

Job 2:

→ Qu'est qu'un réseau ?

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations.

→ À quoi sert un réseau informatique ?

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil.

→ Quel matériel avons-nous besoin pour construire un réseau ?

Détaillez les fonctions de chaque pièce.

Concentrateur (hub)

Commutateur (switch)

Routeur

Pont (bridge)

Passerelle (gateway)

Modem

Répéteur

Point d'accès

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 câbles de connexion. Le concentrateur est le plus simple de la famille des équipements de connexion réseau, car il connecte des composants LAN ayant des protocoles identiques.

Un concentrateur peut fonctionner avec des données numériques et analogiques, à condition que ses paramètres soient configurés de manière à préparer le formatage des données entrantes. Si, par exemple, les données entrantes sont au format numérique, le concentrateur doit les transmettre sous forme de paquets ; mais si les données entrantes sont analogiques, le concentrateur les transmet sous forme de signal.

Les concentrateurs ne remplissent pas de fonctions de filtrage ou d'adressage de paquets ; ils envoient simplement des paquets de données à tous les

appareils connectés. Les concentrateurs opèrent au niveau de la couche Physique du modèle d'interconnexion des systèmes ouverts (OSI). Il existe deux types de concentrateurs : à port simple et multiport.

Commutateur (switch)

Les commutateurs jouent généralement un rôle plus intelligent que les concentrateurs. Un commutateur est un dispositif multiport qui améliore l'efficacité du réseau. Le commutateur gère des informations de routage limitées sur les nœuds du réseau interne et permet des connexions à des systèmes tels que les concentrateurs ou les routeurs. Les brins des réseaux locaux sont généralement connectés à l'aide de commutateurs. En général, les commutateurs peuvent lire les adresses matérielles des paquets entrants afin de les transmettre à la destination appropriée.

L'utilisation de commutateurs améliore l'efficacité du réseau par rapport aux concentrateurs ou aux routeurs, en raison de leur capacité à créer des circuits virtuels. Les commutateurs améliorent également la sécurité du réseau, car les circuits virtuels sont plus difficiles à examiner avec des moniteurs réseau. Vous pouvez considérer un commutateur comme un dispositif qui possède une combinaison de certaines des capacités les plus intéressantes des routeurs et des concentrateurs. Un commutateur peut opérer soit sur la couche Liaison de données, soit sur la couche Réseau du modèle OSI. Un commutateur multicouche est un commutateur qui peut fonctionner sur les deux couches, ce qui signifie qu'il peut servir à la fois de commutateur et de routeur. Un commutateur multicouche est un équipement hautes performances prenant en charge les mêmes protocoles de routage que les routeurs.

Les commutateurs peuvent faire l'objet d'attaques par déni de service distribué (DDoS) ; des systèmes de prévention des attaques par saturation sont utilisés pour empêcher le trafic malveillant d'arrêter le commutateur. La sécurité des ports des commutateurs est importante, veillez à sécuriser vos commutateurs : Désactivez tous les ports inutilisés et utilisez l'espionnage DHCP, l'inspection ARP et le filtrage des adresses MAC.

Routeur

Les routeurs contribuent à transmettre des paquets vers leurs destinations en traçant un chemin dans l'océan des équipements réseau interconnectés, à l'aide de différentes topologies de réseau. Les routeurs sont des appareils intelligents qui stockent des informations sur les réseaux auxquels ils sont

connectés. La plupart des routeurs peuvent être configurés de manière à fonctionner comme pare-feu à filtrage de paquets et utilisent des listes de contrôle des accès (ACL). Les routeurs, conjointement avec une unité de service de canal/unité de service de données (CSU/DSU), servent également à traduire le tramage LAN en tramage WAN. Ceci est nécessaire car les réseaux locaux (LAN) et les réseaux étendus (WAN) utilisent des protocoles différents. De tels routeurs sont appelés routeurs frontière. Ils assurent la connexion externe d'un réseau local à un réseau étendu, et ils fonctionnent à la frontière de votre réseau.

Les routeurs servent également à scinder les réseaux internes en deux ou plusieurs sous-réseaux. Il est également possible de connecter des routeurs en interne à d'autres routeurs, pour créer des zones qui opèrent indépendamment les unes des autres. Les routeurs établissent la communication en gérant des tables sur les destinations et les connexions locales. Un routeur contient des informations sur les systèmes qui y sont connectés et sur la destination des requêtes à envoyer si celle-ci n'est pas connue. Les routeurs communiquent généralement les informations de routage et autres en utilisant l'un des trois protocoles standard : le protocole d'informations de routage (RIP), le protocole de passerelle frontière (BGP) ou le chemin le plus court ouvert en premier (OSPF).

Les routeurs sont votre première ligne de défense et doivent être configurés de manière à ne transmettre que le trafic autorisé par les administrateurs réseau. Les routages eux-mêmes peuvent être configurés comme statiques ou dynamiques. S'ils sont statiques, ils ne peuvent être configurés que manuellement et restent ainsi jusqu'à ce qu'ils soient modifiés. S'ils sont dynamiques, les routeurs apprennent l'existence des autres routeurs de leur environnement et utilisent les informations sur ceux-ci pour élaborer leurs tables de routage.

Les routeurs sont des appareils universels qui interconnectent deux ou plusieurs réseaux hétérogènes. Ils sont généralement dédiés à des ordinateurs spécialisés et dotés d'interfaces réseau entrée et sortie séparées pour chaque réseau connecté. Les routeurs et les passerelles constituant la colonne vertébrale des grands réseaux informatiques comme Internet, ils possèdent des caractéristiques spéciales qui leur donnent la souplesse et la capacité de s'adapter aux différents systèmes d'adressage réseau et tailles de trame en segmentant les gros paquets en plus petits, adaptés aux nouveaux composants réseau. Chaque interface de routeur possède son propre

protocole de résolution d'adresses (ARP), sa propre adresse LAN (adresse de carte réseau) et sa propre adresse IP (protocole Internet). Le routeur, grâce à une table de routage, connaît les itinéraires qu'un paquet peut prendre de sa source à sa destination. La table de routage, comme pour le pont et le commutateur, se développe de manière dynamique. Dès réception d'un paquet, le routeur supprime son en-tête et son trailer, puis analyse l'en-tête IP en déterminant les adresses source et destination et le type de données, et en notant l'heure de réception. Il met également à jour la table de routage avec de nouvelles adresses qui n'y figurent pas déjà. L'en-tête IP et les informations d'heure d'arrivée sont entrées dans la table de routage. Les routeurs opèrent normalement au niveau de la couche Réseau du modèle OSI.

Pont (bridge)

Les ponts servent à connecter deux ou plusieurs hôtes ou segments de réseau. Le rôle fondamental des ponts dans l'architecture réseau est de stocker et de transférer les trames entre les différents segments qu'ils relient. Ils utilisent les adresses MAC (contrôle d'accès au support) des équipements pour le transfert des trames. En examinant l'adresse MAC des appareils connectés à chaque segment, les ponts peuvent transmettre les données ou les empêcher de traverser. Les ponts peuvent également être utilisés pour connecter deux réseaux locaux physiques en un réseau local logique plus grand.

Les ponts ne fonctionnent qu'au niveau des couches Physique et Liaison de données du modèle OSI. Les ponts servent à scinder les grands réseaux en sections plus petites en se plaçant entre deux segments de réseau physique et en gérant le flux des données entre les deux.

Les ponts ressemblent aux concentrateurs à bien des égards, y compris le fait qu'ils relient des composants LAN ayant des protocoles identiques. Cependant, les ponts filtrent les paquets de données entrants, appelés trames, d'après leurs adresses avant de les transmettre. Alors qu'ils filtrent les paquets de données, les ponts n'apportent aucune modification au format ni au contenu des données entrantes. Les ponts filtrent et transfèrent les trames dans le réseau à l'aide d'une table de pont dynamique. Cette table de pont, qui est initialement vide, gère les adresses LAN de chaque ordinateur du réseau local et les adresses de chaque interface de pont qui relie le réseau local aux autres réseaux locaux. Les ponts, comme les concentrateurs, peuvent être à port simple ou multiple.

Les ponts sont largement tombés en désuétude ces dernières années et ont été remplacés par des commutateurs, qui offrent plus de fonctionnalités. De fait, les commutateurs sont parfois appelés « ponts multiports » en raison de leur mode de fonctionnement.

Passerelle (gateway)

Les passerelles opèrent généralement au niveau des couches Transport et Session du modèle OSI. Au niveau de la couche Transport et des couches supérieures, de nombreux protocoles et standards issus de différents fournisseurs sont utilisés ; les passerelles servent à les gérer. Les passerelles assurent la traduction entre des technologies réseau telles que l'interconnexion des systèmes ouverts (OSI) et TCP/IP (protocole de contrôle de transmission/protocole Internet). Ainsi, les passerelles connectent deux ou plusieurs réseaux autonomes, chacun ayant ses propres algorithmes de routage, protocoles, topologie, service de noms de domaine, procédures et politiques d'administration réseau.

Les passerelles remplissent toutes les fonctions des routeurs et plus encore. En fait, un routeur doté d'une fonctionnalité supplémentaire de traduction est une passerelle. La fonction qui assure la traduction entre les différentes technologies de réseau s'appelle un convertisseur de protocole.

Modem

Les modems (modulateurs-démodulateurs) servent à transmettre des signaux numériques via des lignes téléphoniques analogiques. Les signaux numériques sont donc convertis par le modem en signaux analogiques de différentes fréquences et transmis à un autre modem au lieu de réception. Le modem récepteur effectue la transformation inverse et fournit une sortie numérique au dispositif qui y est connecté, généralement un ordinateur. Les données numériques sont habituellement transférées vers/depuis le modem via une liaison série et une interface standard RS-232. De nombreuses compagnies téléphoniques offrent des services DSL et de nombreux câblo-opérateurs utilisent des modems comme terminaux finaux pour l'identification et la reconnaissance des utilisateurs individuels. Les modems opèrent à la fois sur les couches Physique et Liaison de données.

Répéteur

Un répéteur est un appareil électronique qui amplifie le signal qu'il reçoit. Vous pouvez considérer un répéteur comme un appareil qui reçoit un signal et le

retransmet à un niveau plus élevé ou à une puissance supérieure, afin qu'il puisse couvrir de plus longues distances, plus de 100 mètres pour les câbles LAN standard. Les répéteurs opèrent sur la couche Physique.

Point d'accès

Même si un point d'accès peut techniquement comporter une connexion câblée ou sans fil, il s'agit généralement d'un dispositif sans fil. Un point d'accès fonctionne au niveau de la deuxième couche OSI, la couche Liaison de données, et il peut fonctionner soit comme un pont reliant un réseau câblé standard à des appareils sans fil ou comme un routeur transmettant des données d'un point d'accès à un autre.

Les points d'accès sans fil (WAP) se composent d'un émetteur et d'un récepteur, qui permettent de créer un réseau local sans fil (WLAN). Les points d'accès sont généralement des équipements réseau distincts dotés d'une antenne, d'un émetteur et d'un adaptateur intégrés. Les points d'accès utilisent le mode réseau d'infrastructure sans fil pour fournir un point de connexion entre les réseaux locaux sans fil (WLAN) et un réseau local Ethernet câblé. Ils disposent également de plusieurs ports, ce qui vous permet d'étendre le réseau afin de prendre en charge des clients supplémentaires. Selon la taille du réseau, un ou plusieurs points d'accès peuvent être nécessaires pour assurer une couverture complète. Des points d'accès supplémentaires permettent d'accéder à un plus grand nombre de clients sans fil et d'étendre la portée du réseau sans fil. Chaque point d'accès est limité par sa portée de transmission : la distance à laquelle un client peut se trouver du point d'accès tout en obtenant un signal utilisable et une vitesse de traitement des données exploitable. La distance réelle dépend du standard sans fil, des obstacles et des conditions environnementales entre le client et le point d'accès. Les points d'accès haut de gamme sont équipés d'antennes haute puissance, grâce auxquelles ils peuvent étendre la portée du signal sans fil.

Les points d'accès peuvent également fournir de nombreux ports qui permettent d'augmenter la taille du réseau, les capacités du pare-feu et le service DHCP (protocole de configuration dynamique des hôtes). Nous avons donc des points d'accès qui sont à la fois un commutateur, un serveur DHCP, un routeur et un pare-feu.

Pour vous connecter à un point d'accès sans fil, il vous faut un SSID (identifiant d'ensemble de services). Les réseaux sans fil 802.11 utilisent le

SSID pour identifier tous les systèmes appartenant au même réseau, et les postes clients doivent être configurés avec le SSID pour être authentifiés par le point d'accès. Le point d'accès peut diffuser le SSID, ce qui permet à tous les clients sans fil de la zone de voir son SSID. Cependant, pour des raisons de sécurité, les points d'accès peuvent être configurés de manière à ne pas diffuser le SSID, ce qui signifie qu'un administrateur doit donner le SSID aux systèmes clients au lieu d'autoriser sa découverte automatique. Les appareils sans fil sont livrés avec des SSID par défaut, des paramètres de sécurité par défaut, des canaux par défaut, des mots de passe par défaut et des noms d'utilisateur par défaut. Pour des raisons de sécurité, il est fortement recommandé de modifier ces paramètres dès que possible, car de nombreux sites Internet répertorient les paramètres par défaut des fabricants.

Les points d'accès peuvent être « légers » ou « lourds ». Les points d'accès lourds, aussi appelés points d'accès autonomes, doivent être configurés manuellement avec les paramètres de réseau et de sécurité ; ensuite, ils fonctionnent globalement tout seuls et servent les clients jusqu'à ce qu'ils ne puissent plus fonctionner. Les points d'accès légers peuvent être configurés à distance à l'aide d'un contrôleur. Comme les clients légers ne nécessitent pas d'être configurés manuellement, ils peuvent être facilement reconfigurés et surveillés. Les points d'accès peuvent dépendre d'un contrôleur ou être autonomes.

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

j'ai choisi un câble croisé.

Un câble croisé (copper cross-over) est utilisé pour relier directement deux dispositifs similaires sans avoir besoin d'un équipement intermédiaire comme un commutateur ou un routeur.

Dans un câble croisé, les fils utilisés pour la transmission de données sur un bout sont connectés aux fils utilisés pour la réception de données sur l'autre bout, et vice-versa. Cela permet aux PC de communiquer directement entre eux.

Les ordinateurs, lorsqu'ils utilisent des câbles Ethernet standard (non croisés), s'attendent à envoyer des données sur certains fils et à recevoir des données sur d'autres fils. Si vous essayez de connecter deux PC avec un câble standard, ils essaieront tous les deux d'émettre sur les mêmes fils et de

recevoir sur les mêmes fils, ce qui entraîne des collisions et l'absence de communication. Les câbles croisés résout ce problème en "croisant" les fils d'émission et de réception.

Cependant, il convient de noter que de nombreux équipements modernes, y compris les cartes réseau sur les ordinateurs récents, sont équipés de la fonctionnalité "Auto MDI/MDI-X". Cela leur permet de détecter automatiquement le type de câble et de configurer leur ports en conséquence, rendant parfois le câble croisé, obsolète pour de telles connexions. Mais dans les situations où l'équipement ne dispose pas de cette fonctionnalité, un câble croisé reste essentiel pour connecter directement deux PC.

Conclusion

Une bonne connaissance des types d'équipements réseau existants vous permet de concevoir et de construire un réseau sécurisé et bien adapté à votre organisation. Toutefois, pour garantir en permanence la sécurité et la disponibilité de votre réseau, vous devez surveiller attentivement vos équipements réseau et les activités qui les concernent, afin de détecter rapidement les problèmes de matériel ou de configuration et les attaques.

Job 4:

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet Protocol.

→ À quoi sert un IP ?

Concrètement, ce matricule sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet.

→ Qu'est-ce qu'une adresse MAC ?

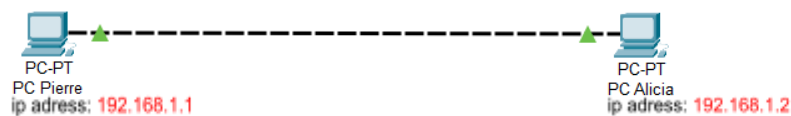
L'adresse MAC (pour Media Access Control) est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est sensée être unique au monde. On peut donc considérer qu'elle constitue une sorte de plaque d'immatriculation des appareils électroniques.

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

Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

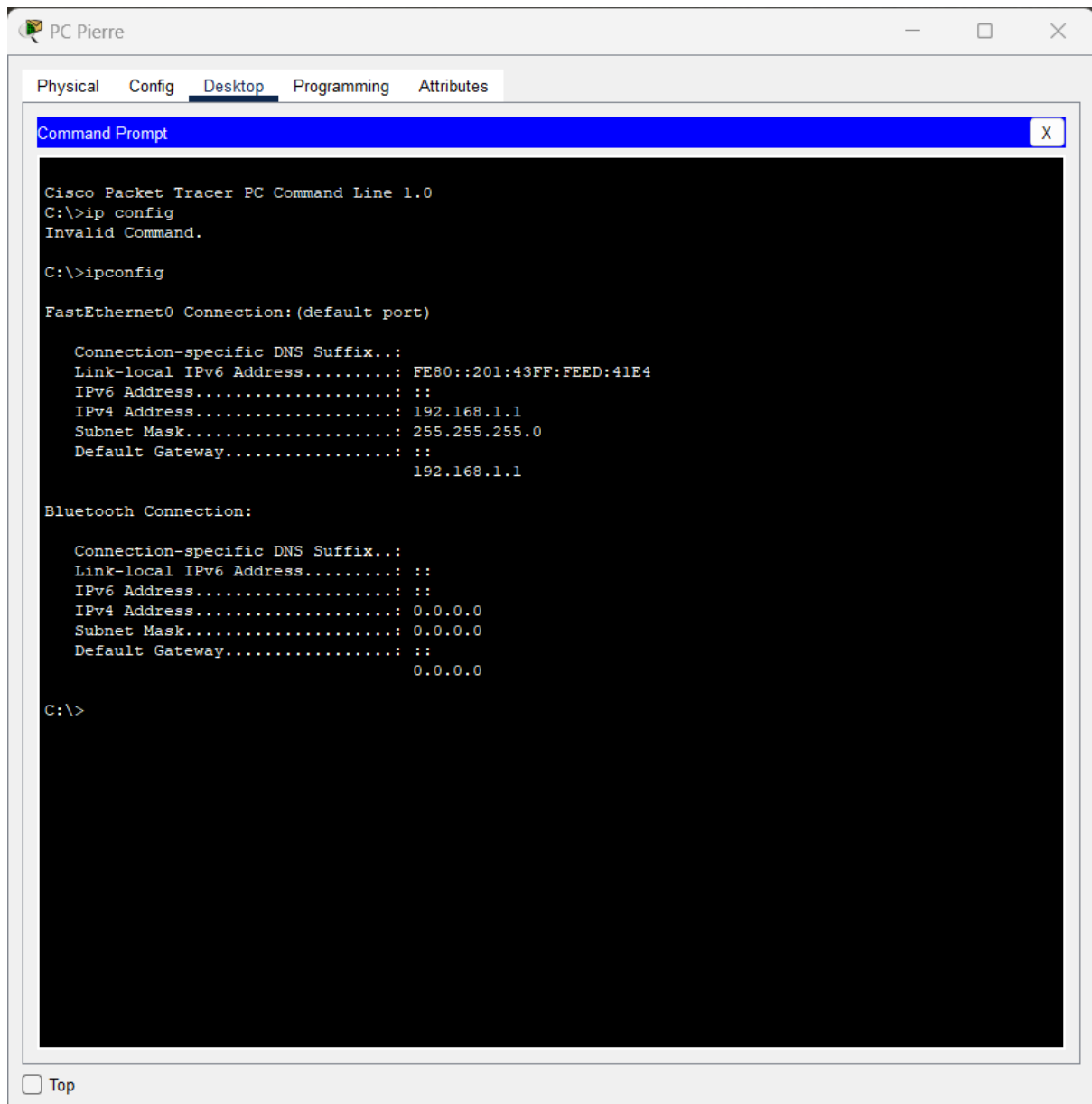
→ Quelle est l'adresse de ce réseau ?

Une adresse réseau est un nombre de 32 bits. Il identifie de manière unique un hôte (ordinateur ou autre appareil, tel qu'une imprimante ou un routeur) sur un réseau TCP/IP. Les adresses IP sont généralement exprimées au format décimal en pointillés, avec quatre nombres séparés par des points
Exemple: 192.168.123.132.

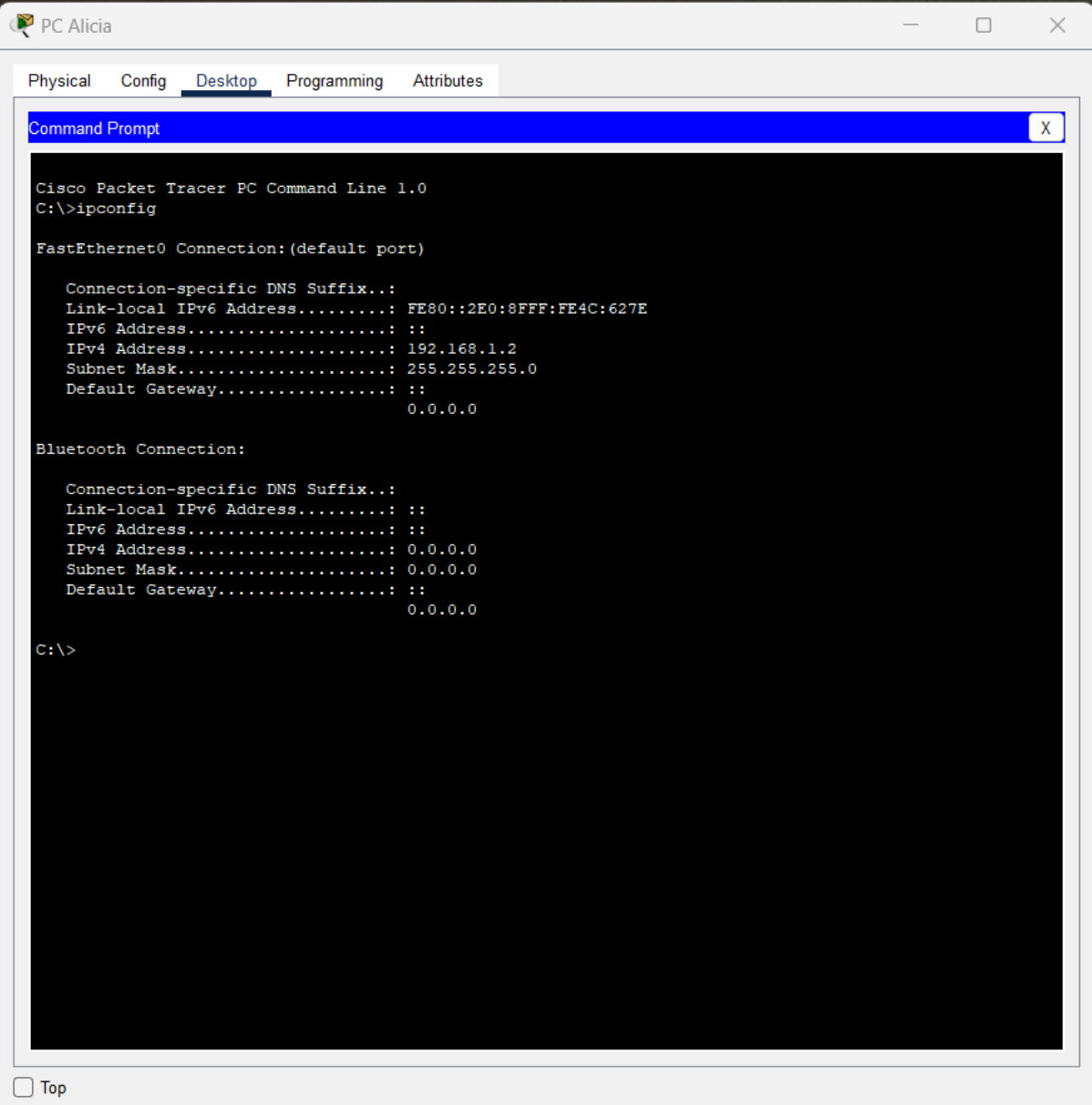


Job 5:

pierre:



Alicia:



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:8FFF:FE4C:627E
    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 . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

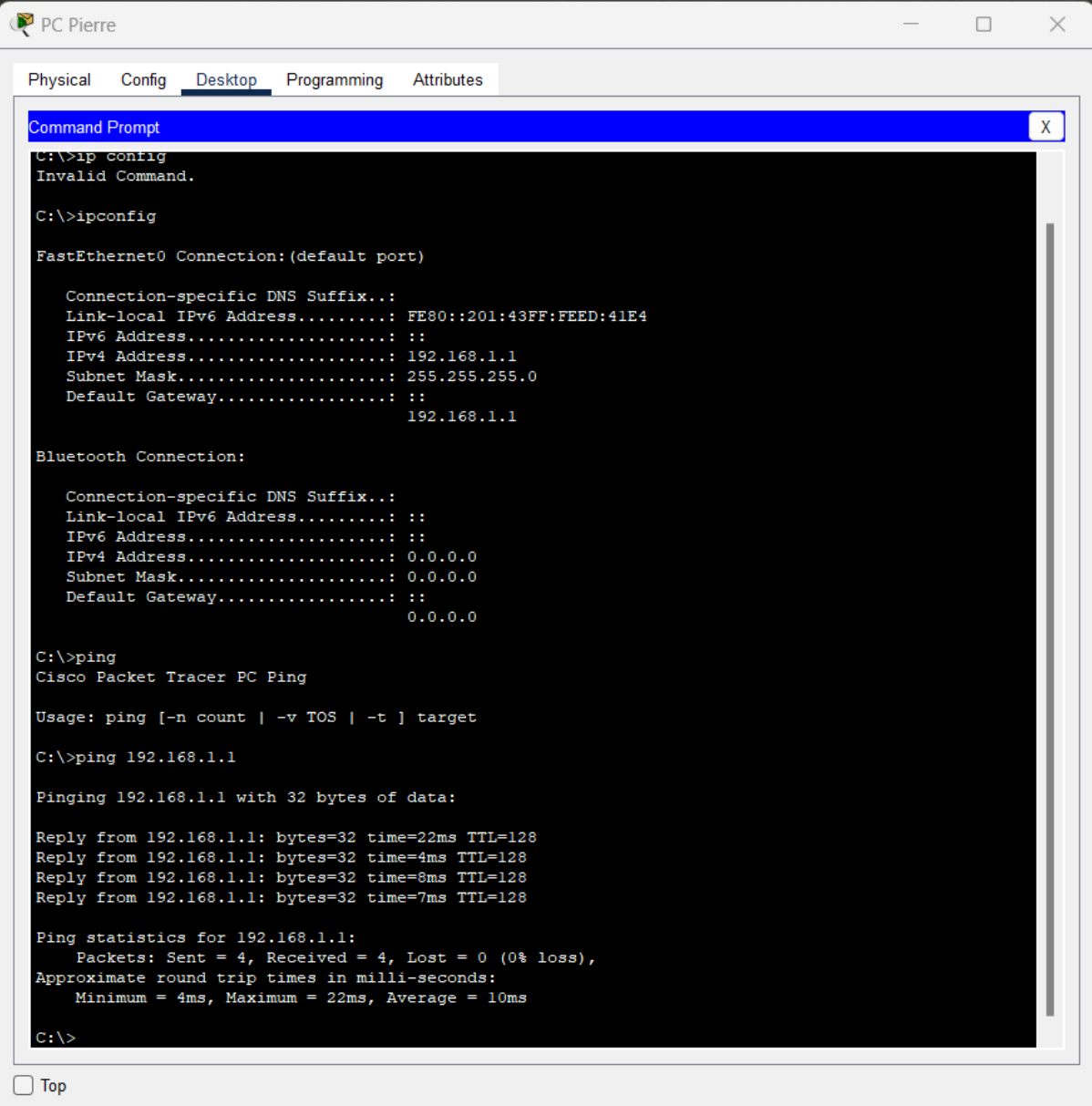
C:\>
```

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

dans command prompt la commande a noté est: ipconfig

Job 6:

Pierre:



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ip config
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:43FF:FEED:41E4
    IPv6 Address . . . . .: ::
    IPv4 Address. . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.1.1

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:\>ping
Cisco Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

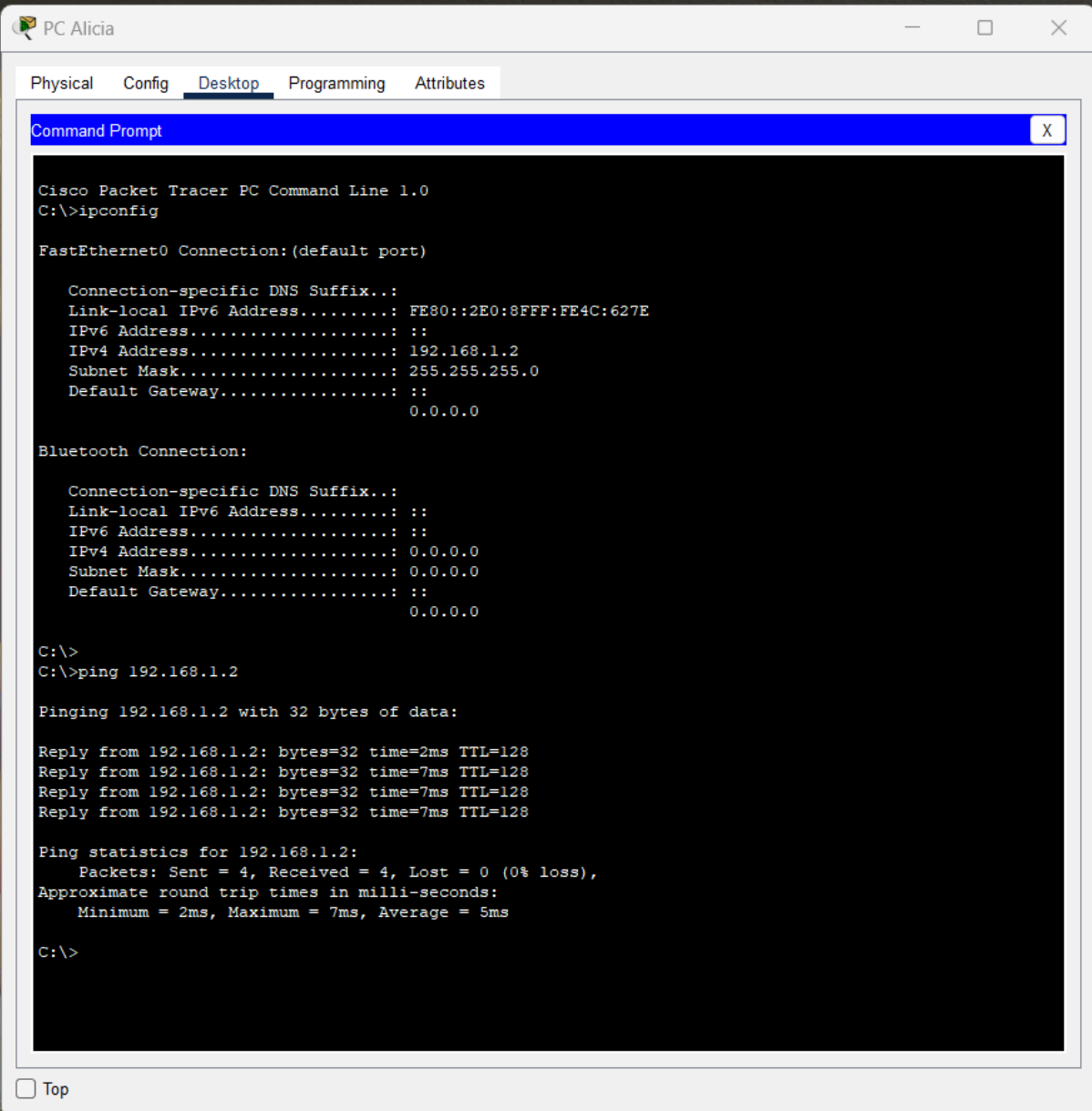
Reply from 192.168.1.1: bytes=32 time=22ms TTL=128
Reply from 192.168.1.1: bytes=32 time=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=8ms TTL=128
Reply from 192.168.1.1: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 22ms, Average = 10ms

C:\>
```

☐ Top

Alicia:



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt X
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:8FFF:FE4C:627E
    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 . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

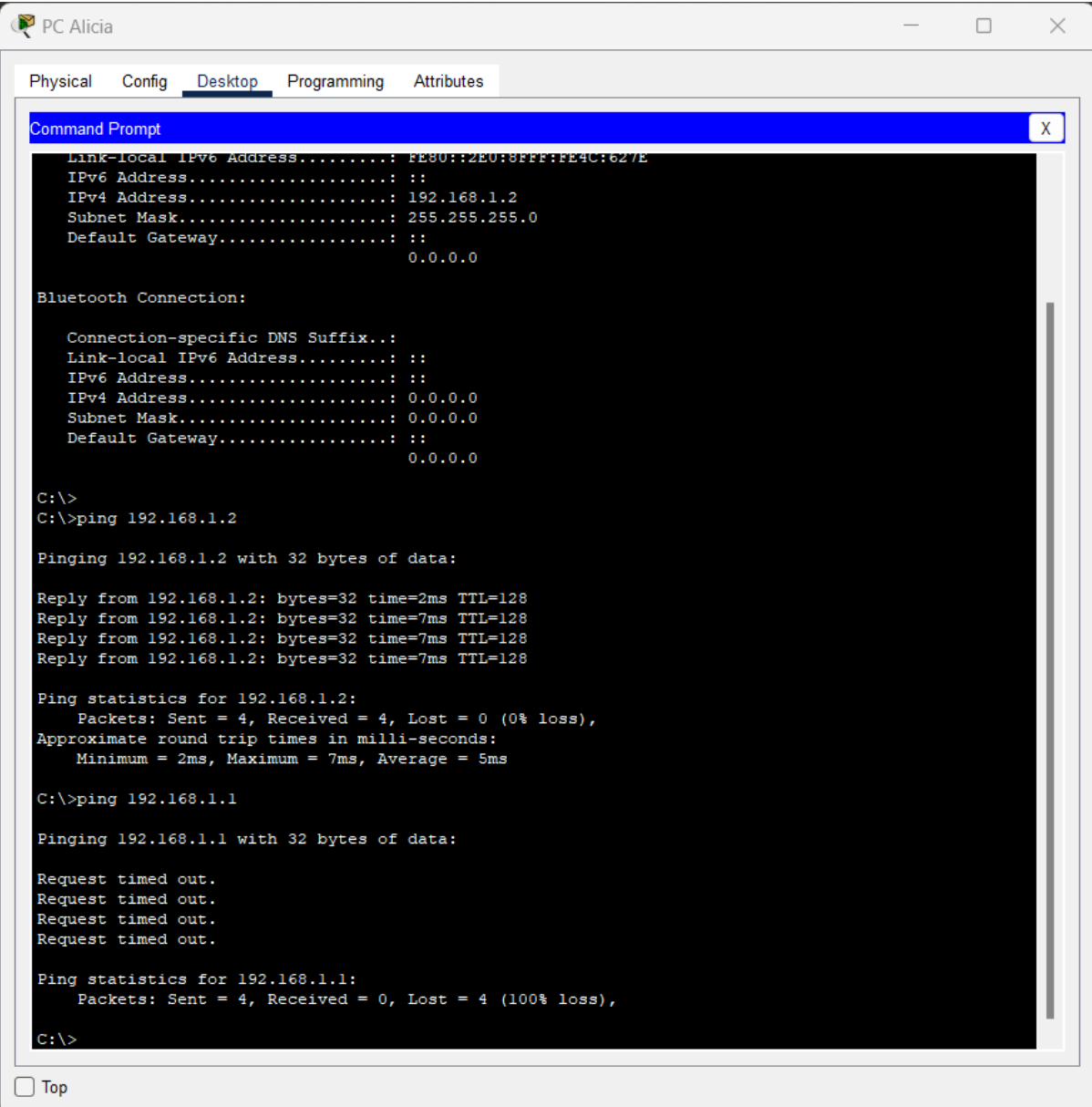
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 5ms

C:\>
```

→ Quelle est la commande permettant de Ping entre des PC ?
la commande est: ping + adress ip
ex: ping 192.168.1.1

Job 7:



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt
Link-local IPv6 Address.....: FE80::2E0:8FFF:FE4C:627E
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.....: ::
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::
0.0.0.0

C:\>
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=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms 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 = 2ms, Maximum = 7ms, Average = 5ms

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:\>
```

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

Non pierre n'a reçu aucun paquets envoyés par Alicia il est même précisé sur le terminal

Packets; Sent=4, Received=0, Lost=4 (100% loss).

Ce qui signifie que 4 paquets avaient été envoyer par Alicia, que Pierre en a bien reçu 0 et qu'il en a perdu 4 paquets.

→ Expliquez pourquoi.

Car Pierre a le PC éteint, ce qui amène à couper les fils du réseau entre Pierre et Alicia et aussi cela pour cause une adresse IP "muette".

Job 8:

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

La grande différence entre le hub et le switch informatique est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée tandis que Le commutateur effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

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

Un hub, dans le domaine des réseaux informatiques, est un dispositif matériel utilisé pour connecter plusieurs appareils électroniques au sein d'un réseau local. Voici comment il fonctionne, ainsi que ses avantages et inconvénients :

Fonctionnement d'un hub:

1. Connexion multiple : Un hub possède plusieurs ports permettant de connecter plusieurs appareils, tels que des ordinateurs, des imprimantes, des scanners, etc.
2. Diffusion des données: Lorsqu'un appareil envoie des données vers le hub, celui-ci les diffuse vers tous les autres ports du hub, quel que soit le destinataire. Cela signifie que toutes les données atteignent chaque appareil connecté.

Avantages d'un hub :

1. Simplicité d'utilisation: Les hubs sont faciles à installer et à utiliser. Il suffit de connecter les câbles réseau aux ports du hub pour établir des connexions.
2. Coût abordable: Les hubs sont généralement moins chers que d'autres équipements de réseau, comme les commutateurs (switches) ou les routeurs.
3. Capacité à étendre le réseau: Un hub permet d'étendre un réseau en ajoutant davantage d'appareils à celui-ci, car il offre plusieurs ports pour connecter des périphériques.

Inconvénients d'un hub :

1. Collision de données: Étant donné que les données sont diffusées à tous les ports du hub, il peut

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

Un switch est un dispositif de réseau qui permet de relier plusieurs appareils au sein d'un réseau local. Voici les avantages et inconvénients d'un switch :

Avantages d'un switch :

1. Efficacité dans la transmission de données : Contrairement à un hub, un switch envoie les données uniquement vers le port où le destinataire se trouve, ce qui évite la congestion du réseau et accélère le transfert de données.
2. Meilleure sécurité : Comme les données sont transmises uniquement au destinataire spécifique, le switch réduit le risque d'interception de données par des appareils non autorisés.
3. Bande passante partagée : Contrairement à un hub, où la bande passante est partagée entre tous les ports, un switch offre une bande passante dédiée par port. Cela signifie que chaque port du switch a sa propre bande passante, entraînant ainsi les conflits et les ralentissements causés par la congestion du réseau.

Inconvénients d'un switch :

1. Coût supérieur: Les switches sont généralement plus coûteux que les hubs en raison de leur technologie avancée et de leur capacité à gérer le trafic de manière plus efficace.
2. Configuration plus complexe : Configurer un switch peut être plus complexe que configurer un hub, nécessitant une certaine expertise pour optimiser ses fonctionnalités et performances.
3. Utilisation d'énergie: Les switches nécessitent plus d'énergie pour fonctionner par rapport aux hubs en raison de leur traitement des données plus avancé, ce qui peut augmenter la consommation d'électricité dans un réseau.
4. Limitation du nombre de ports : Chaque switch a un nombre limité de ports physiques, ce qui peut devenir un inconvénient si le réseau nécessite de connecter un grand nombre d'appareils. Dans ce cas, il faut utiliser des switches empilables ou des équipements supplémentaires.

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

Un switch est un dispositif réseau utilisé pour diriger le trafic de données entre différents périphériques au sein d'un réseau local (LAN). Il joue un rôle crucial dans la gestion efficace du trafic réseau en acheminant les données uniquement vers les destinataires appropriés plutôt que de les diffuser à tous les appareils du réseau.

Voici comment un switch gère le trafic réseau :

1. Table de commutation (MAC address table):

Le switch maintient une table de correspondance entre les adresses MAC (Media Access Control) et les ports du switch. Cette table aide le switch à déterminer le port vers lequel il doit envoyer les données en fonction de l'adresse MAC de destination.

2. Apprentissage des adresses MAC (MAC learning):

Lorsqu'un switch reçoit des trames réseau, il examine l'en-tête de chaque trame pour extraire l'adresse MAC source. Le switch enregistre cette adresse MAC dans sa table de commutation associée au port par lequel la trame a été reçue.

3. Filtrage et transmission sélective:

Grâce à la table de commutation, le switch détermine le port par lequel la trame doit être envoyée pour atteindre le périphérique destinataire, et il envoie la trame uniquement à ce port, limitant ainsi le trafic inutile sur le réseau.

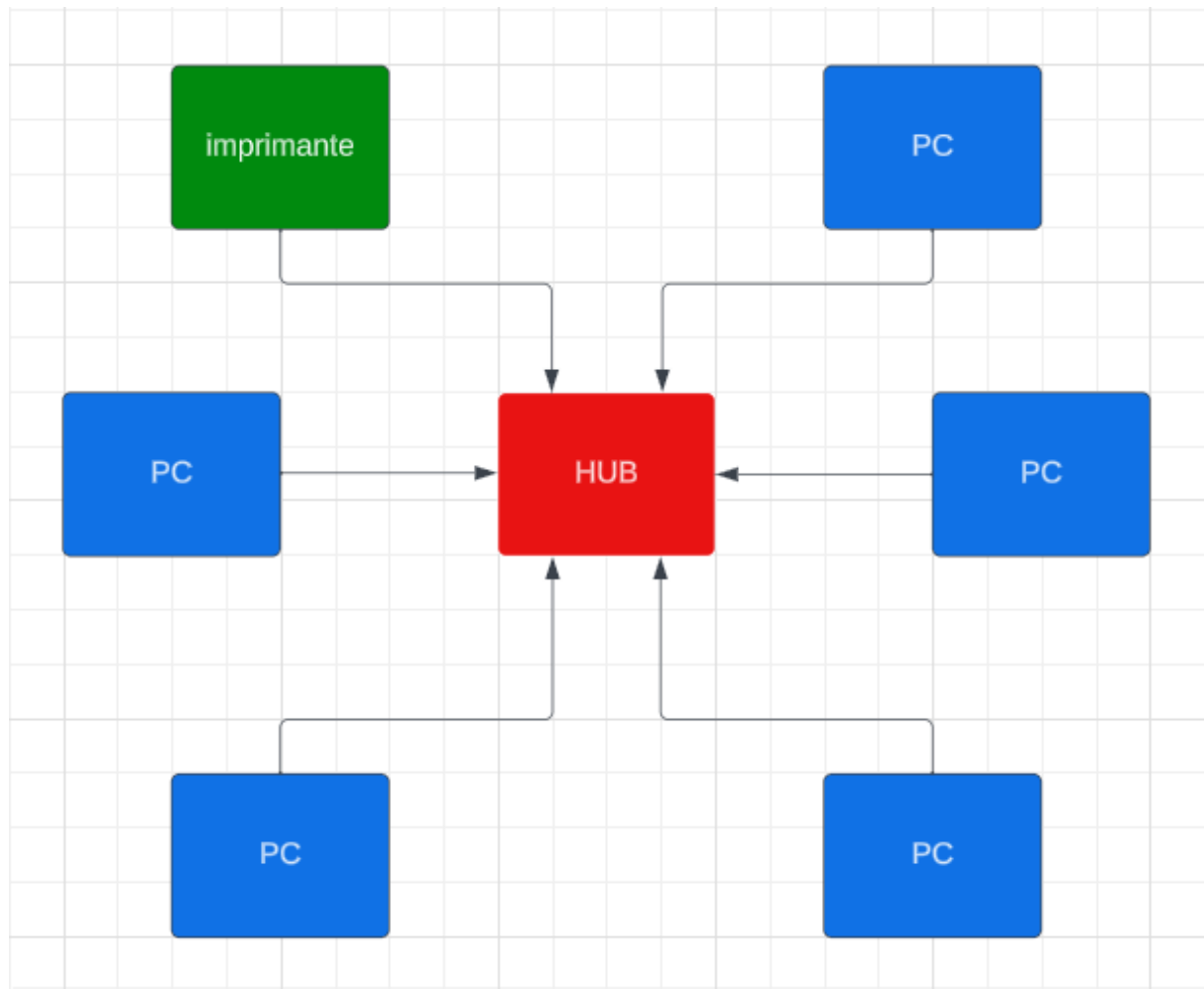
4. Diffusion sélective (unicast):

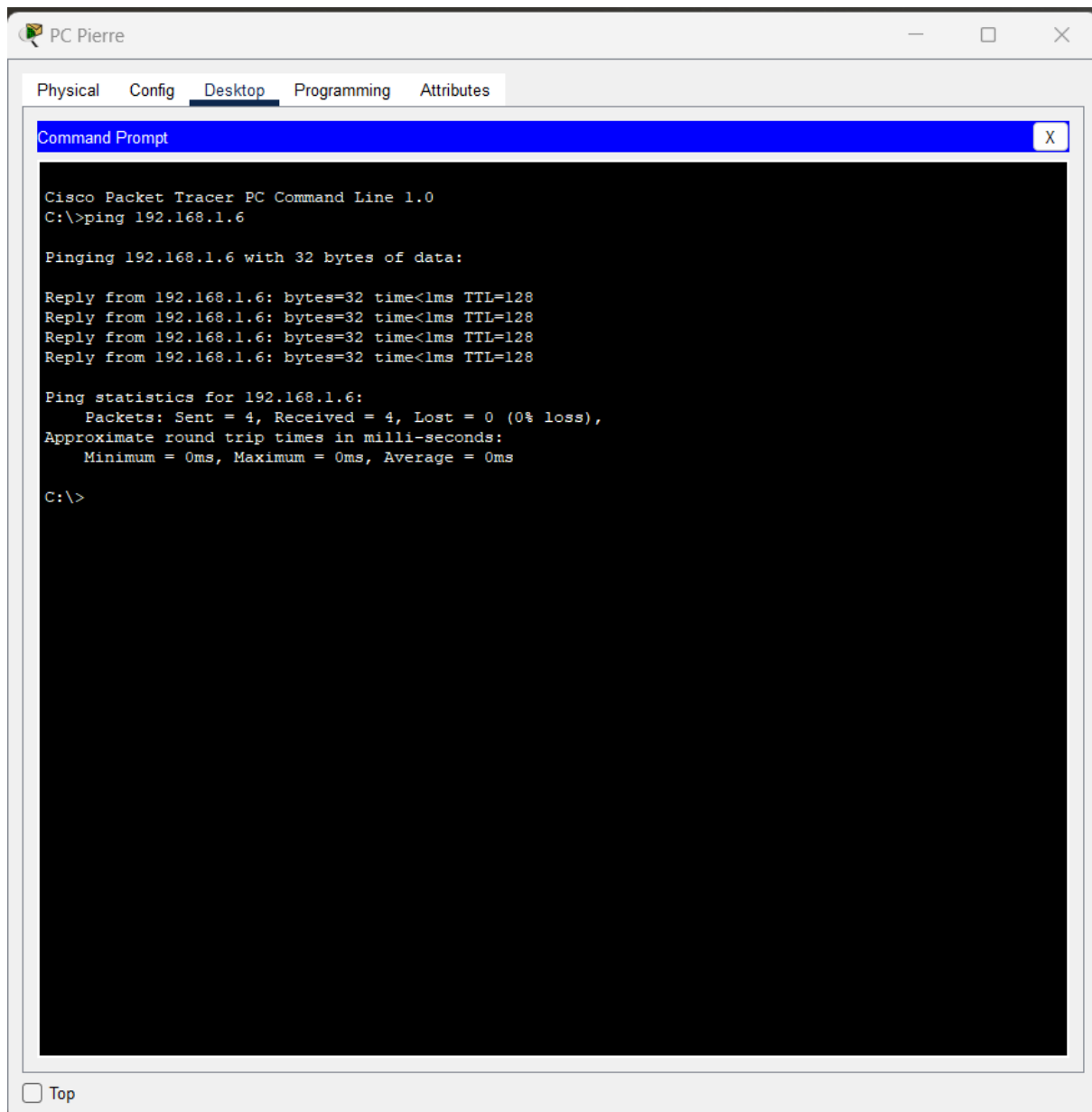
Lorsque le switch reçoit une trame destinée à un périphérique spécifique, il utilise la table de commutation pour trouver le port associé à l'adresse MAC du destinataire et envoie la trame uniquement à ce port.

5. Diffusion à tous les ports (broadcast):

Si une trame est destinée à être diffusée à tous les périphériques du réseau (par exemple, ARP request), le switch envoie la trame à tous les ports.

Job 9:





identifiez au moins trois avantages importants d'avoir un schéma et ajoutez le schéma ainsi que vos explications sur votre documentation.

1. Ils sollicitent tant l'esprit de synthèse et permettent d'avoir une vision globale et immédiate du sujet présenté, que l'esprit d'analyse, ils permettent de visualiser et de comprendre chacun des éléments composant le schéma et comment ces éléments sont liés entre eux.
2. Ils peuvent également rendre compréhensibles des informations abstraites ou non perceptibles (des idées, des théories, des concepts) en permettant leur visualisation, et donc leur analyse.

3. Les schémas qui utilisent l'image réconcilient l'hémisphère droit (qui traite les images) et l'hémisphère gauche (qui traite les textes) du cerveau grâce à l'utilisation conjointe du texte et de l'image qui, réunis, font sens. Le lecteur utilise donc la globalité des capacités de son cerveau.

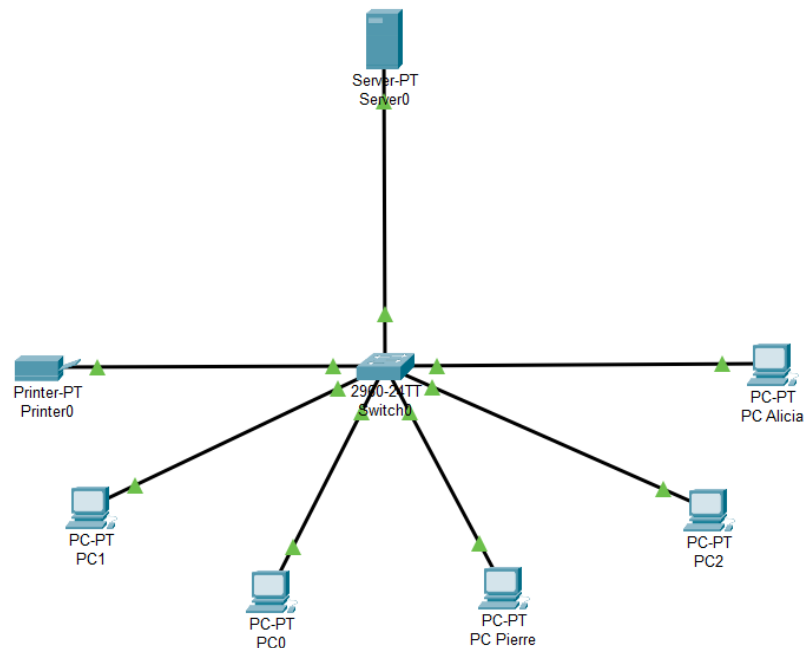
explication du schéma:

Le HUB consiste à relier plusieurs ordinateurs et imprimantes entre eux et à relayer immédiatement les données qu'ils reçoivent. Ils fonctionnent à l'aide d'une alimentation externe et possèdent entre quatre et seize ports (connexions physiques).

Un ordinateur est un appareil qui permet de réaliser, d'exécuter des opérations ou des calculs. Il a la capacité de stocker, récupérer et traiter des données. Vous pouvez également utiliser un ordinateur pour saisir des documents, envoyer des courriels, jouer à des jeux vidéo, naviguer sur Internet et envoyer des données via une imprimante pour pouvoir imprimer des documents.

L'imprimante a pour rôle principal de sortir sur papier un document, une image initialement présente ou créée sur un ordinateur, et peut servir comme une imprimante professionnelle ou personnelle.

Job 10:



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

Une adresse IP (Internet Protocol) est une série unique de chiffres attribuée à chaque appareil connecté à un réseau informatique. La manière dont cette adresse IP est attribuée peut être statique ou dynamique, généralement via DHCP (Dynamic Host Configuration Protocol). Voici les différences entre une adresse IP statique et une adresse IP attribuée par DHCP :

Adresses IP statiques:

- Une adresse IP statique est configurée manuellement par un administrateur réseau ou un utilisateur.
- Elle reste constante et ne change pas, sauf si elle est modifiée manuellement.
- L'attribution d'une adresse IP statique est souvent utilisée pour des serveurs, des imprimantes réseau, des équipements réseau critiques ou des appareils nécessitant une adresse IP permanente et stable.
- Elle nécessite une configuration manuelle de l'adresse IP, de la passerelle, du masque de sous-réseau et des serveurs DNS.

Adresses IP attribuées par DHCP:

- Le DHCP est un protocole réseau qui attribue automatiquement des adresses IP et d'autres paramètres réseau à des appareils clients au sein d'un réseau.
- Les adresses IP attribuées par DHCP sont temporaires et peuvent changer à chaque connexion ou lors du renouvellement du bail DHCP.
- Le DHCP simplifie la gestion des adresses IP, car il évite la nécessité de configurer manuellement chaque appareil avec une adresse IP.
- Il optimise l'utilisation des adresses IP en allouant dynamiquement des adresses disponibles en fonction des besoins du réseau.

En résumé, une adresse IP statique est configurée manuellement et reste constante.

Job 11:

L'adresse de réseau permet de savoir si 2 machines peuvent communiquer entre elles. Si ces 2 machines ont une adresse réseau identique, alors, elles appartiennent au même réseau et elles peuvent communiquer. L'adresse de réseau correspond à l'adresse IP la plus basse d'un réseau.

La réalisation d'un plan d'adressage a pour objectif d'adresses et normes l'ensemble des voies de la commune, qui se voient attribuer une dénomination, et des bâtis qui y sont situés, référencés par un numéro

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

Car elle convient parfaitement au réseau pour de grande entreprise comme ici car elle permet de créer plus de 16 million d'adresse IP.

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

Les classes de réseaux désignent les différentes plages d'adresses IP utilisées dans le protocole IPv4. Elles sont utilisées pour diviser l'espace d'adressage IP en catégories en fonction du nombre d'hôtes qu'elles peuvent prendre en charge. Il existe cinq classes de réseaux principales : A, B, C, D et E. Voici un aperçu de chaque classe de réseau :

1. Classe A (Plage d'adresses : 1.0.0.0 à 126.0.0.0) :

- Plage d'adresse IP très vaste.
- Conçue pour les grands réseaux, comme les réseaux d'entreprise.
- Le premier octet est réservé pour l'identification de la classe, et les trois octets suivants sont utilisés pour l'adresse du réseau.
- Permet environ 16 millions d'adresses IP.

2. Classe B (Plage d'adresses : 128.0.0.0 à 191.255.0.0) :

- Conçue pour les réseaux de taille moyenne.
- Les deux premiers octets sont réservés pour l'identification de la classe, et les deux octets suivants sont utilisés pour l'adresse du réseau.
- Permet environ 65 000 adresses IP.

3. Classe C (Plage d'adresses : 192.0.0.0 à 223.255.255.0) :

- Conçue pour les petits réseaux.
- Les trois premiers octets sont réservés pour l'identification de la classe, et un octet est utilisé pour l'adresse du réseau.
- Permet environ 254 adresses IP.

4. Classe D (Plage d'adresses : 224.0.0.0 à 239.255.255.255) :

- Réservee pour les adresses IP multicast.
- Les adresses de classe D sont utilisées pour la diffusion de données à un groupe de destinataires plutôt qu'à une seule machine.
- Elles ne sont pas utilisées pour attribuer des adresses IP individuelles à des dispositifs.
- Elles sont utilisées pour la transmission de données multimédias, de vidéos en streaming, de jeux en ligne, etc.

5. Classe E (Plage d'adresses : 240.0.0.0 à 255.255.255.255) :

- Réservee à des fins expérimentales et de recherche.
- Les adresses de classe E ne sont pas utilisées dans les réseaux publics ou privés courants.
- Elles ne sont pas destinées à un usage général et ne sont pas utilisées pour l'adressage des hôtes.

Notez que les classes A, B et C sont les plus couramment utilisées dans les réseaux IP classiques, tandis que les

Job 14:

Convertissez les adresses IP suivantes en binaires :

- 145.32.59.24 → 10010001 100000 111011 11000
- 200.42.129.16 → 11001000 101010 10000001 10000
- 14.82.19.54 → 1110 1010010 10011 110110

Job 15:

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission des données entre différents réseaux informatiques. Lorsqu'un appareil (comme un ordinateur, un smartphone, un serveur, etc.) envoie des données à un autre appareil situé sur un réseau différent, ces données doivent être acheminées à travers divers composants du réseau. Le routage consiste à déterminer le chemin le plus efficace pour acheminer ces données d'un point d'origine à leur destination.

→ Qu'est-ce qu'un gateway ?

Une passerelle, souvent appelée "gateway" en anglais, est un dispositif matériel ou logiciel permettant de relier deux réseaux informatiques distincts. C'est essentiellement un point d'entrée ou de sortie permettant aux données de circuler entre ces réseaux, facilitant ainsi la communication et l'échange d'informations.

→ Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network) est un réseau privé qui permet de créer une connexion sécurisée et chiffrée sur Internet, offrant ainsi un niveau élevé de confidentialité et de sécurité des données. Un VPN établit un tunnel sécurisé entre votre appareil (ordinateur, smartphone, tablette) et un serveur VPN distant, masquant ainsi votre adresse IP réelle et chiffrant le trafic entre vous et ce serveur.

→ Qu'est-ce qu'un DNS ?

DNS, qui signifie "Domain Name System" en anglais, est un système hiérarchique permettant de traduire les noms de domaine facilement à mémoriser en adresses IP numériques, nécessaires pour acheminer le trafic sur Internet. En d'autres termes, il permet de faire correspondre les adresses web conviviales (comme www.google.com) aux adresses IP associées (comme 192.168.1.1).