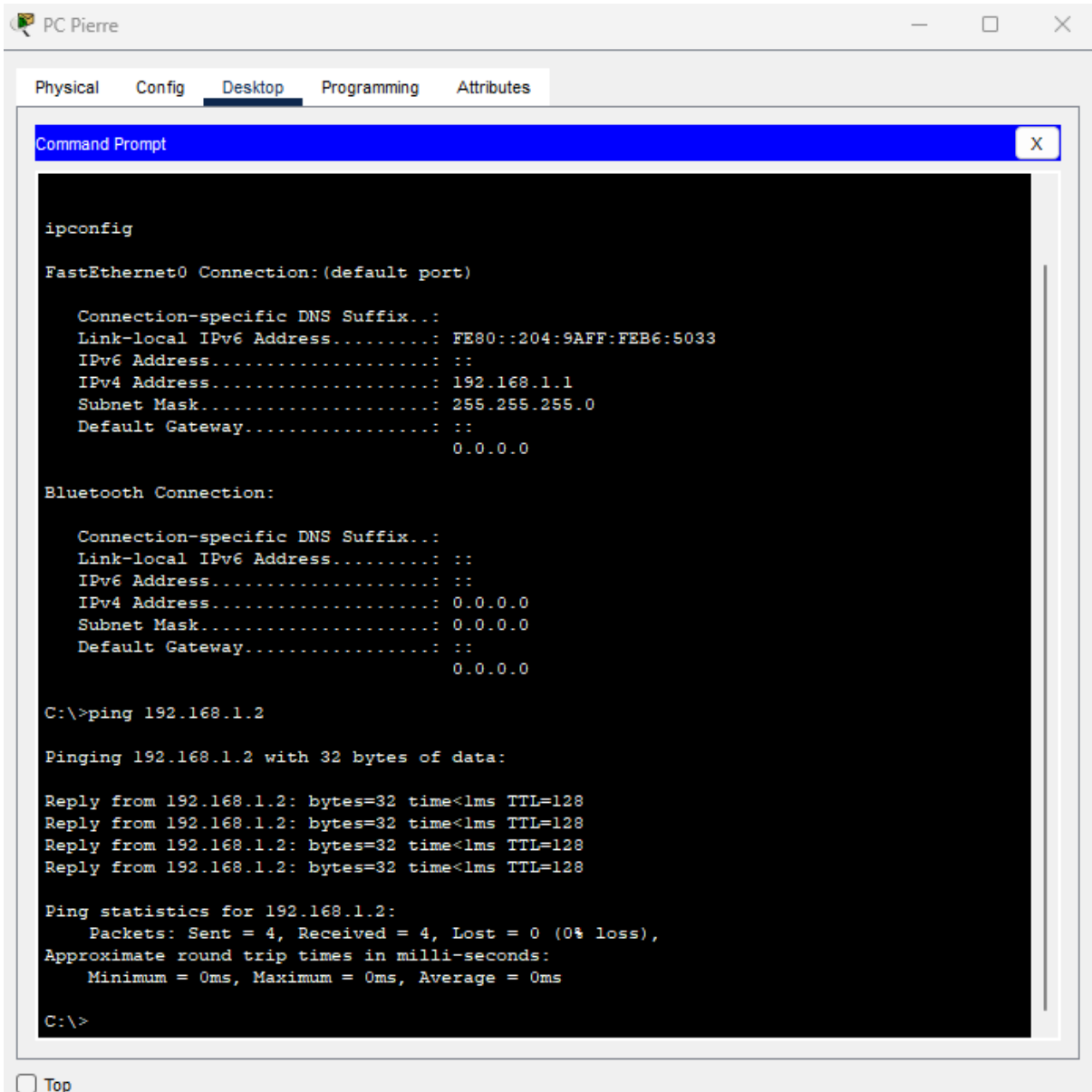
☐ Top



job 6

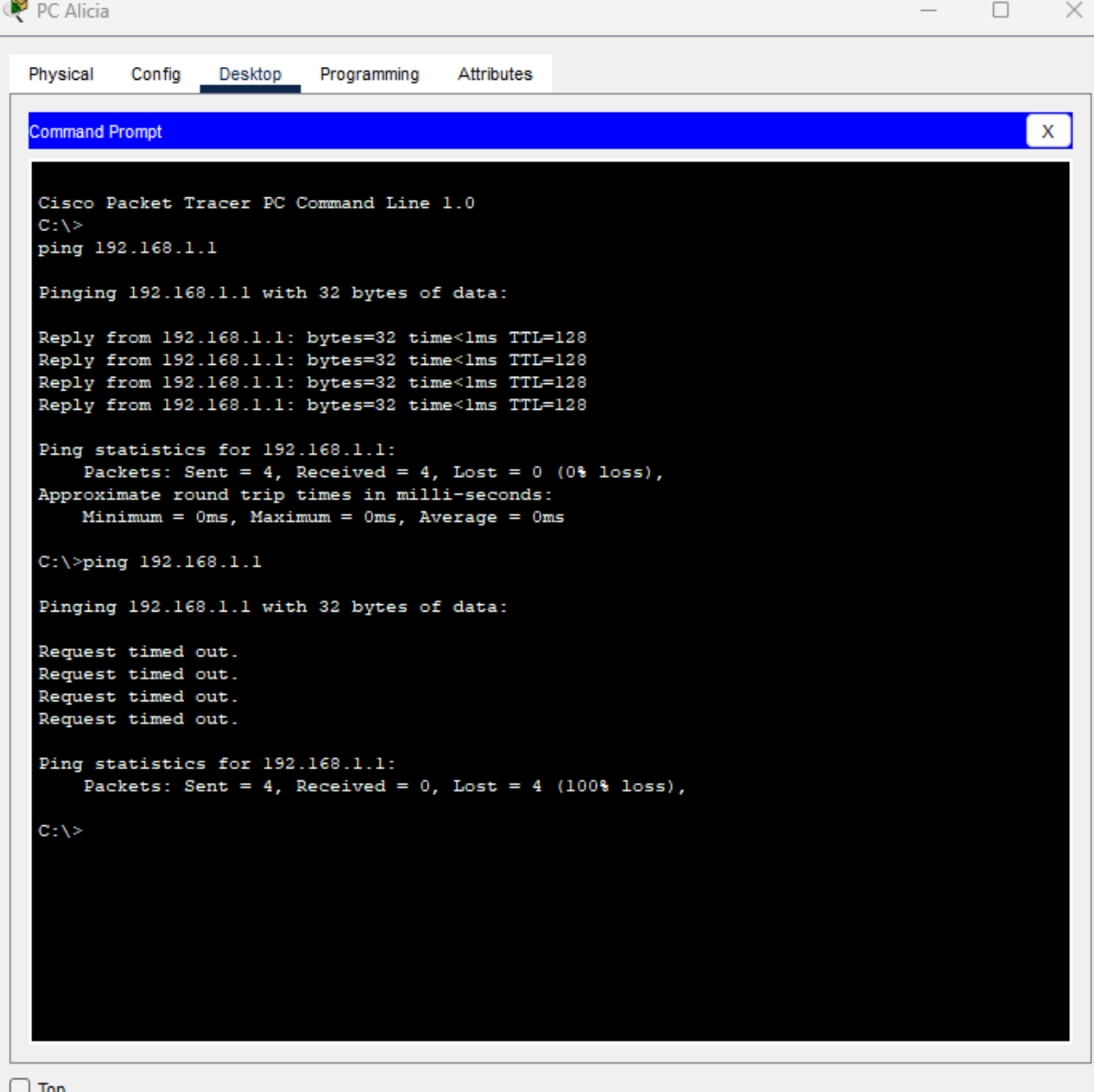
→ Quelle est la commande permettant de Ping entre des PC ?
ping+ adresse IP (exemple ping 192.168.1.1)





job 7

→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?
Non le PC Pierre n'a pas reçu les paquets envoyés par Alicia



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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

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:\>
```

☐ Top

→ Expliquez pourquoi.
le PC Pierre et Éteint donc la communication entre les deux PC n'a pas été établie avec succès.

job 8

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

Un hub et un switch sont des dispositifs de réseau utilisés pour connecter plusieurs appareils dans un réseau local (LAN). Cependant, ils fonctionnent de manière très différente :

Hub : Un hub fonctionne au niveau de la couche physique du modèle OSI. Il transmet simplement les données reçues à tous les ports sans tenir compte de l'adresse de destination. Tous les dispositifs connectés au hub reçoivent donc toutes les données, indépendamment de leur destination.

Switch : Un switch fonctionne au niveau de la couche de liaison de données du modèle OSI. Il apprend les adresses MAC des dispositifs connectés à ses ports et transmet les données uniquement au port approprié en fonction de l'adresse MAC de destination. Cela rend la communication plus efficace et sécurisée, car seuls les dispositifs destinataires reçoivent les données.

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

Fonctionnement :

Un hub répète simplement les signaux entrants à tous les ports, créant ainsi un réseau partagé où tous les dispositifs reçoivent toutes les données.

Avantages :

Simplicité et coût réduit.

Facilité d'installation et de maintenance.

Inconvénients :

Utilisation inefficace de la bande passante, car tous les dispositifs partagent la même bande passante.

Manque de sécurité, car toutes les données sont visibles par tous les dispositifs.

Peu approprié pour les réseaux de grande taille en raison de la congestion du trafic.

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

Avantages :

Efficace car il transmet les données uniquement aux dispositifs destinataires, optimisant ainsi l'utilisation de la bande passante.

Il permet l'isolation du trafic entre les ports, ce qui renforce la sécurité.

Augmente la performance car il convient aux réseaux de toutes tailles grâce à une gestion efficace du trafic.

Inconvénients :

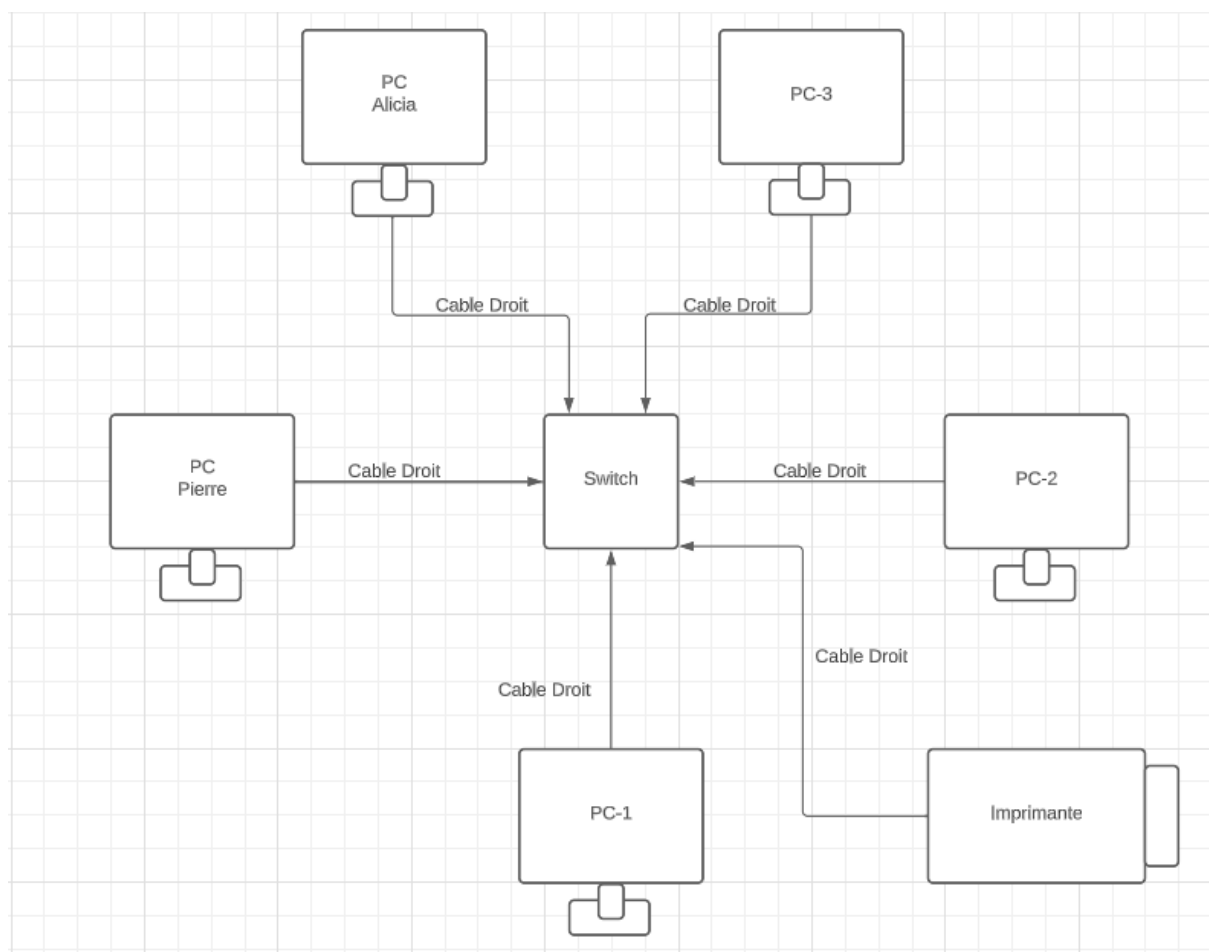
Coût plus élevé que les hubs.

La configuration et la maintenance peuvent être plus complexes que celles des hubs.

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

Un switch gère le trafic réseau en apprenant les adresses MAC des dispositifs connectés à ses ports. Lorsqu'un dispositif envoie des données, le switch examine l'adresse MAC de destination dans les trames Ethernet. En fonction de cette adresse, le switch sait quel port doit être utilisé pour atteindre le dispositif de destination. Il transmet ensuite les données uniquement à ce port, ce qui réduit la congestion du réseau et améliore les performances. En conséquence, un switch assure une gestion efficace du trafic en évitant la diffusion inutile de données sur tous les ports, contrairement à un hub.

job 9



Avoir un schéma de réseau bien conçu offre de nombreux avantages. Un schéma de réseau fournit une représentation visuelle de la topologie et de la configuration du réseau. Cela facilite la compréhension de la manière dont les dispositifs sont interconnectés et comment les données circulent, ce qui simplifie la résolution de problèmes, la maintenance et la gestion. En cas de problème ou de panne dans le réseau, un schéma bien documenté permet de localiser rapidement la source du problème. Un schéma de réseau est aussi essentiel pour planifier les mises à jour, les extensions et les changements dans le réseau. Il permet de modéliser l'impact de nouvelles connexions ou de l'ajout de dispositifs, d'identifier les points de congestion potentiels et de concevoir des solutions pour améliorer les performances. Le schéma sert également de référence pour documenter les modifications apportées au réseau au fil du temps.

En résumé,

- Clarté et compréhension
- Dépannage facilité
- Planification et évolution du réseau

sont les trois plus importants avantages que confère un schéma de réseau.

job 10

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

Avec une adresse IP statique, l'adresse IP est configurée manuellement sur chaque dispositif. Cela signifie qu'une adresse IP spécifique est attribuée de manière permanente à chaque dispositif et ne change pas sauf si elle est manuellement modifiée.

Et une adresse IP attribuée par DHCP est gérée automatiquement et peut changer à chaque connexion.

job 11

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

Les adresses IP de classe A sont réservées aux réseaux de grande envergure, car elles offrent un grand espace d'adressage avec des millions d'adresses uniques.

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

Les adresses IP sont regroupées en classes (A, B, C, D et E) et sont distinguées en fonction de leur plage d'adresses et de leur structure. Les adresses de classe A ont un octet de réseau et trois octets d'hôte. Elles sont adaptées aux réseaux de grande envergure, car elles permettent un grand nombre d'hôtes, mais elles utilisent également beaucoup d'adresses IP. Exemple : 10.0.0.0.

Les adresses de classe B ont deux octets de réseau et deux octets d'hôte. Elles sont adaptées aux réseaux de taille moyenne. Exemple : 172.16.0.0.

Les adresses de classe C ont trois octets de réseau et un octet d'hôte. Elles sont adaptées aux petits réseaux. Exemple : 192.168.0.0.

Les adresses de classe D sont réservées pour la multidiffusion et ne sont pas utilisées pour identifier des hôtes individuels.

Les adresses de classe E sont réservées à des fins expérimentales et ne sont pas utilisées dans les réseaux publics.

job 12

Couche OSI	Description du rôle	Matériels/Protocoles associés
Couche 7 - Application	Fournit des services aux applications utilisateur, tels que la messagerie électronique, la navigation web, etc.	HTML, FTP, SSL/TLS, PPTP
Couche 6 - Présentation	Gère la traduction, la compression et le chiffrement des données pour s'assurer qu'elles sont compréhensibles par l'application.	SSL/TLS, HTML (pour la mise en forme des données)
Couche 5 - Session	Établit, gère et termine les sessions de communication entre les applications.	PPTP, FTP (pour l'établissement de sessions)
Couche 4 - Transport	Gère la communication de bout en bout, la fiabilité, le contrôle de flux et la segmentation/déségmentation des données.	TCP, UDP
Couche 3 - Réseau	Gère le routage des données, le choix du meilleur chemin pour atteindre la destination, ainsi que la fragmentation et le réassemblage des paquets.	IPv4, IPv6, routeur
Couche 2 - Liaison de données	Gère la communication entre dispositifs directement connectés sur le même réseau local. Elle gère également le contrôle d'accès au support.	Ethernet, MAC, Wi-Fi, câble RJ45
Couche 1 - Physique	Gère la transmission de bits bruts sur un support physique (câble, fibre optique, etc.)	Fibre optique, câble RJ45

job 13

→ Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est une architecture simple, basée sur une topologie en étoile. Les quatre PC sont connectés à un switch, qui relie également les deux serveurs. Cette architecture en étoile est courante dans les réseaux locaux (LAN).

→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est généralement l'adresse réseau de la plage d'adresses utilisée pour les dispositifs. Dans notre cas, l'adresse réseau est 192.168.10.0/24.

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

Le nombre de machines que l'on peut brancher sur ce réseau est de 254 machines.

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

L'adresse de diffusion de ce réseau est généralement l'adresse la plus élevée dans la plage d'adresses IP. Dans notre cas, l'adresse de diffusion est 192.168.10.255.

job 14

145.32.59.24 :

145 en binaire : 10010001

32 en binaire : 00100000

59 en binaire : 00111011

24 en binaire : 00011000

Adresse IP complète en binaire : 10010001.00100000.00111011.00011000

200.42.129.16 :

200 en binaire : 11001000

42 en binaire : 00101010

129 en binaire : 10000001

16 en binaire : 00010000

Adresse IP complète en binaire : 11001000.00101010.10000001.00010000

14.82.19.54 :

14 en binaire : 00001110

82 en binaire : 01010010

19 en binaire : 00010011

54 en binaire : 00110110

Adresse IP complète en binaire : 00001110.01010010.00010011.00110110

job 15

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission de données d'un réseau à un autre, en choisissant le chemin optimal pour acheminer les données de la source à la destination

→ Qu'est-ce qu'un gateway ?

Une passerelle, ou gateway en anglais, est un dispositif ou un système qui agit en tant que point d'entrée ou de sortie entre deux réseaux distincts, permettant ainsi la communication entre eux.

→ Qu'est-ce qu'un VPN ?

Un réseau privé virtuel est une technologie qui permet de créer une connexion sécurisée entre deux réseaux distants via un réseau public, généralement Internet. Un VPN utilise un tunnel sécurisé pour chiffrer les données en transit, garantissant ainsi la confidentialité et la sécurité de la communication.

→ Qu'est-ce qu'un DNS ?

Le DNS est un système de noms de domaine qui convertit les noms de domaine, tels que www.example.com, en adresses IP, comme 192.168.1.1. Il s'agit d'une infrastructure essentielle sur Internet qui permet aux utilisateurs d'accéder aux sites web, aux serveurs de messagerie et à d'autres services en utilisant des noms faciles à retenir au lieu d'adresses IP numériques.