

Runtrack

Réseau

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

By Alyson He YU-COOPER



Du Câble au Cosmique

- Après l'évolution de nos ordinateurs, il a fallu permettre la communication entre ces machines. Initialement, les premiers réseaux informatiques étaient de portée limitée, ne couvrant que quelques dizaines de mètres.
- Cependant, au fil du temps, ces réseaux ont connu une expansion et une amélioration constantes, jusqu'à ce que nous soyons désormais capables de communiquer depuis l'espace.

JOB 01

Cisco Packet Tracer

Cisco Packet Tracer est un outil de simulation de réseau puissant qui vous permet de pratiquer des compétences en réseau, IoT et cybersécurité dans un laboratoire virtuel sans avoir besoin de matériel. Il est utilisé par les apprenants explorant les carrières en réseau et en technologie, les étudiants en réseau, IoT et cybersécurité, les ingénieurs, les éducateurs, les formateurs et pour l'enseignement et l'apprentissage à distance. Vous pouvez l'utiliser pour pratiquer la construction de réseaux simples et complexes, visualiser comment fonctionne un réseau, pratiquer les compétences de rack, de stack et de câblage dans le laboratoire virtuel, et intégrer des appareils IoT, du code Python ou de l'automatisation de réseau. La dernière version de Cisco Packet Tracer est la 8.





JOB 02

→ Qu'est-ce qu'un réseau ?

- Un réseau, dans son sens étymologique, représente un ensemble de points entrelacés par un ensemble de relations. Par extension, cela désigne un ensemble interconnecté d'équipements et de leurs relations, autorisant la circulation en continu ou discontinue.

On trouve différents types de réseaux:

Réseau en arbre

L'architecture est divisée en niveaux. Le sommet représente la racine ou le sommet et est connecté à plusieurs nœuds du niveau inférieur.

Réseau en étoile

C'est la topologie la plus courante. Elle permet une gestion et un dépannage très facile.

1

2

3

4

5

Réseau en anneau

Toutes les stations ou équipements sont connectés en chaîne les uns aux autres par une liaison bipoint de la dernière à la première.

Réseau en bus

Le câblage s'effectue via une liaison unique des unités.

Réseau maillé

Cela correspond à plusieurs liaisons point à point où chaque unité est reliée à N-1 point permettant ainsi de la mettre en relation avec l'ensemble des autres équipements.

- Dans le domaine informatique, un réseau est défini par la mise en relation d'au moins deux systèmes informatiques au moyen d'un câble ou sans fil, par liaison radio.
- Un réseau peut aussi être un ensemble de circuits, de canalisations et des appareils qui les relient, permettant la circulation et la distribution de l'électricité, de l'eau, du gaz, du téléphone, etc..





À quoi sert un réseau informatique ?

- Un réseau informatique sert à connecter plusieurs ordinateurs et appareils pour partager des ressources et des données, facilitant ainsi la communication et le partage entre différents systèmes informatiques.
- Un réseau informatique sert à connecter plusieurs ordinateurs et appareils, généralement à l'aide de câbles ou de fils. Le but principal d'un réseau informatique est de partager des ressources et des données entre les systèmes informatiques. Ces ressources partagées peuvent inclure le stockage de données, les imprimantes, les connexions Internet et d'autres appareils.

- Dans un réseau domestique classique, par exemple, le routeur joue le rôle de serveur. Il est relié à Internet et met la ressource « Internet » à disposition des autres appareils (ordinateur, smartphone, etc.). Le routeur rassemble tous les appareils, par connexion filaire et sans fil, au sein d'un réseau local. Dans le contexte d'une entreprise, un réseau informatique permet la mise en relation de tous les postes ordinateurs d'une même société par le biais d'un serveur commun. Cela donne à chaque employé une connexion sécurisée et facilite l'échange des données au sein de la société.
- En somme, un réseau informatique facilite la communication et le partage de ressources entre différents systèmes informatiques.



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

Pour construire un réseau informatique, vous aurez besoin des équipements suivants:



Ordinateurs

Plusieurs ordinateurs fonctionnels disposant des cartes réseau Ethernet et ou wifi.



Routeur

Il permet de relier les réseaux et ainsi de faire circuler (router) des données d'un réseau à un autre de façon optimale. Il est généralement connecté à Internet et met la ressource « Internet » à disposition des autres appareils.



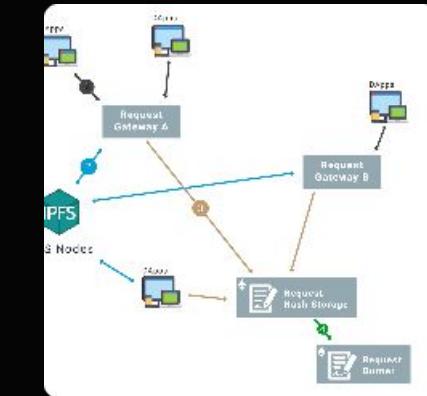
Concentrateur (Hub)

Les concentrateurs connectent plusieurs équipements du réseau informatique. Un concentrateur sert également de répéteur, en ce sens qu'il amplifie les signaux, qui se détériorent après avoir parcouru de longues distances sur les



Commutateur Réseau (Switch)

Les commutateurs jouent généralement un rôle plus intelligent que les concentrateurs. Un commutateur est un dispositif multiport qui améliore l'efficacité du réseau.



Modem

- Il est utilisé pour fournir une connexion Internet à un réseau local.

Firewall (coupe-feu)

- Il est utilisé pour protéger le réseau contre les menaces externes.

Serveur

- Il est utilisé pour stocker des données et des applications qui peuvent être accessibles par tous les utilisateurs du réseau.

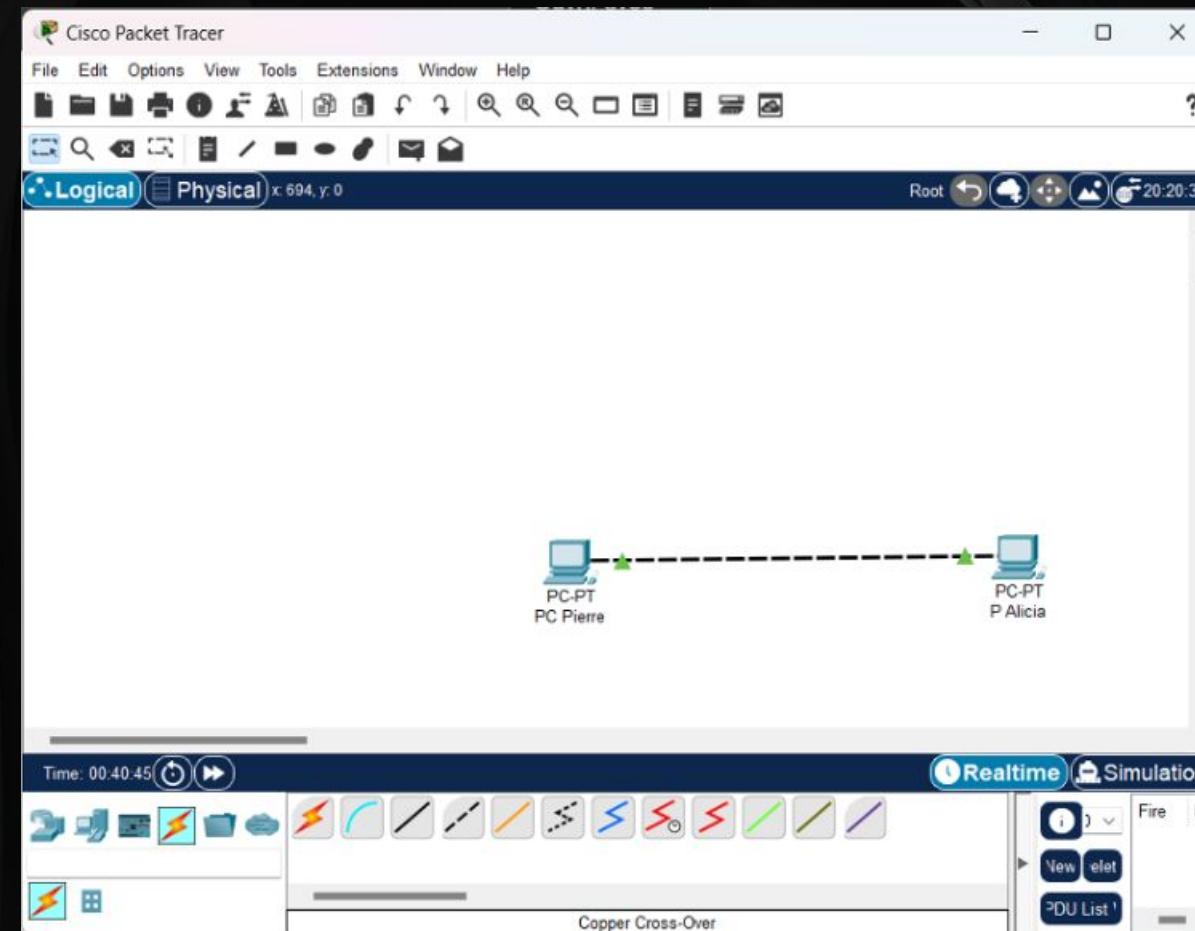
Passerelles (Gateways)

- Elles sont utilisées pour connecter deux réseaux qui utilisent des protocoles de communication différents.

JOB 03

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

- J'ai choisi le cable copper cross-over, parce que les sont généralement utilisés pour connecter deux équipements du même type.



Dans Cisco Packet Tracer, Connections est un outil qui permet de connecter des équipements réseau. Voici les types de connexions courantes :

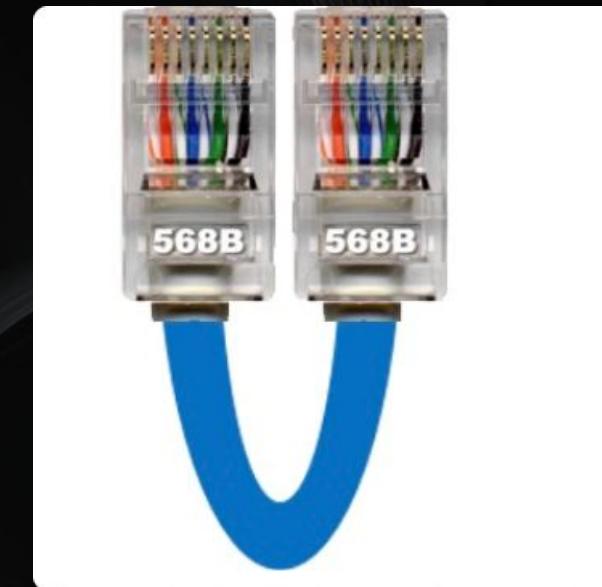
- Choisir automatiquement le type de connexion : Il s'agit d'une option qui choisit automatiquement le type de connexion. Lorsque vous utilisez cette option, Packet Tracer choisira automatiquement le type de câble approprié en fonction du type d'équipement que vous souhaitez connecter.





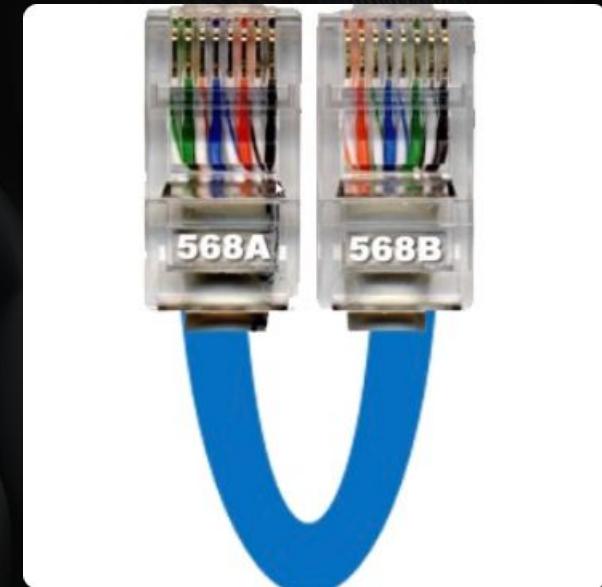
Console

Les câbles de console sont généralement utilisés pour se connecter au port de console d'un routeur ou d'un commutateur pour configurer l'équipement.



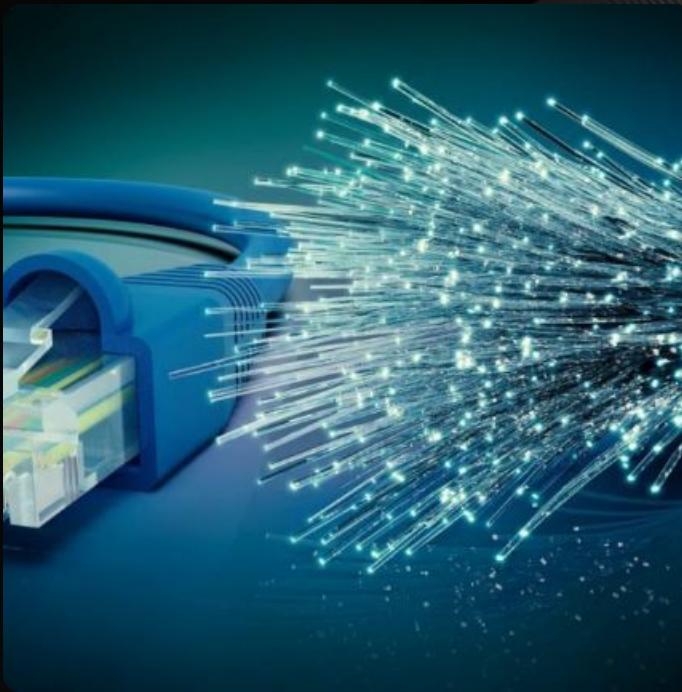
Copper Straight-Through

Les câbles droits sont généralement utilisés pour connecter deux types d'équipements différents, par exemple pour connecter un commutateur à un routeur ou à un ordinateur.



Copper Cross-Over

Les câbles croisés sont généralement utilisés pour connecter deux équipements du même type, par exemple pour connecter un ordinateur à un ordinateur ou un commutateur à un commutateur.



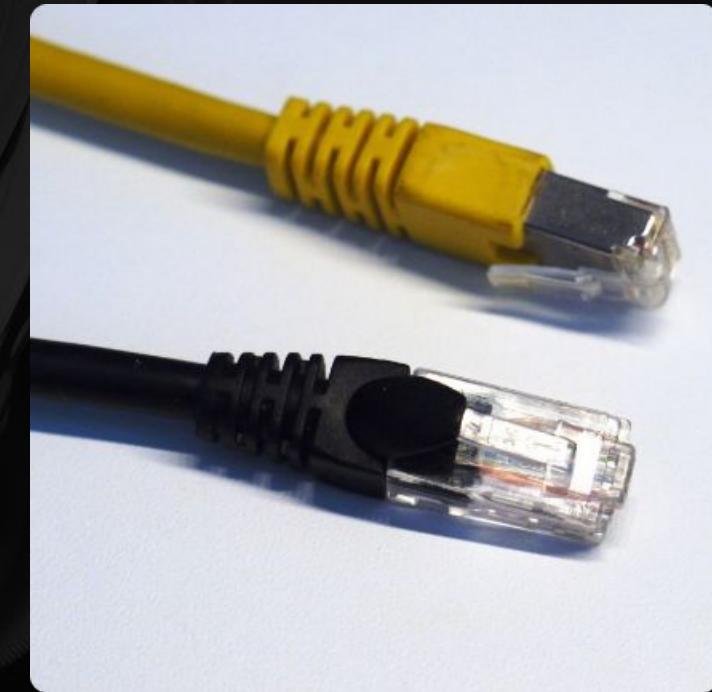
Fiber

Les câbles en fibre optique sont généralement utilisés pour les connexions réseau à longue distance et à grande vitesse.



Phone

Les câbles téléphoniques sont généralement utilisés pour les connexions Internet par modem ou DSL.



Coaxial

Les câbles coaxiaux sont généralement utilisés pour les services de télévision par câble et d'Internet haut débit.



Serial DTE :

DTE (Data Terminal Equipment) désigne un équipement terminal qui convertit les informations utilisateur en signaux ou reconvertit les signaux reçus.

Dans une connexion série, le DTE est généralement un ordinateur ou un terminal.

Octal

Les câbles octaux sont généralement utilisés pour établir des connexions série entre les routeurs.

USB

Les câbles USB sont généralement utilisés pour connecter des ordinateurs à divers périphériques, tels que des imprimantes, des scanners et des dispositifs de stockage.

Job 04

1

Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet.

2

À quoi sert un IP ?

Une adresse IP est une représentation numérique de l'endroit où un appareil est connecté à Internet. C'est ainsi que vous identifiez l'endroit où se trouve un élément et, dans une certaine mesure, la nature de cet élément.

3

Qu'est-ce qu'une adresse MAC ?

MAC signifie "Media Access Control" et cette adresse correspond à l'adresse physique d'un équipement réseau.

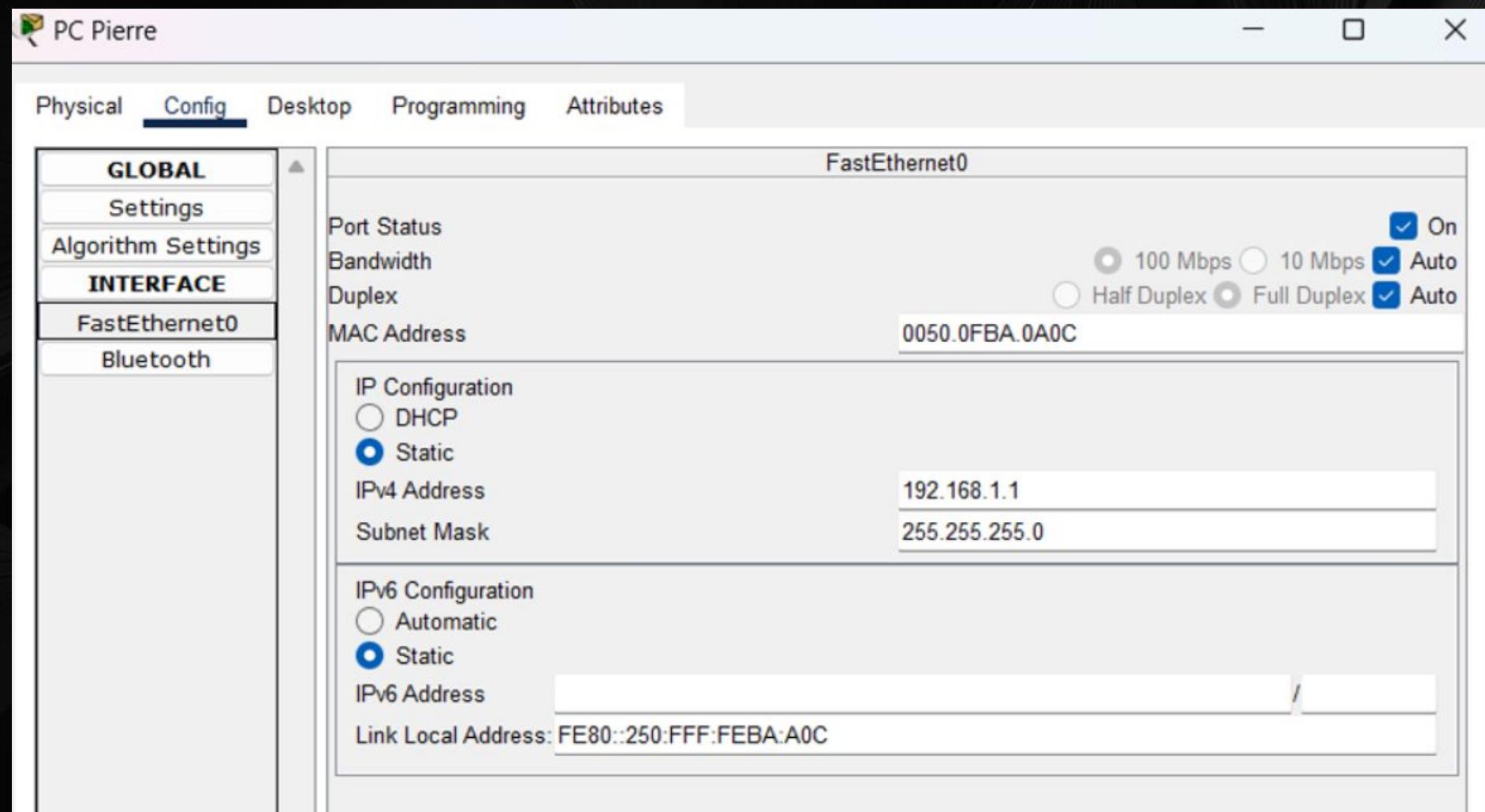
4

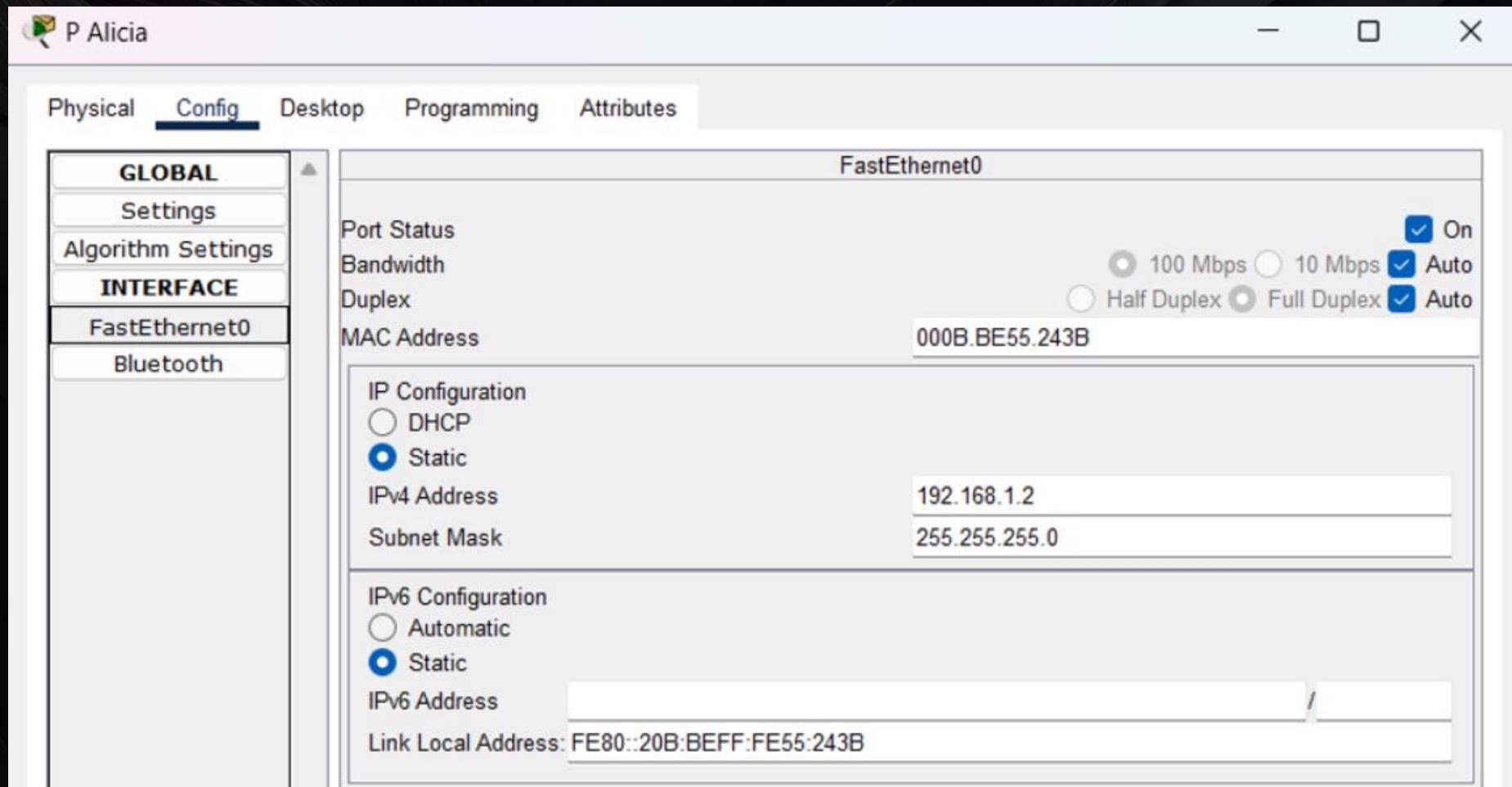
Qu'est-ce qu'une IP publique et privée ?

Les adresses IP publiques sont utilisées pour interagir avec Internet, alors que les IP privées fonctionnent quant à elles sur les réseaux locaux.

→ 5. Quelle est l'adresse de ce réseau ?

- Pour le réseau que vous avez mentionné, l'adresse du réseau peut être déterminée en utilisant l'adresse IP et le masque de sous-réseau du PC Pierre ou du PC Alicia (car ils sont sur le même réseau). Ici, l'adresse IP est 192.168.1.1 ou 192.168.1.2 et le masque de sous-réseau est 255.255.255.0. Lorsque nous appliquons le masque de sous-réseau à l'adresse IP, nous obtenons l'adresse du réseau. Dans ce cas, l'adresse du réseau est 192.168.1.0

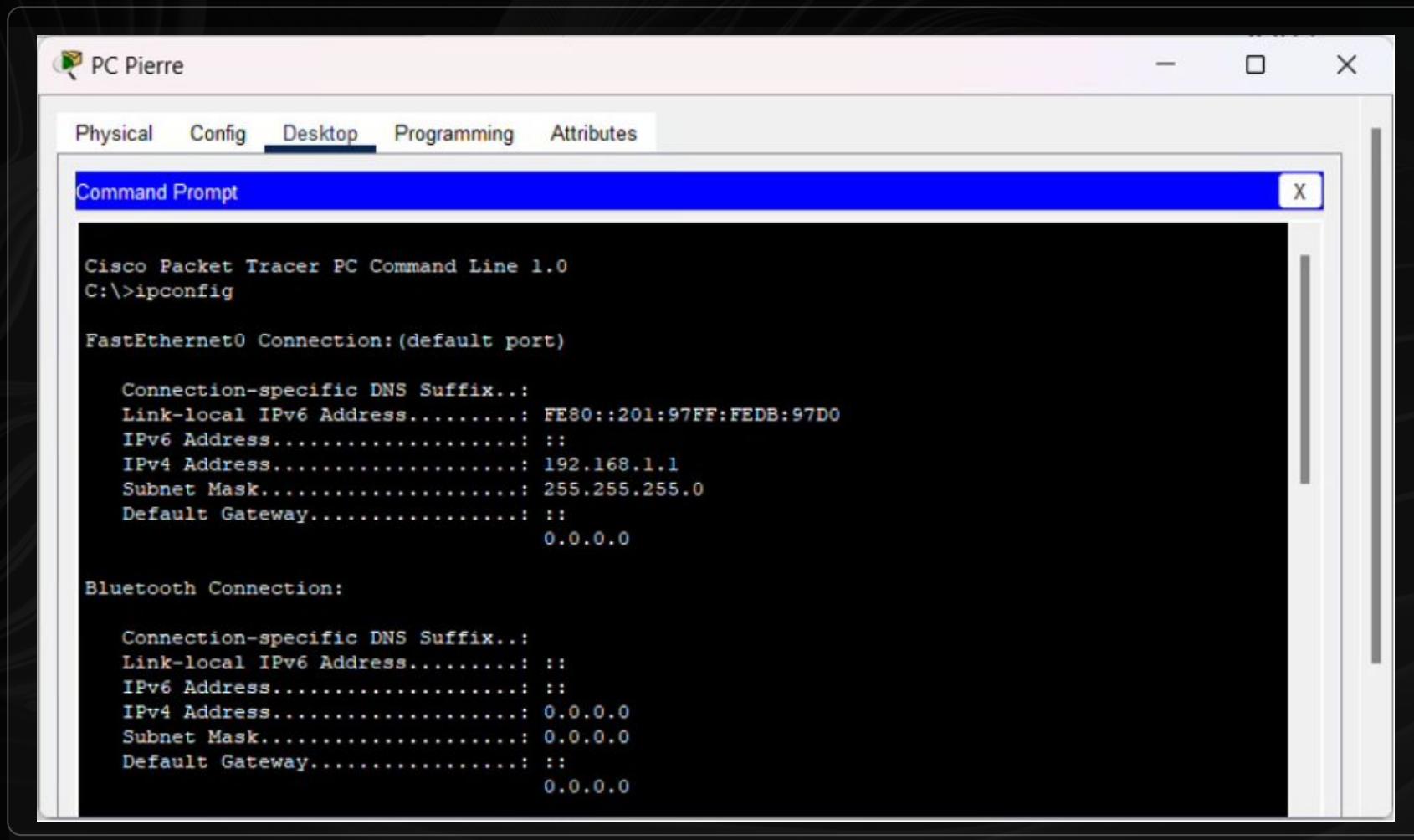




JOB 05

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

- D'abord, j'ai sélectionné l'ordinateur que je souhaite vérifier. Après dans la fenêtre de l'ordinateur, sélectionnez l'onglet Desktop, puis cliquez sur Command Prompt. Ensuite, dans l'invite de commandes, tapez ipconfig et appuyez sur Entrée. Cela affichera les informations d'adresse IP de l'ordinateur.



The screenshot shows a window titled "PC Pierre" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside, a Command Prompt window is open with the title "Command Prompt". The output of the ipconfig command is displayed:

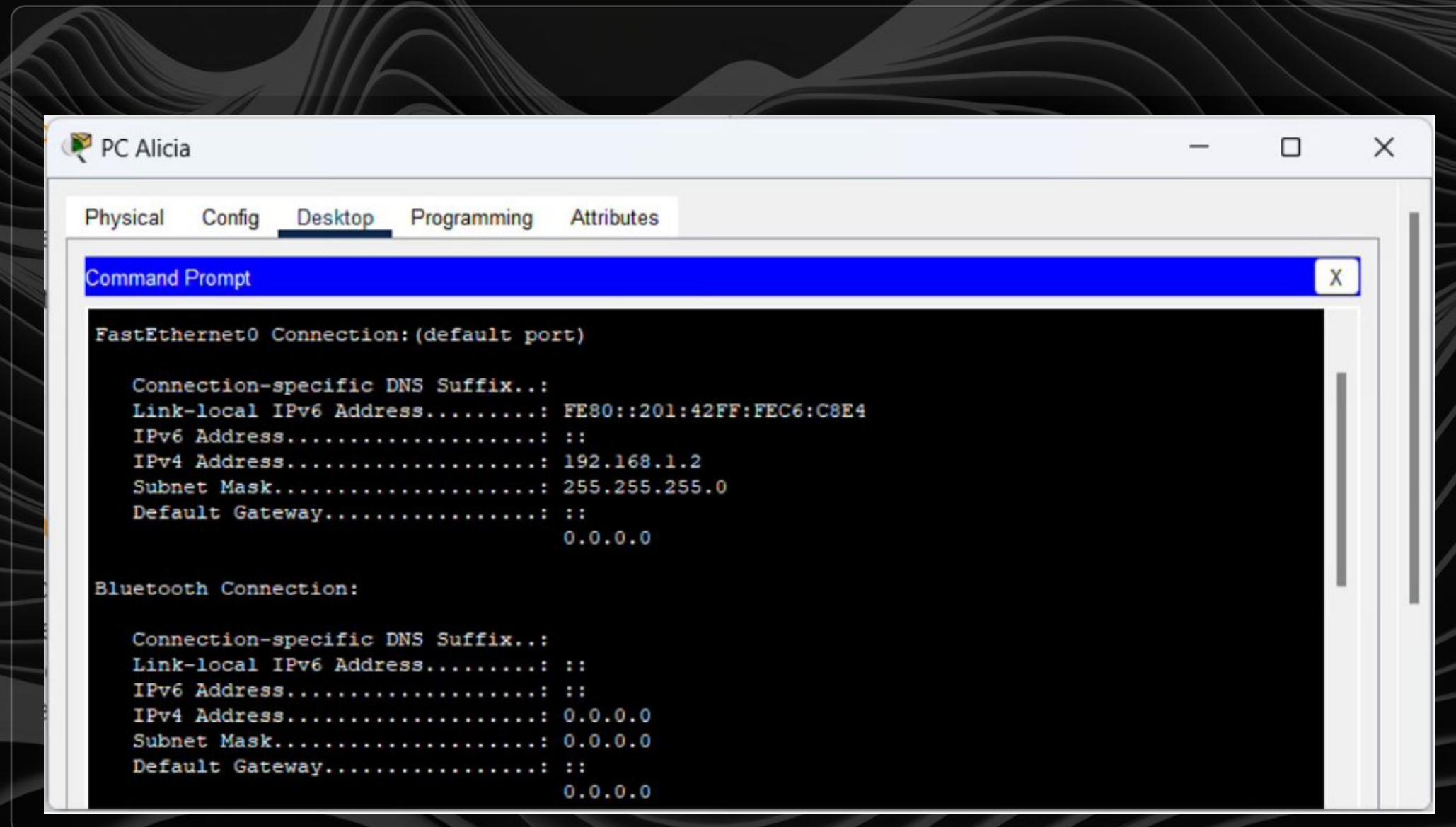
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:97FF:FEDE:97D0
IPv6 Address.....: :::
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
0.0.0.0

Bluetooth Connection:

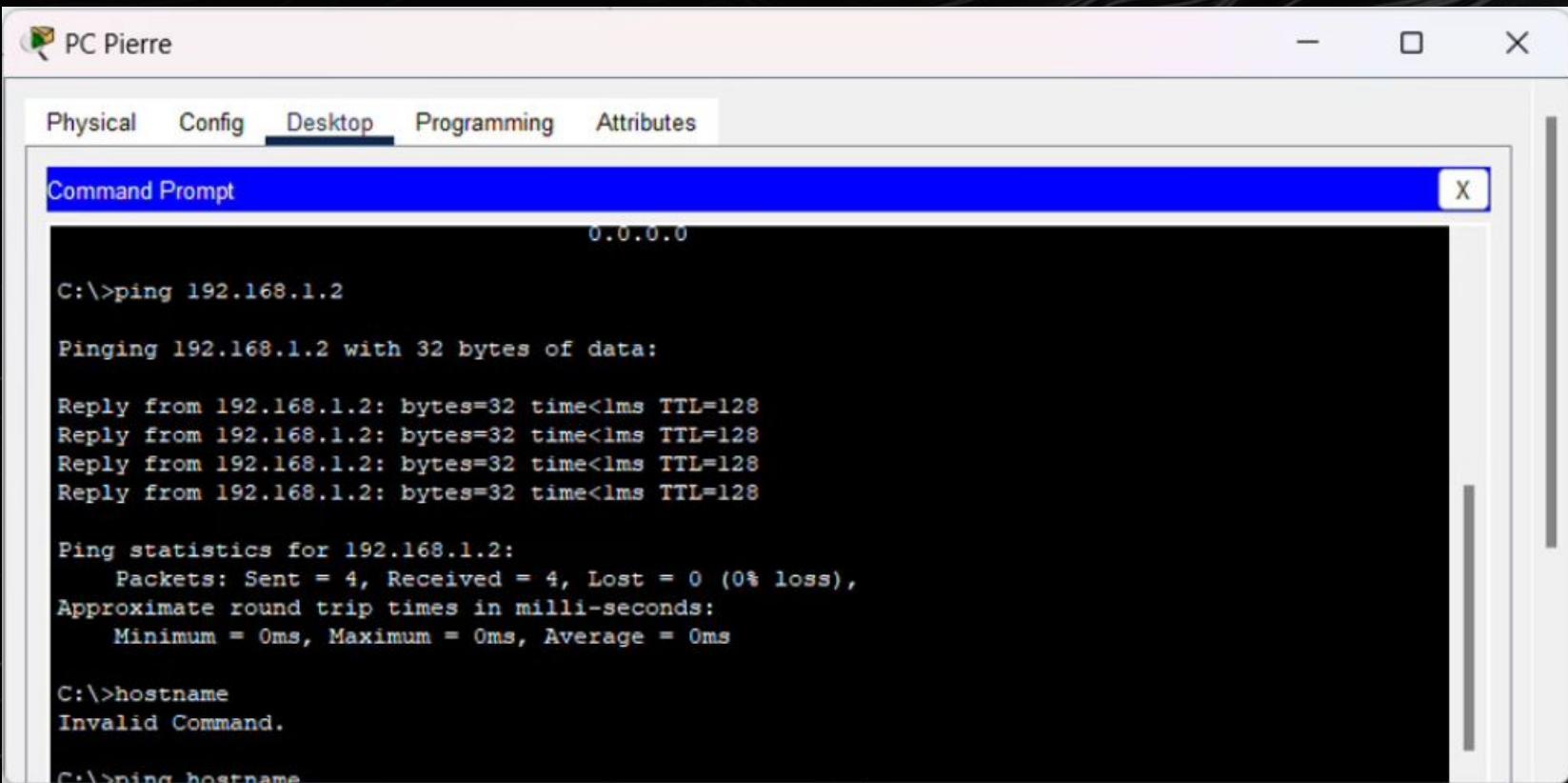
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: :::
IPv6 Address.....: :::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: :::
0.0.0.0
```



JOB 06

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

- Si vous souhaitez tester la connectivité réseau entre les ordinateurs, vous pouvez utiliser la commande ping. Par exemple, si je veux vérifier la connexion entre le PC Pierre (adresse IP 192.168.1.1) et le PC Alicia (adresse IP 192.168.1.2), je peux taper ping 192.168.1.2 dans l'invite de commandes du PC Pierre et appuyer sur Entrée. Si la connexion réseau est bonne, je verrai des réponses provenant de 192.168.1.2.



The screenshot shows a Windows Command Prompt window titled "Command Prompt" with the title bar color set to blue. The window is part of a larger application interface for "PC Pierre" with tabs for Physical, Config, Desktop, Programming, and Attributes, where "Desktop" is currently selected. The main window displays the following command-line session:

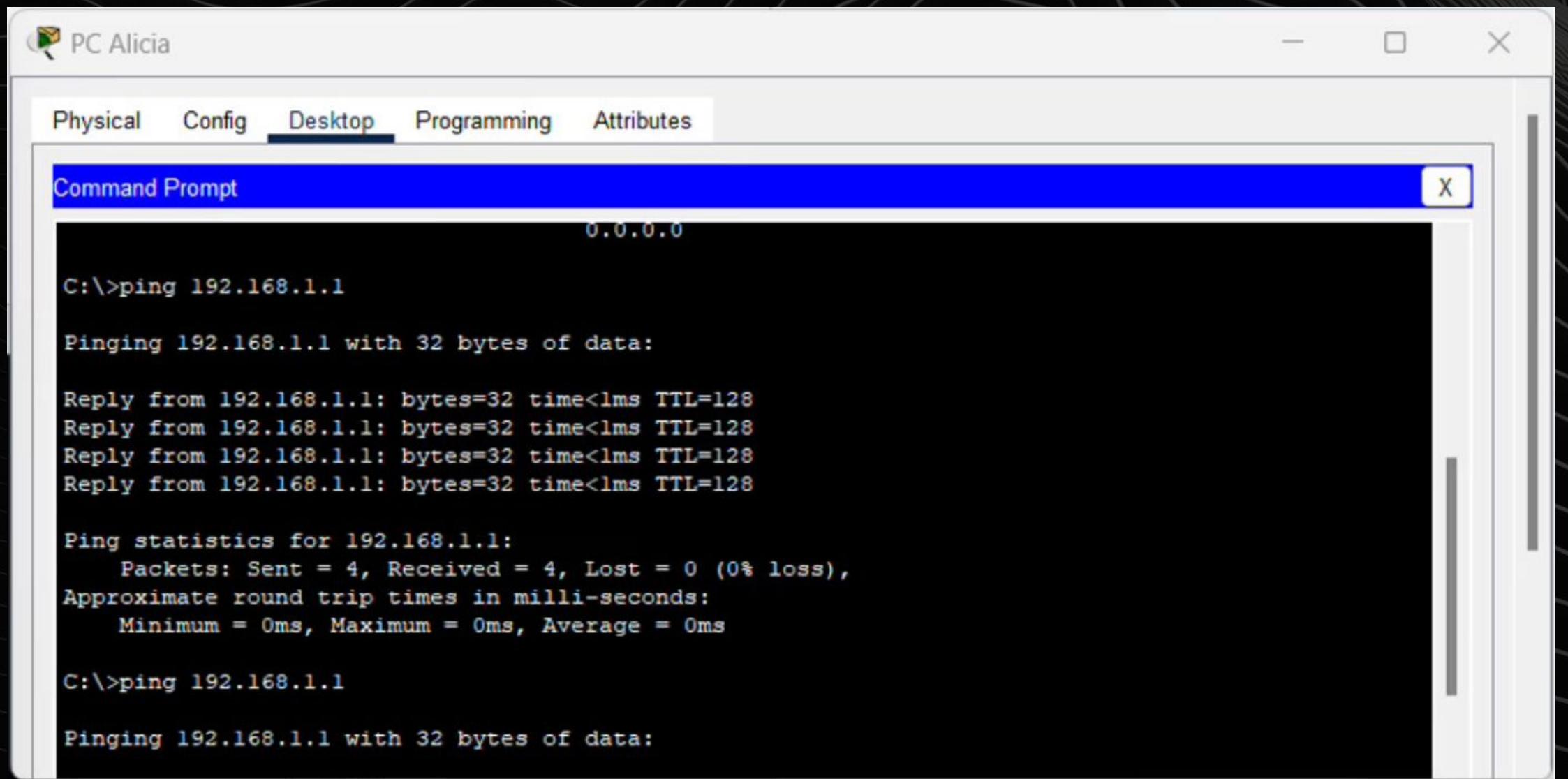
```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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:\>hostname
Invalid Command.

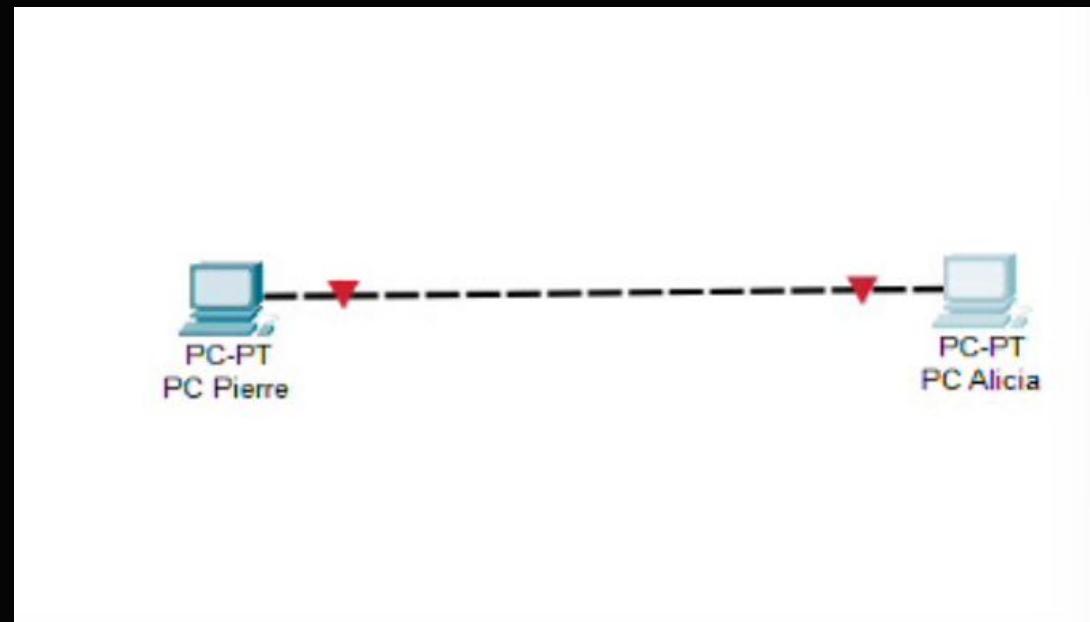
C:\>ping hostname
```



JOB 07

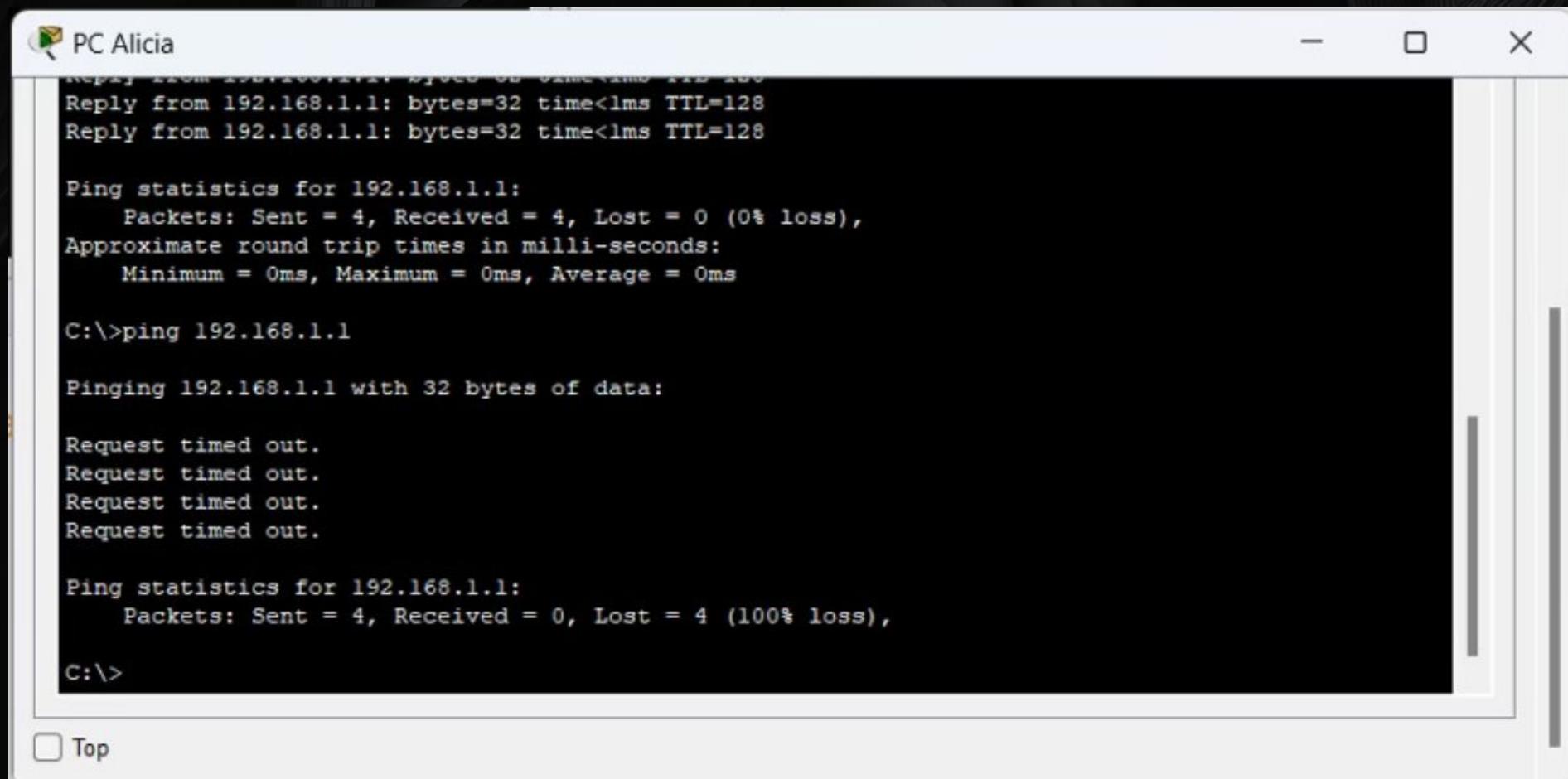
Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

- Si le PC Pierre est déjà éteint, on ne reçoit aucune réponse de la part du PC Pierre. C'est parce que lorsqu'un ordinateur est éteint, il ne répond à aucune demande réseau, y compris les demandes Ping.



→ Expliquez pourquoi.

- Lorsqu'un ordinateur est éteint, tous ses systèmes sont inactifs, y compris le système d'exploitation et la carte réseau. Par conséquent, il ne peut ni recevoir ni traiter aucune requête réseau. De plus, la commande ping fonctionne en envoyant une requête ICMP Echo Request à l'ordinateur cible et en attendant une réponse ICMP Echo Reply. Si l'ordinateur cible est éteint, aucune réponse ne sera renvoyée.



The screenshot shows a Windows Command Prompt window titled "PC Alicia". The window displays the output of a ping command. The first two lines show successful replies from the target IP 192.168.1.1. The third line shows the statistics for the first ping. The fourth line shows the command "C:\>ping 192.168.1.1". The fifth line starts a new ping attempt, showing "Pinging 192.168.1.1 with 32 bytes of data:". The next four lines show "Request timed out." for each attempt. The final line shows the statistics for the second ping, indicating 100% loss.

```
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

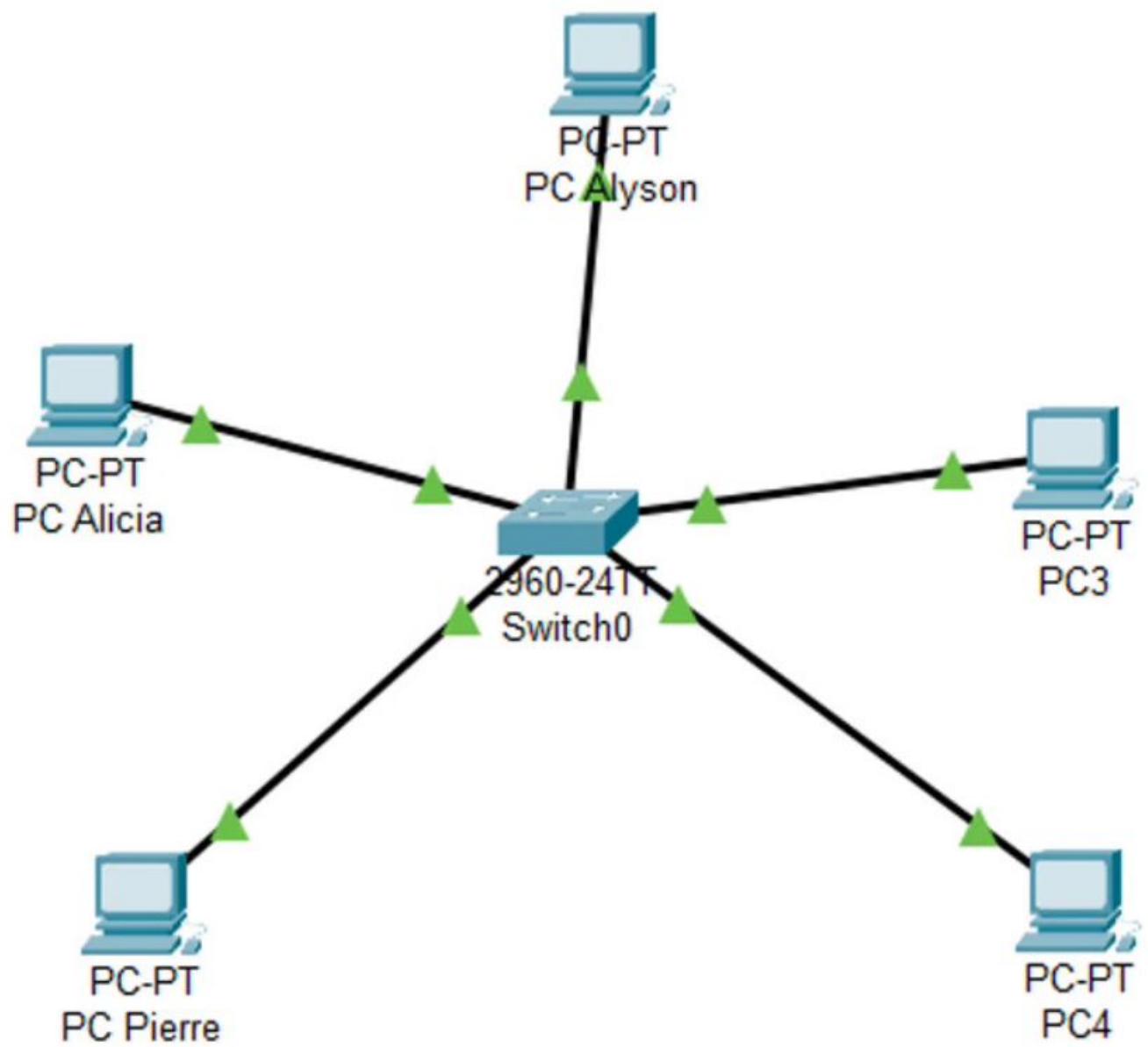
Pinging 192.168.1.1 with 32 bytes of data:

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),
```

Top

JOB 08



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



Hub (concentrateur)

Un hub est un appareil simple qui reçoit des bits (ou des symboles) d'un port et les envoie à tous les autres ports. Cela signifie que si un hôte envoie des informations à un autre hôte, tous les autres hôtes connectés au hub peuvent écouter ces informations. Cela peut poser des problèmes de sécurité. De plus, comme tous les appareils partagent la bande passante, le hub est en duplex semi, ce qui peut entraîner des conflits.



Switch (commutateur)

Contrairement au hub, le switch peut examiner les paquets de données et décider à quel port les envoyer. Cela signifie qu'il peut envoyer directement des informations d'un port à un autre sans affecter les autres ports. Par conséquent, le switch peut gérer efficacement le trafic réseau et améliorer les performances du réseau.

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

○ Avantages du Hub :

Comme le hub est directement connecté physiquement à la carte réseau de chaque appareil, le risque de perte de connexion est plus faible.

○ Inconvénients du Hub :

Comme tous les appareils partagent la bande passante, il peut y avoir des conflits. De plus, comme le hub se contente de diffuser les paquets reçus d'un port à tous les autres ports, le contenu qu'un hôte envoie à un autre hôte peut être écouté par d'autres hôtes non concernés, ce qui pose des problèmes de sécurité.



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

○ Avantages du Switch :

Le switch peut gérer efficacement le trafic réseau et améliorer les performances du réseau. Les paquets de données sont envoyés au port spécifié en fonction de l'adresse MAC, il n'y a pas de problème de sécurité lié à la diffusion aveugle du hub.

○ Inconvénients du Switch :

Je n'ai pas trouvé d'informations spécifiques sur les inconvénients du switch. Cependant, toute technologie a ses limites et peut poser des problèmes. Par exemple, dans certaines situations, si la configuration du réseau est incorrecte ou s'il y a une défaillance matérielle, le switch peut causer des problèmes de réseau.



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

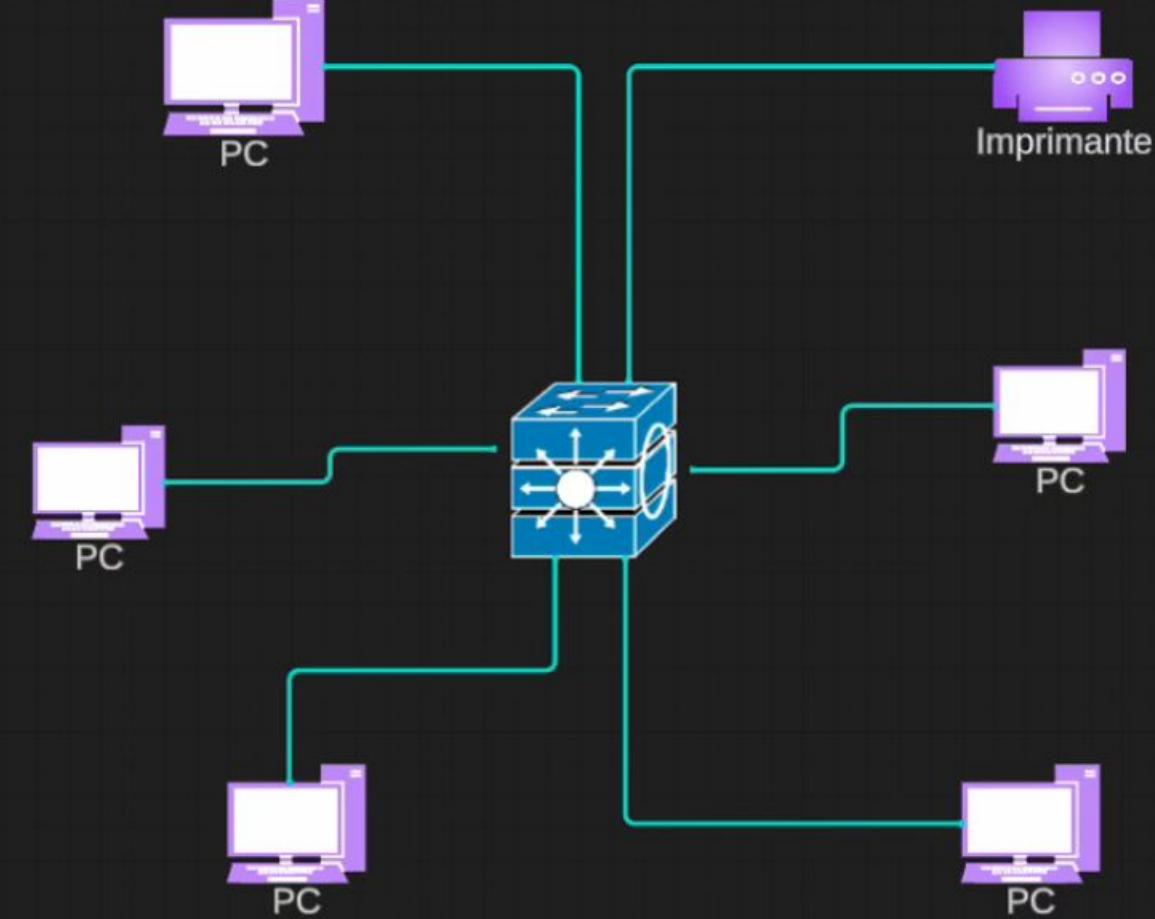
- Un switch, ou commutateur, est un élément clé dans la gestion du trafic réseau.
- un switch fonctionne de manière similaire à un switch physique Cisco.



Voici quelques points clés sur la façon dont un switch gère le trafic réseau:

- 🤖 Fonctions de base: Par défaut, un switch effectue des fonctions de base dans son état d'installation initiale. Il reçoit des informations de tous les appareils connectés, stocke ces informations et les transmet aux appareils appropriés sur le réseau.
- 🔧 Paramètres modifiables: Il existe plusieurs paramètres qu'un administrateur réseau peut modifier pour sécuriser et optimiser un réseau local. Par exemple, vous pouvez configurer les paramètres de base d'un commutateur de couche 2, configurer l'accès à distance sécurisé de votre commutateur, et plus encore.
- 🌐 Gestion des VLANs: Les VLANs (Virtual Local Area Networks) sont utilisés pour segmenter un réseau physique en plusieurs réseaux logiques. Ils peuvent aider à réduire les domaines de diffusion et améliorer la sécurité et les performances du réseau.
- 🔌 Configuration des interfaces: Pour être disponible, une interface doit être configurée avec au moins une adresse IP et être activée.
👤 La configuration précise peut varier en fonction du modèle spécifique du switch et des besoins spécifiques de votre réseau.

JOB 09



→ Pour réaliser un schéma de réseau :

1

Ajouter des appareils

Dans la zone des appareils en bas à gauche du logiciel, sélectionnez un Switch 2960 (commutateur) et les ordinateurs (PC) dont vous avez besoin, puis déployez-les dans la zone de travail.

2

Connecter les appareils

Utilisez un câble direct pour connecter chaque PC au Switch. Pour ce faire, connectez le port FastEthernet0 de chaque PC aux ports FastEthernet du Switch.

3

Configurer les adresses IP

Configurez une adresse IP, un masque de sous-réseau et une adresse de passerelle pour chaque PC. Il faut s'assurer que tous ces PC sont sur le même réseau.

4

Tester la

connectivité :

Vous pouvez tester la connectivité en envoyant un ping d'un PC à un autre à l'aide de la commande ping dans le terminal de chaque PC

→ identifiez au moins trois avantages importants d'avoir un schéma



Compréhension claire

- Un schéma de réseau donne une vue d'ensemble claire et concise de la façon dont votre réseau est configuré. Il montre comment les différents composants sont connectés et interagissent entre eux.



Dépannage

- Lorsqu'il y a des problèmes de réseau, le schéma de réseau peut aider à identifier rapidement où se situe le problème.



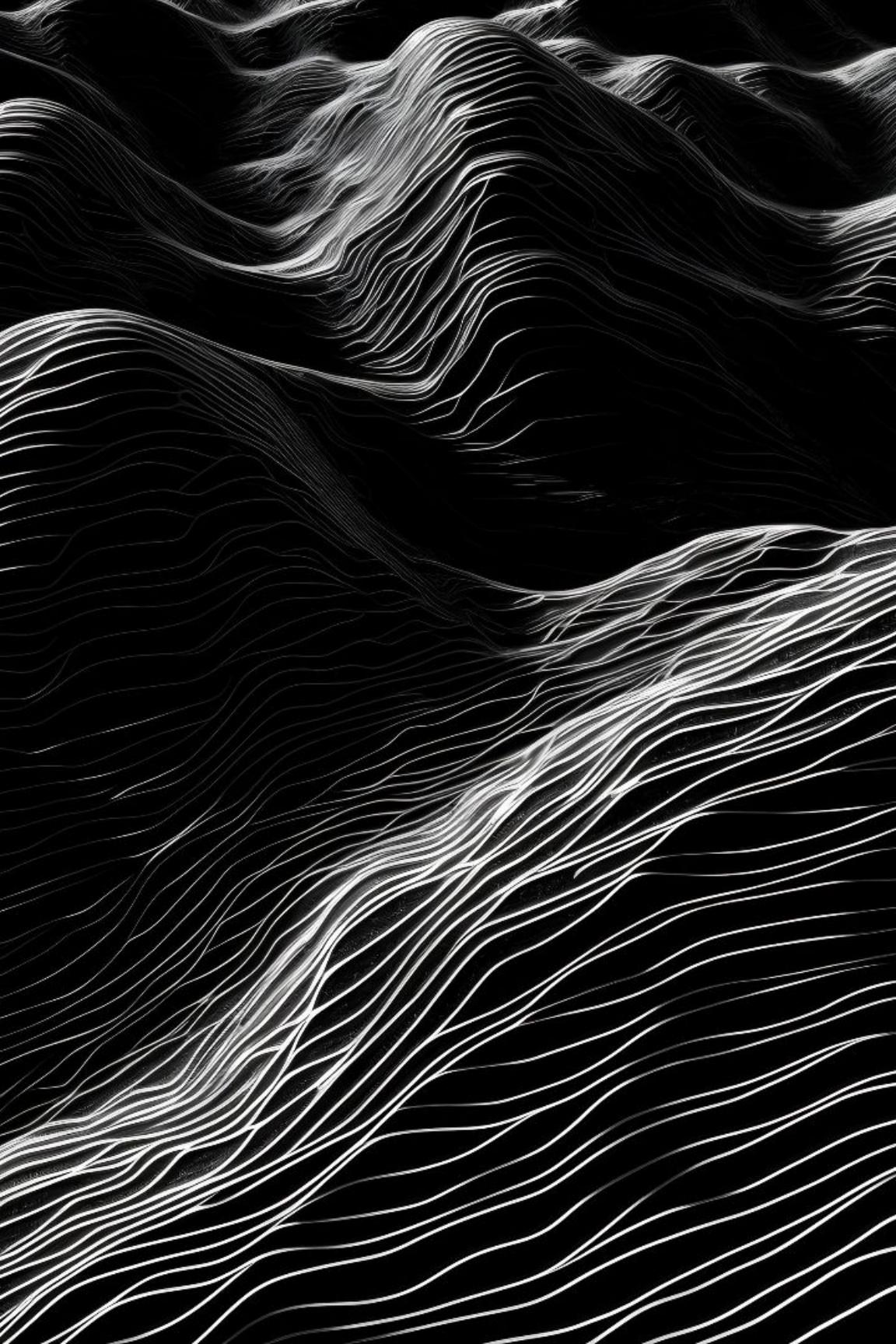
Planification et mise à niveau :

- Si vous prévoyez d'étendre ou de mettre à niveau votre réseau, le schéma de réseau peut aider à planifier ces modifications en montrant où les nouveaux composants peuvent être ajoutés ou comment les composants existants peuvent être réorganisés.

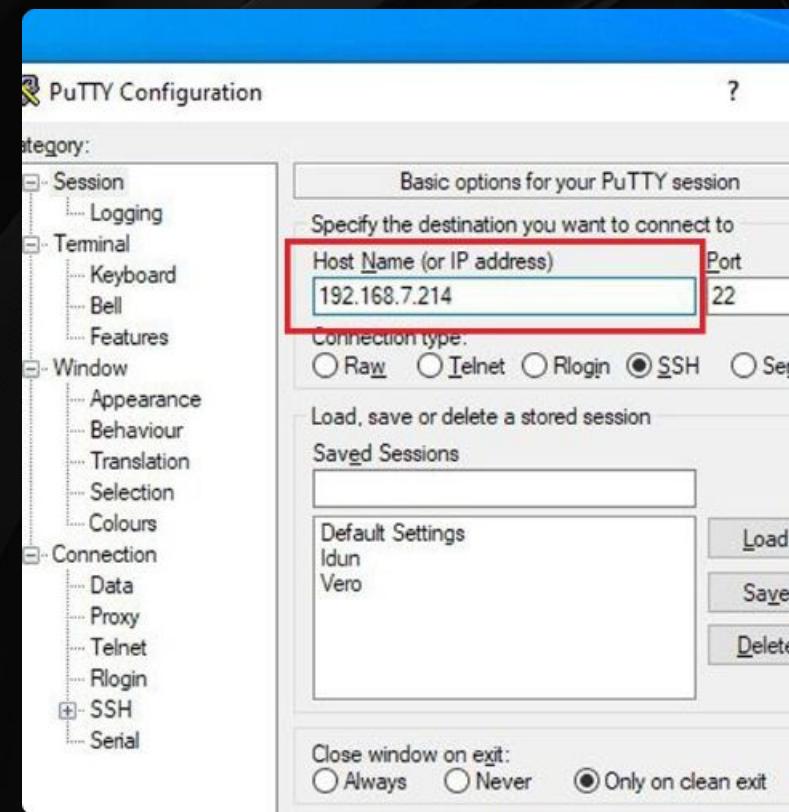
JOB 10

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

- Une adresse IP statique est une adresse fixe qui est manuellement attribuée à un appareil et qui ne change jamais.
- En revanche, une adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) est une adresse temporaire qui peut changer périodiquement. Le DHCP est un protocole qui attribue automatiquement des adresses IP aux appareils d'un réseau.

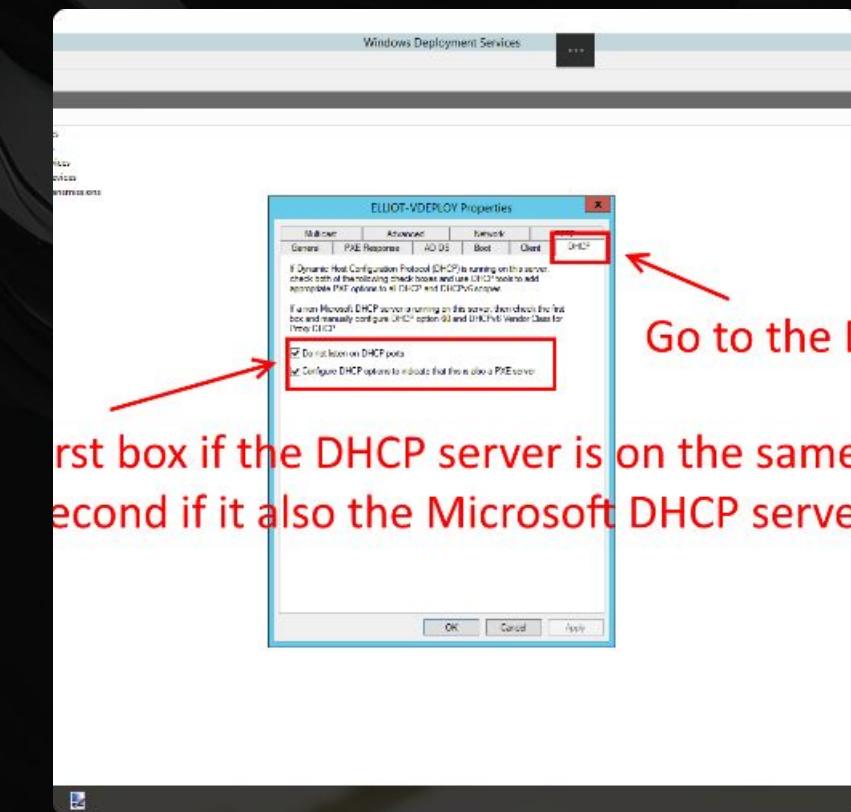


Voici quelques différences clés entre les deux :



Adresse IP statique

- Elle est généralement utilisée par des serveurs ou d'autres équipements importants. Une fois que votre appareil s'est vu attribuer une adresse IP statique, ce numéro reste généralement le même jusqu'à ce que l'appareil soit mis hors service ou que votre architecture réseau change.



Adresse IP attribuée par DHCP :

- La plupart des réseaux domestiques utilisent des adresses IP dynamiques, car ces adresses sont à la fois plus faciles à gérer et plus économiques pour les fournisseurs d'accès à Internet (FAI). Votre FAI dispose d'un service DHCP qui attribue automatiquement des adresses IP libres à partir d'une plage donnée

JOB 11

Network address	Network address	Cidr	Subnet address	No. of hosts	Address range	Broadcast address
10.0.0.0	255.255.255.2	28	10.1.0.0	14	10.1.0.1 to 10.1.0.14	10.1.0.15
10.0.0.0	255.255.255.2	27	10.2.0.0	30	10.2.0.1 to 10.2.0.30	10.2.0.31
10.0.0.0	255.255.255.2	27	10.3.0.0	30	10.3.0.1 to 10.3.0.30	10.3.0.31
10.0.0.0	255.255.255.2	27	10.4.0.0	30	10.4.0.1 to 10.4.0.30	10.4.0.31
10.0.0.0	255.255.255.2	27	10.5.0.0	30	10.5.0.1 to 10.5.0.30	10.5.0.31
10.0.0.0	255.255.255.2	27	10.6.0.0	30	10.6.0.1 to 10.6.0.30	10.6.0.31
10.0.0.0	255.255.255.1	25	10.7.0.0	12	10.7.0.1 to 10.7.0.126	10.7.0.127
		28		6		

<i>Network address</i>	<i>Network address</i>	<i>Cidr</i>	<i>Subnet address</i>	<i>No. of hosts</i>	<i>Address range</i>	<i>Broadcast address</i>
10.0.0.0	255.255.255.1	25	10.8.0.0	12	10.8.0.1 to 6	10.8.0.127
10.0.0.0	255.255.255.1	25	10.9.0.0	12	10.9.0.1 to 6	10.9.0.127
10.0.0.0	255.255.255.1	25	10.10.0.0	12	10.10.0.1 to 6	10.10.0.127
10.0.0.0	255.255.255.1	25	10.11.0.0	12	10.11.0.1 to 6	10.11.0.127
10.0.0.0	255.255.255.0	24	10.12.0.0	25	10.12.0.1 to 4	10.12.0.254
10.0.0.0	255.255.255.0	24	10.13.0.0	25	10.13.0.1 to 4	10.13.0.254
10.0.0.0	255.255.255.0	24	10.14.0.0	25	10.14.0.1 to 4	10.14.0.254
10.0.0.0	255.255.255.0	24	10.15.0.0	25	10.15.0.1 to 4	10.15.0.254
10.0.0.0	255.255.255.0	24	10.16.0.0	25	10.16.0.1 to 4	10.16.0.254

**→ créer 21 sous-réseaux à partir de l'adresse réseau de classe A 10.0.0.0.
Pour cela, nous devons d'abord déterminer le nombre de bits
nécessaires pour chaque sous-réseau**

1. Pour le sous-réseau de 12 hôtes, nous avons besoin de 4 bits ($2^4 = 16$, moins 2 pour l'adresse réseau et l'adresse de diffusion, ce qui donne 14 adresses disponibles, suffisantes pour 12 hôtes).
2. Pour les sous-réseaux de 30 hôtes, nous avons besoin de 5 bits ($2^5 = 32$, moins 2 donne 30 adresses disponibles).
3. Pour les sous-réseaux de 120 hôtes, nous avons besoin de 7 bits ($2^7 = 128$, moins 2 donne 126 adresses disponibles).
4. Pour les sous-réseaux de 160 hôtes, nous avons besoin de 8 bits ($2^8 = 256$, moins 2 donne 254 adresses disponibles).

→ **Sous-réseau de 12 hôtes :**

- Plage d'adresses : 10.0.0.0 à 10.0.0.15
- Masque de sous-réseau : 255.255.255.240

→ **Sous-réseaux de 30 hôtes :**

- 10.0.0.16 à 10.0.0.47
- 10.0.0.48 à 10.0.0.79
- 10.0.0.80 à 10.0.0.111
- 10.0.0.112 à 10.0.0.143
- 10.0.0.144 à 10.0.0.175
- Masque de sous-réseau : 255.255.255.224

→ Sous-réseaux de 120 hôtes :

- 10.0.0.176 à 10.0.0.303
- 10.0.0.304 à 10.0.0.431
- 10.0.0.432 à 10.0.0.559
- 10.0.0.560 à 10.0.0.687
- 10.0.0.688 à 10.0.0.815
- Masque de sous-réseau : 255.255.255.128

→ Sous-réseaux de 160 hôtes :

- 10.0.0.816 à 10.0.0.975
- 10.0.0.976 à 10.0.1.135
- 10.0.1.136 à 10.0.1.295
- 10.0.1.296 à 10.0.1.455
- 10.0.1.456 à 10.0.1.615
- Masque de sous-réseau : 255.255.255.0



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

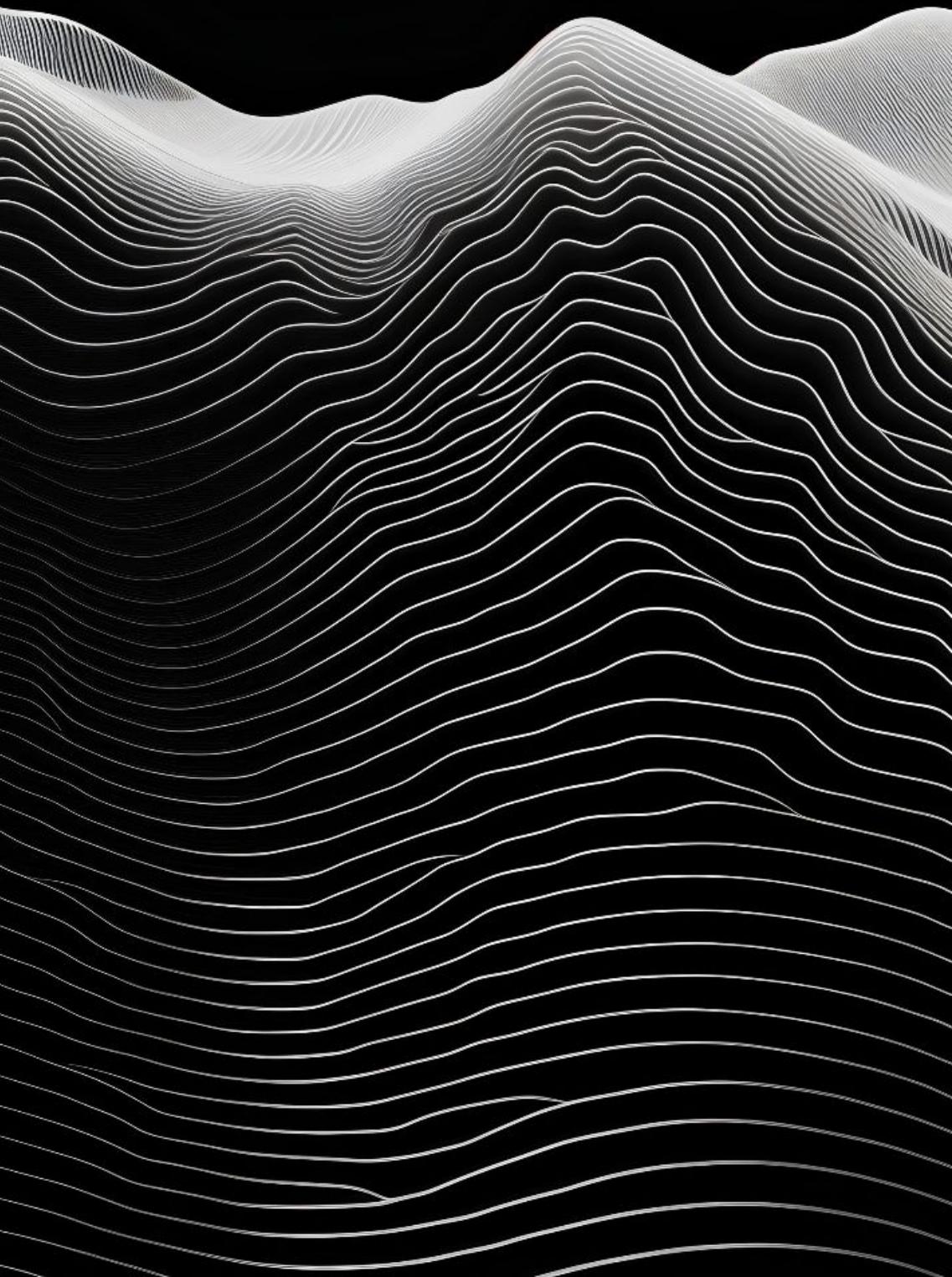
- On a choisi une adresse de classe A car elle offre un grand nombre d'adresses IP, ce qui est utile pour les grands réseaux.

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

- Les différents types d'adresses sont principalement les adresses de classe A, B et C, qui diffèrent par le nombre d'adresses IP qu'elles peuvent offrir et leur utilisation dans les petits, moyens et grands réseaux.

Job 12

- Le modèle OSI (Open Systems Interconnection) est une architecture en couches qui définit comment les données sont transmises d'un système à un autre. Chaque couche a une fonction spécifique à effectuer.

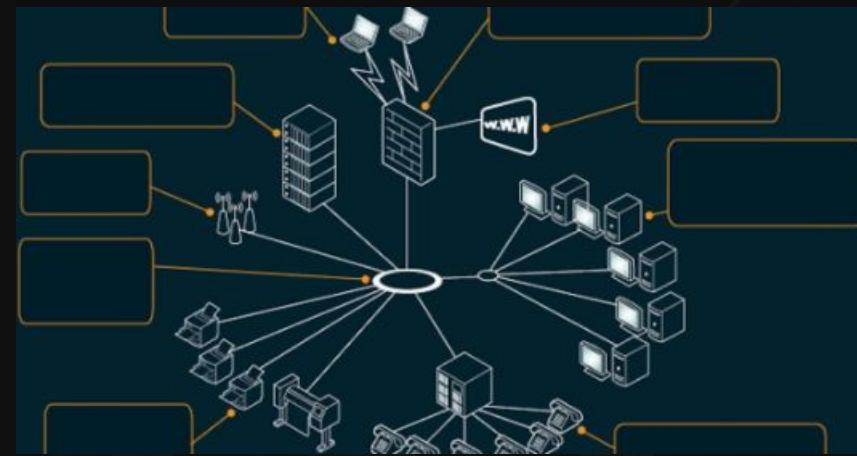


Voici un tableau décrivant les sept couches du modèle OSI et les protocoles/matériels associés :

Layer	Description	Protocols/Hardware
7.Application	Provides an interface for applications to access network services.	HTML, FTP
6.Prestation	Transforms data into a format that the receiving system can understand.	SSL/TLS
5.Session	Establishes, manages, and terminates connections between local and remote applications.	PPTP
4.Transport	Provides reliable end-to-end data transfer.	TCP, UDP
3.Network	Determines the best way to route data packets to their destination.	IPv4, IPv6, Router
2.Data Link	Provides data transfer from one node to another and regulates the flow of data between systems.	Ethernet, MAC, Wi-Fi
1.Physical	Transmits raw bits over the physical communication medium.	Optical Fiber, RJ45 Cable

JOB 13

→ Quelle est l'architecture de ce réseau ?



- Ce réseau est basé sur une architecture de classe C12. Le masque de sous-réseau 255.255.255.0 indique que les trois premiers octets (192.168.10) représentent l'identifiant du réseau et le dernier octet représente l'identifiant de l'hôte au sein du réseau.

→ Indiquer quelle est l'adresse IP du réseau ?



- L'adresse IP du réseau est déterminée en appliquant le masque de sous-réseau à n'importe quelle adresse IP du réseau. Dans ce cas, l'adresse IP du réseau est 192.168.10.03

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

- Nombre de machines pouvant être connectées à ce réseau : Avec un masque de sous-réseau de 255.255.255.0, nous avons 8 bits pour les adresses d'hôtes, ce qui signifie que nous pouvons avoir
 - $2^8=256$
- adresses IP . Cependant, deux de ces adresses sont réservées : l'adresse du réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255). Par conséquent, le nombre maximal de machines qui peuvent être connectées à ce réseau est de
 - $256-2=254$



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

- Adresse de diffusion du réseau : L'adresse de diffusion est généralement la dernière adresse IP valide dans un sous-réseau. Dans ce cas, l'adresse de diffusion serait 192.168.10.2555.

JOB 14

- 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

JOB 15

→ Qu'est-ce que le routage ?



- Le routage est le processus de sélection d'un chemin à travers un ou plusieurs réseaux. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP (Internet Protocol) pour se rendre de leur origine à leur destination.

→ Qu'est-ce qu'un gateway ?



- Une gateway, ou passerelle en français, désigne en informatique un dispositif matériel et logiciel qui permet de relier deux réseaux informatiques, ou deux réseaux de télécommunications, aux caractéristiques différentes. La plupart du temps, la passerelle applicative a pour mission de relier un réseau local à Internet.

→ Qu'est-ce qu'un VPN ?

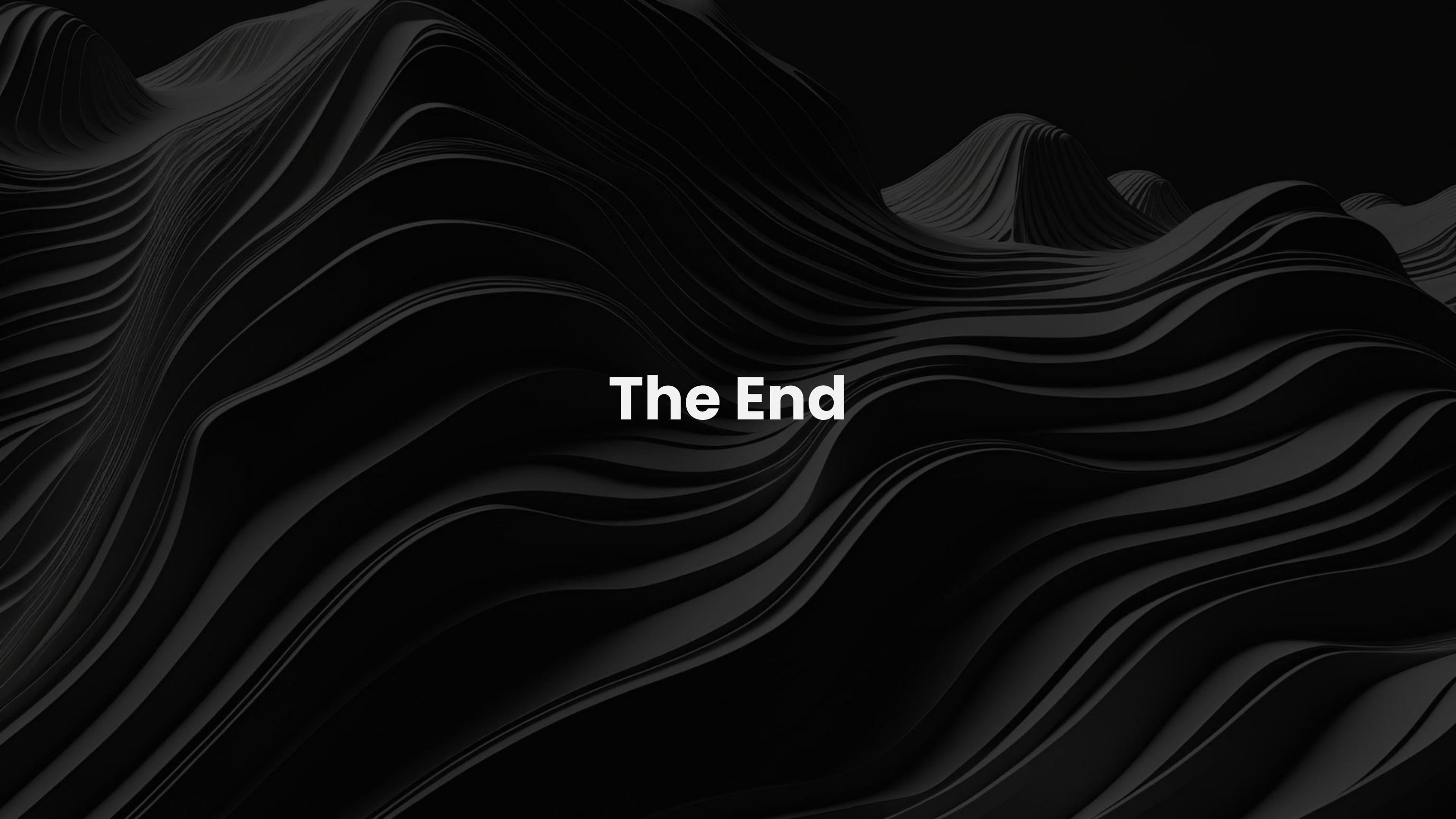


- VPN est l'abréviation de « Virtual Private Network » (réseau privé virtuel). Il s'agit d'un service qui vous aide à préserver votre confidentialité en ligne en chiffrant la connexion entre votre appareil et Internet. Cette connexion sécurisée fournit un tunnel privé pour vos données et communications lorsque vous utilisez des réseaux publics.

→ Qu'est-ce qu'un DNS ?



- Le système de noms de domaine (DNS, Domain Name System) est la méthode par laquelle une adresse IP (Internet Protocol), un ensemble de chiffres (173.194.39.78), est convertie sur un ordinateur ou un autre dispositif connecté en un nom de domaine lisible par l'homme

The background of the image is a dark, almost black, surface with a complex, organic texture. It features numerous fine, light-colored, wavy lines that create a sense of depth and motion, resembling ripples in water or folds in fabric. These lines are more concentrated in the center and become more sparse towards the edges.

The End