Runtrack Réseau

JOB 1

Installer packet tracer

JOB 2

Réponses aux questions :

➔ *Qu'est-ce qu'un réseau ?*

Un réseau est un groupement de deux ou plusieurs ordinateurs ou autres appareils électroniques permettant l'échange de données et le partage de ressources communes.

➔ *À quoi sert un réseau informatique ?*

Un réseau informatique permet la communication, le partage de ressources, l'accès à l'information, la collaboration et bien d'autres fonctions qui facilitent la vie quotidienne et le travail.

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

La création d'un réseau informatique implique l'utilisation de divers composants matériels, chacun ayant un rôle spécifique dans le bon fonctionnement du réseau. Voici les principaux éléments matériels nécessaires pour construire un réseau, ainsi que leurs fonctions :

1. **Dispositifs finaux** :
   - Ordinateurs: Les appareils tels que les ordinateurs de bureau, les ordinateurs portables, les tablettes et les smartphones constituent les points finaux du réseau, à partir desquels les utilisateurs accèdent aux ressources partagées.

2. **Serveurs** :
   - Serveurs de fichiers : Ces serveurs stockent et gèrent les fichiers que les utilisateurs partagent sur le réseau.
   - Serveurs d'applications : Ils hébergent des logiciels et des applications que les utilisateurs peuvent exécuter à distance.
   - Serveurs de messagerie : Ils gèrent les courriers électroniques et les services de messagerie pour les utilisateurs.

3. **Dispositifs de mise en réseau** :

- Routeurs : Les routeurs dirigent le trafic entre différents réseaux. Ils sont responsables du routage des données entre les réseaux locaux (LAN) et les réseaux étendus (WAN).
- Commutateurs (Switches) : Les commutateurs sont utilisés pour connecter plusieurs dispositifs au sein d'un même réseau local (LAN) en transférant efficacement les données entre eux.
- Points d'accès sans fil (WAP) : Ils permettent la connexion sans fil des appareils au réseau. Les WAP sont utilisés dans les réseaux sans fil (Wi-Fi).

4. **Câblage et infrastructure physique** :
- Câbles Ethernet : Ils servent à connecter les dispositifs au réseau, couramment utilisés pour les réseaux câblés.
- Fibre optique : Utilisée pour les réseaux à haut débit sur de longues distances.
- Armoires et boîtiers de raccordement : Ils abritent les équipements de réseau et fournissent un point centralisé pour la gestion du câblage.

5. **Serveurs de sécurité** :
- Firewalls : Les pare-feux protègent le réseau contre les menaces extérieures en surveillant et en filtrant le trafic entrant et sortant.
- Systèmes de détection d'intrusion (IDS) : Ils détectent les activités suspectes ou malveillantes sur le réseau.
- VPN (Virtual Private Network) Gateway : Ils permettent la création de connexions sécurisées pour les utilisateurs distants.

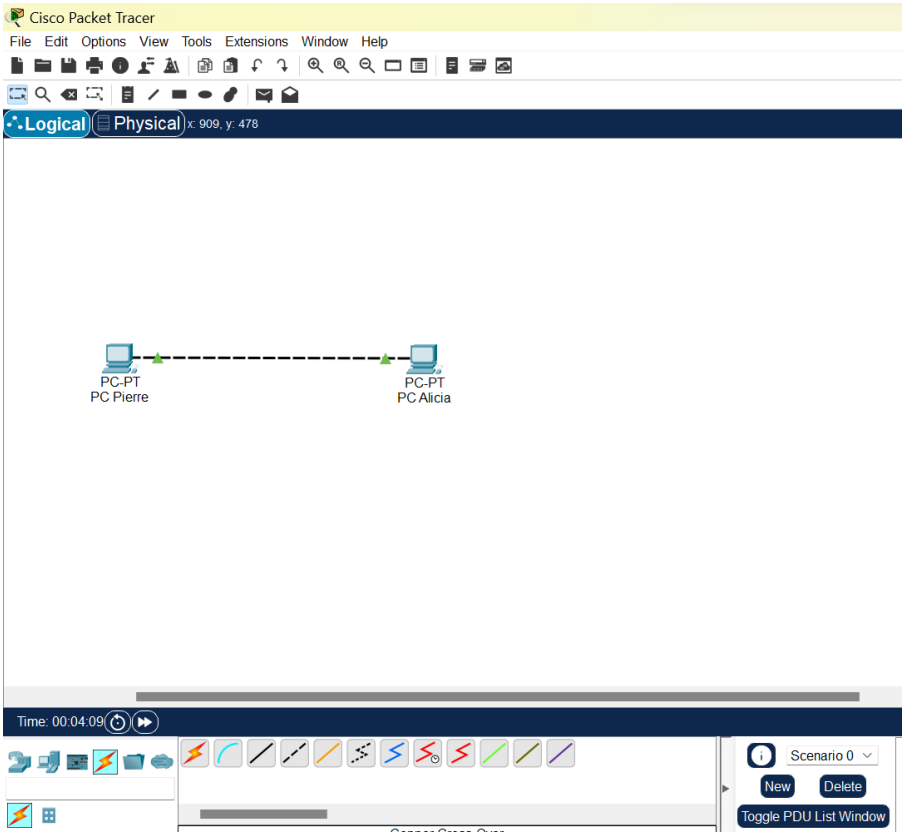
6. **Modems et passerelles** :
- Modems : Ils permettent la connexion du réseau local à Internet.
- Passerelles : Elles connectent deux réseaux différents, souvent en traduisant les protocoles.

7. **Périphériques réseau** :
- Imprimantes réseau : Elles sont accessibles depuis n'importe quel point du réseau pour l'impression partagée.
- Caméras de sécurité réseau (IP) : Utilisées pour la surveillance vidéo sur le réseau.

8. **Alimentation électrique et climatisation** :
- L'alimentation électrique ininterrompue (UPS) garantit que le réseau reste opérationnel en cas de panne de courant.
- La climatisation assure que les équipements matériels restent à des températures appropriées pour éviter la surchauffe.

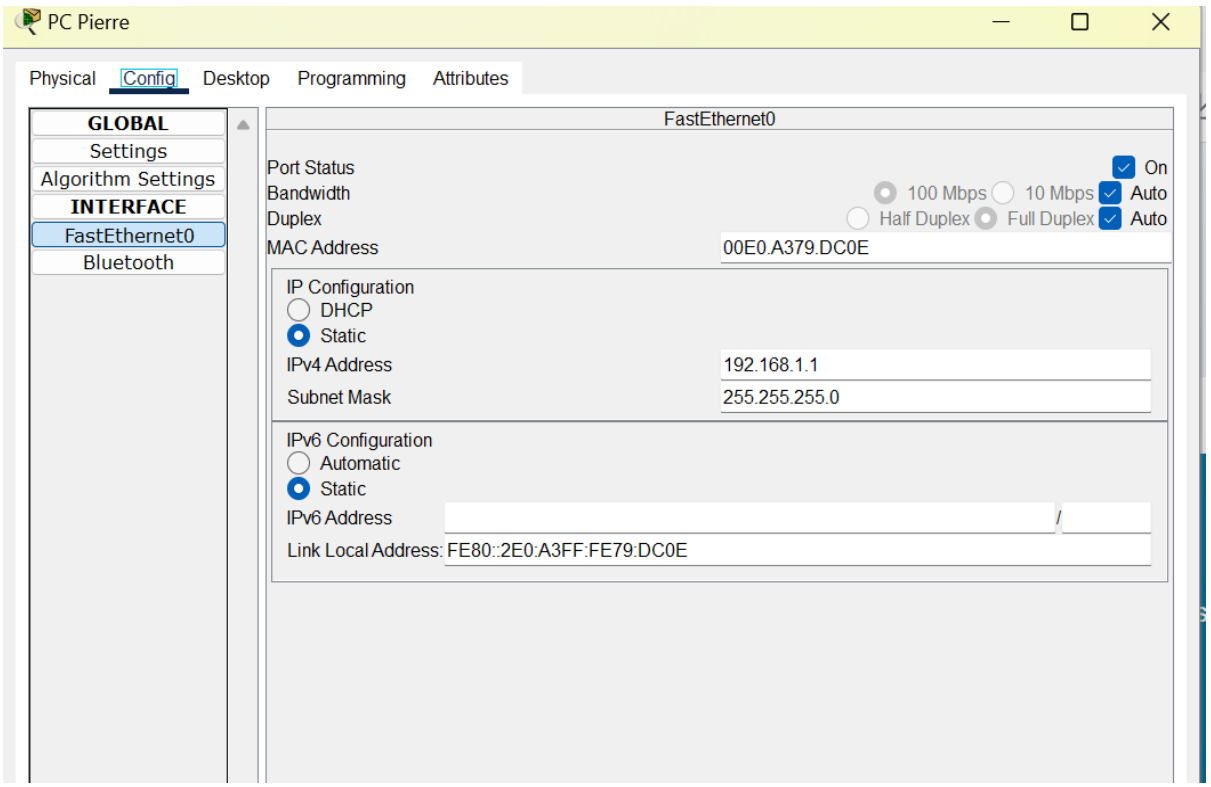
Chaque composant a un rôle spécifique dans la construction et le fonctionnement du réseau, garantissant la connectivité, la gestion des données et la sécurité. Le choix de ces composants dépendra de la taille et des besoins spécifiques du réseau.

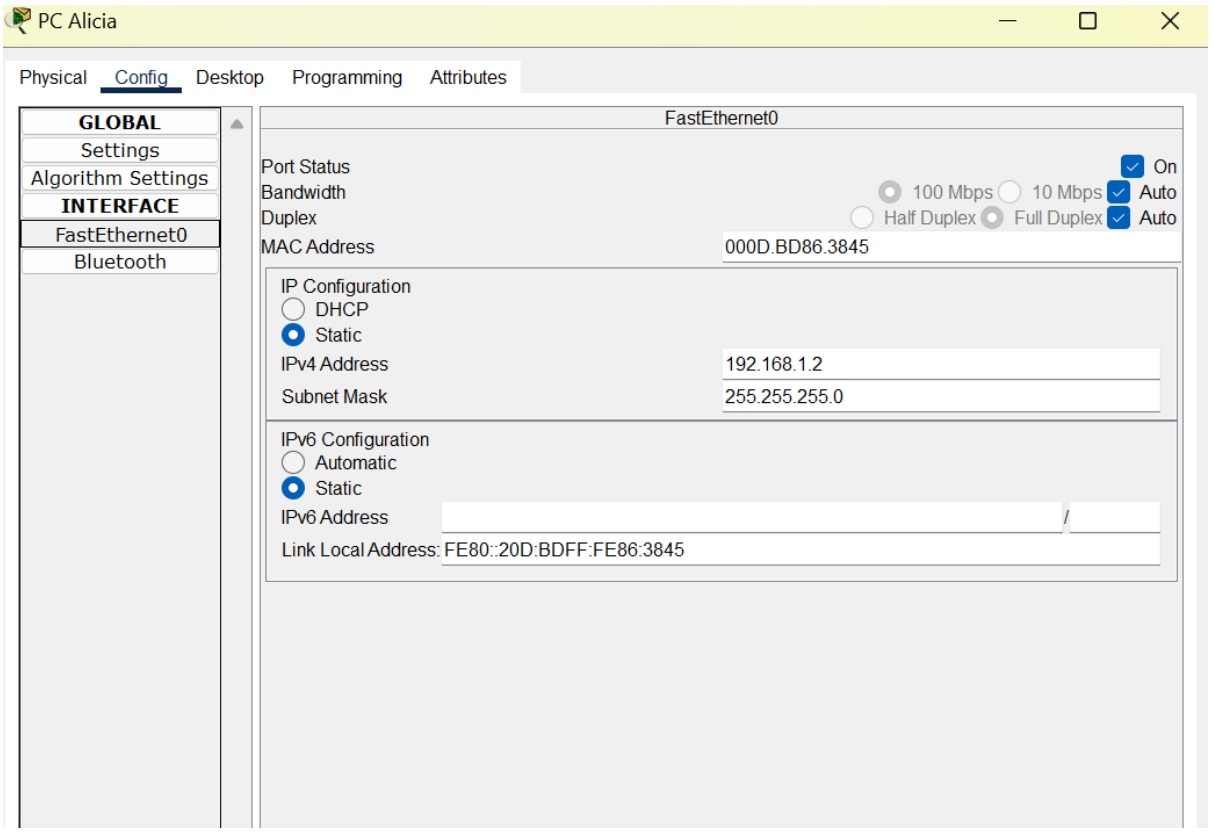
JOB 3



➔ J’ai utilisé le cable Copper Cross Over car il est utilisé pour relier directement deux dispositifs similaires, tels que deux ordinateurs, deux commutateurs ou deux routeurs sans nécessiter un équipement intermédiaire, comme un routeur.

JOB 4





➔ *Qu'est-ce qu'une adresse IP ?*

Une adresse IP (Internet Protocol address) est une suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet. Les adresses IP permettent d'identifier et de différencier les milliards d'appareils en ligne, y compris les ordinateurs et les téléphones mobiles, et les aident à communiquer entre eux.

➔ *À quoi sert un IP ?*

L'adresse IP est utilisée pour permettre aux appareils de communiquer entre eux sur un réseau informatique. Lorsqu'un appareil envoie des données à un autre appareil, il inclut l'adresse IP de l'appareil destinataire dans le paquet de données. Le routeur utilise ensuite cette adresse IP pour acheminer le paquet de données vers l'appareil destinataire.
L'adresse IP est également utilisée pour identifier l'emplacement géographique approximatif d'un appareil. Les services basés sur la localisation, tels que les moteurs de recherche et les publicités ciblées, utilisent souvent l'adresse IP pour déterminer l'emplacement géographique d'un utilisateur.

➔ *Qu'est-ce qu'une adresse MAC ?*

L'adresse MAC signifie "Media Access Control" 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.

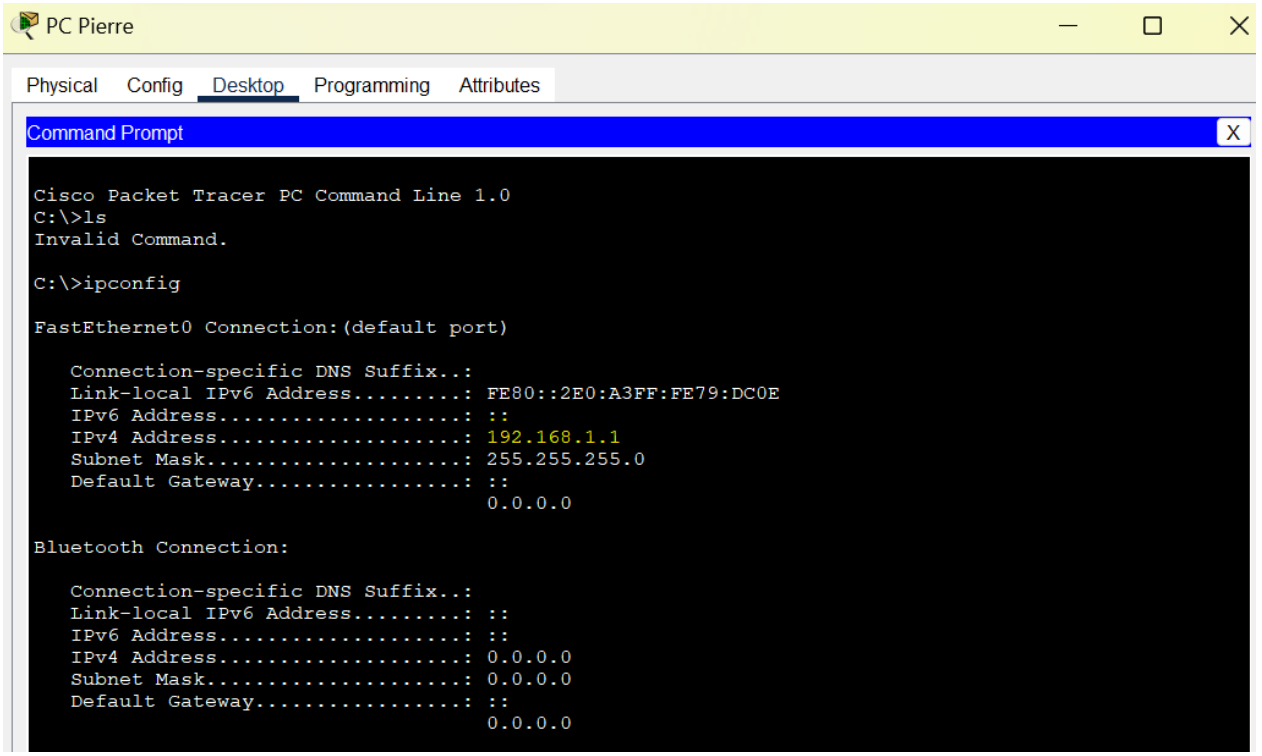
➔ *Qu'est-ce qu'une IP publique et privée ?*

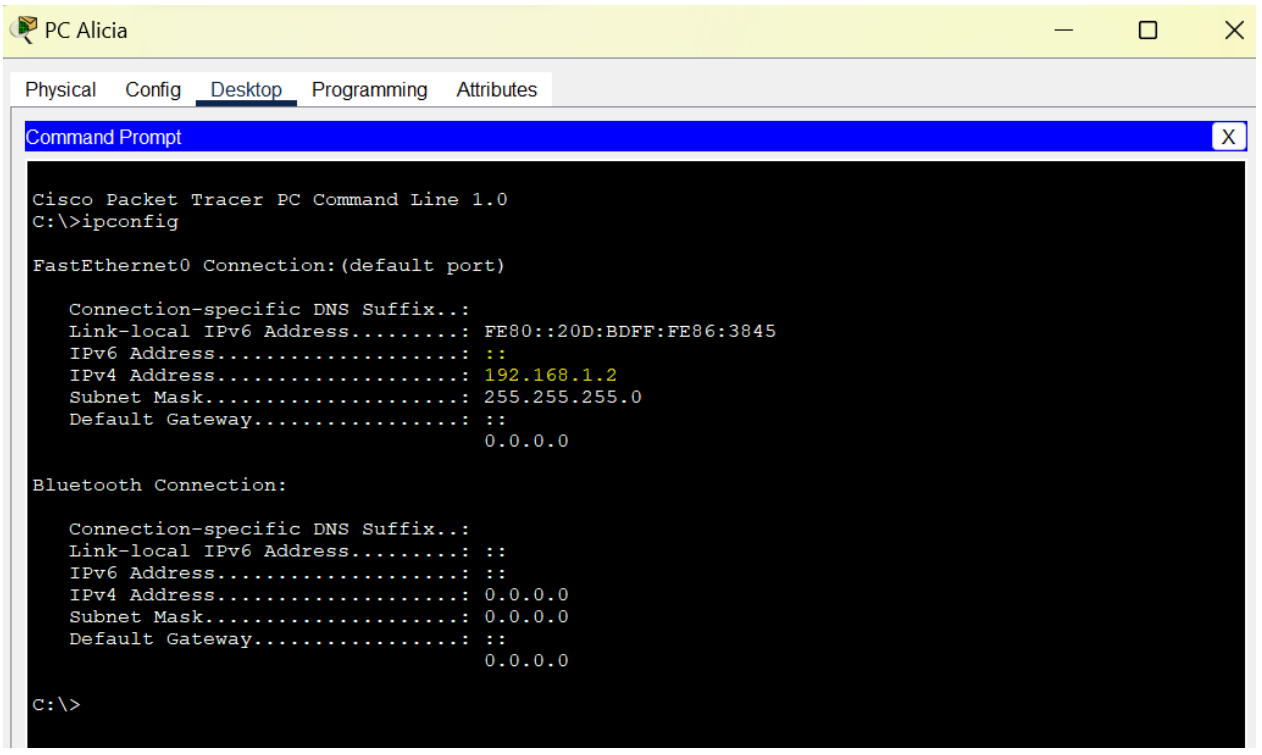
Une adresse IP privée ce sont toutes les adresses IP qui ne sont pas utilisables sur internet, par exemple le réseau de votre entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les plages d'adresses IP non accessibles depuis Internet. Elles permettent de communiquer localement avec vos différents périphériques… En revanche, les adresses IP publiques ne sont pas utilisées dans un réseau local mais uniquement sur internet.
Une adresse IP publique est unique dans le monde alors que pour une adresse IP privée c'est dans le réseau local qu'elle est unique.
En somme, les adresses IP publiques sont utilisées pour l'identification sur Internet et des adresses IP privées pour l'identification à l'intérieur d'un réseau local.

➔ *Quelle est l'adresse de ce réseau ?*

Subnet Mask	255.255.255.0

JOB 5





➔ *Ligne de commande utilisée pour vérifier l'id des machines* : **ipconfig**

JOB 6

```
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=5ms 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 = 5ms, Average = 1ms

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=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms 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 = 9ms, Average = 3ms

C:\>
```

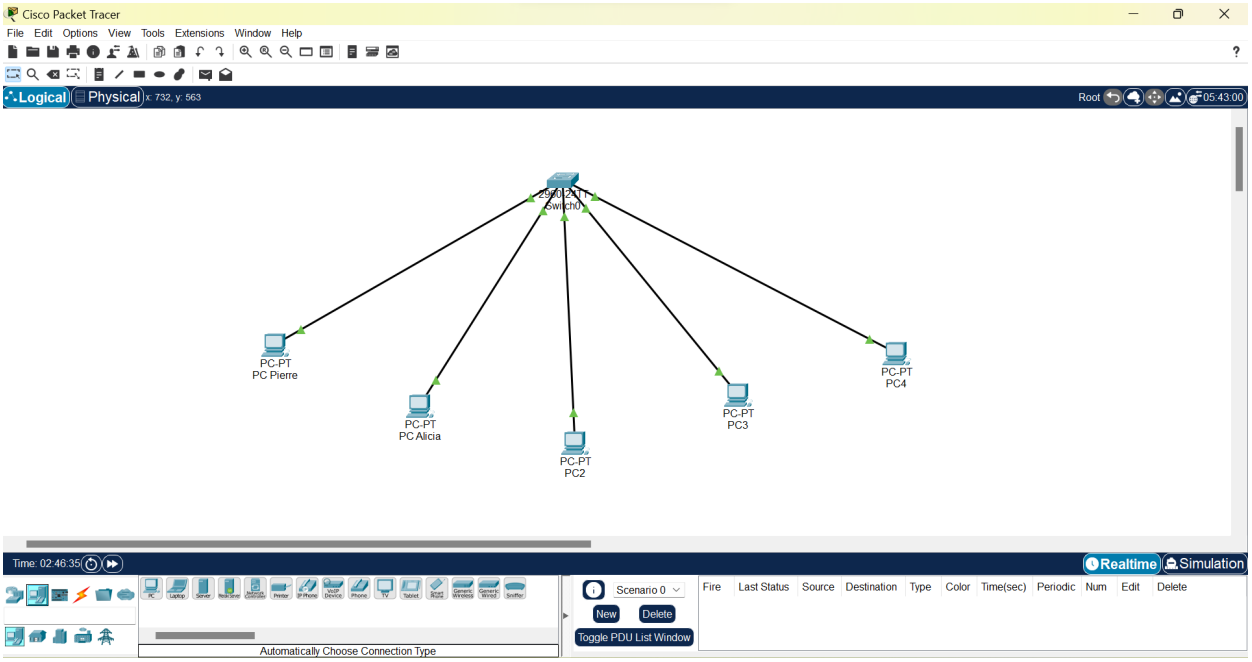
La commande permettant de Ping entre des PC est : **ping + adresse ip**

JOB 7

```
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:\>
```

Non, le PC de Pierre n'a pas reçu les paquets envoyés par Alicia car son PC est éteint.

JOB 8



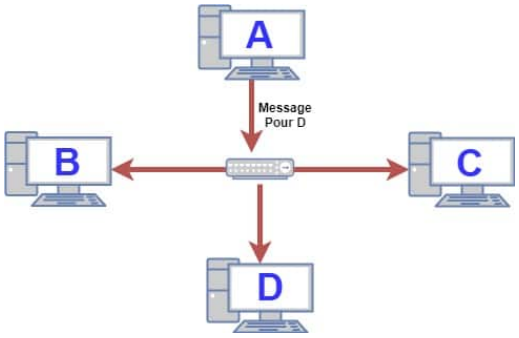
➔ *Quelle est la différence entre un hub et un switch ?*

Le Hub est presque plus utilisé, il transmet les paquets à tout le monde en espérant que le destinataire recevra. On peut le considérer comme une multiprise électrique. Par contre, **le**

switch permet un filtrage des paquets reçus pour les transférer uniquement au destinataire prévu. **Un switch** est donc un bien plus intelligent et avec ses prix actuels, il a remplacé **les hubs** partout.

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

- **Fonctionnement d'un hub**



Comme vous pouvez le voir dans l'image ci-contre, le hub est beaucoup moins intelligent que le switch car lorsque A va vouloir envoyer un message à D, le hub va retransmettre l'intégralité de celui-ci à tous les appareils connectés (on utilise aussi le terme de répétiteur pour le hub en français), et avec un peu de chance D recevra le message. 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)

- **Avantages**

Les hubs sont ***simples*** à utiliser et à configurer. Il n'y a généralement aucune configuration requise, ce qui les rend adaptés aux utilisateurs novices. Ils sont généralement ***moins chers*** que d'autres dispositifs réseau tels que les commutateurs…

- **Inconvénients**

Les Hubs souffrent de limitations majeures en termes de ***performances***, de ***sécurité*** et de ***flexibilité***. Le fait de retransmettre les messages à l'ensemble du réseau à chaque fois surcharge le réseau inutilement, et génère une baisse des débits et en raison de la nature de la transmission de données sur un hub, il peut y avoir ***des collisions*** de données lorsque plusieurs périphériques tentent de transmettre simultanément, ce qui peut entraîner des erreurs de transmission…

➔ *Quels sont les avantages et inconvénients d'une switch ?*

Avantages des Switchs :

- Ils augmentent la capacité de transfert de données accessible de l'organisation.

- Ils aident à réduire la charge exceptionnelle sur les ordinateurs hôtes individuels.

- Ils incrémentent la présentation de l'organisation.

- Moins d’impacts sur le boîtier: Les réseaux qui utilisent des commutateurs auront moins d’impacts sur le boîtier. Cela est dû à la façon dont les commutateurs créent des zones d’impact pour chaque association.

- Simple car les commutateurs peuvent être directement associés aux postes de travail.

- Il augmente la bande passante disponible du réseau.

- Les réseaux qui utilisent des commutateurs auront moins de collisions de trames
- Plus sécurisé car étant donné que le commutateur est isolé, les données n’iront qu’à la destination.

Inconvénients des switchs :

Coûteux : Ils sont plus coûteux que les étendues de réseau.

Problèmes de disponibilité difficiles : Les problèmes de disponibilité du réseau sont difficiles à suivre via le changement d’organisation.

Problèmes de diffusion du trafic : Le trafic de diffusion peut être problématique.

Sans défense : Si les commutateurs sont en mode aveugle, ils sont sans défense contre les attaques de sécurité, par exemple la caricature d’adresse IP ou la capture de contours Ethernet.

Nécessité d’une planification appropriée : Une planification et un agencement appropriés sont nécessaires pour traiter les colis multidiffusion.

Les composants mécaniques peuvent s’user : Les composants mécaniques du commutateur peuvent s’user avec le temps.

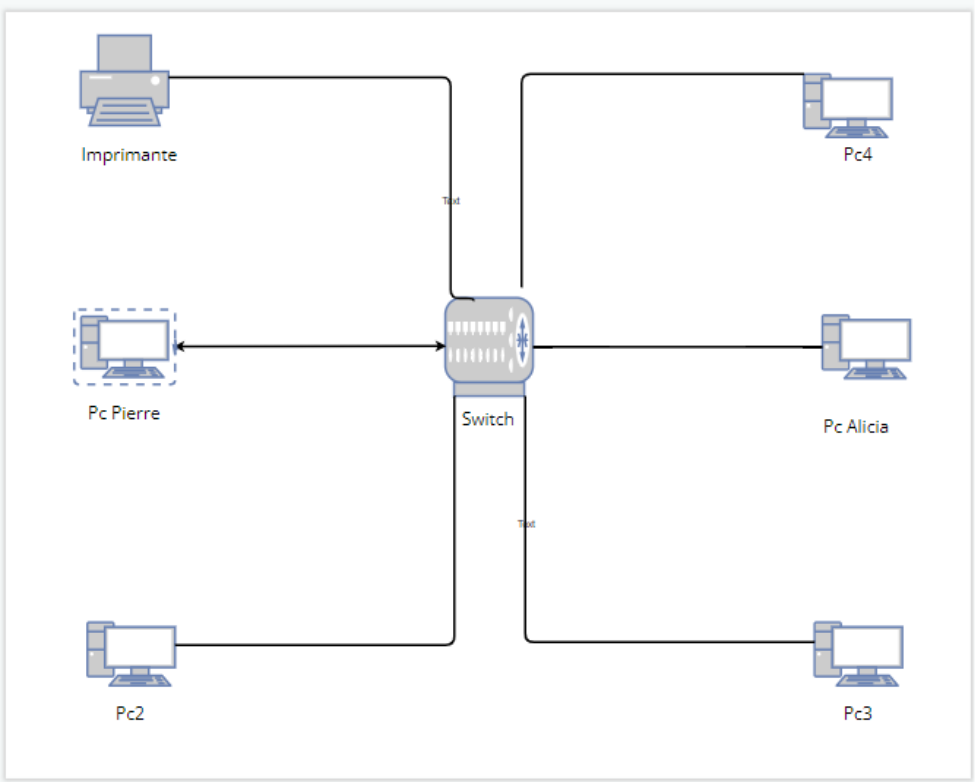
Le contact physique est obligatoire : Doit avoir un contact physique avec l’objet à actionner.

En résumé, les switches offrent une meilleure performance et une meilleure sécurité que les concentrateurs, mais ils sont plus coûteux et nécessitent une configuration et une gestion plus avancées. Le choix entre un switch et d'autres périphériques dépend des besoins spécifiques de votre réseau.

➔ *Comment un switch gère-t-il le trafic réseau ?*

Un switch gère le trafic réseau en utilisant des adresses MAC pour déterminer sur quel port envoyer les données. Il maintient une table de commutation des adresses MAC pour rationaliser la transmission de données, réduisant ainsi le trafic inutile et améliorant l'efficacité du réseau.

JOB 9



Trois avantages importants d'avoir un schéma de réseau

Clarté de la conception : Un schéma de réseau bien conçu permet de visualiser rapidement la topologie du réseau, en montrant la manière dont les composants (ordinateurs, commutateurs, routeurs, etc.) sont connectés les uns aux autres. Cela rend plus facile la compréhension de la configuration du réseau.

Dépannage plus efficace : En cas de problème de réseau, disposer d'un schéma précis peut grandement faciliter le processus de dépannage. Vous pouvez identifier rapidement le point de défaillance, ce qui permet de gagner du temps lors de la résolution des problèmes.

Planification et évolution du réseau : Un schéma de réseau vous aide à planifier des améliorations, des mises à jour ou des extensions de votre réseau. Vous pouvez voir comment les nouveaux composants s'intégreront dans la topologie existante, ce qui permet une croissance plus efficace et évolutive du réseau.

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 attribuée manuellement à votre appareil et qui ne change jamais. Elle permet aux dispositifs de réseau de conserver la même adresse IP en permanence. En revanche, le DHCP est un protocole qui attribue automatiquement des adresses IP aux appareils d'un réseau. Elle est donc une adresse temporaire qui peut changer périodiquement.

*

JOB 11

Plan d'adressage

- **1 sous-réseau de 12 hôtes**

Pour cela, nous avons besoin de 4 bits pour les hôtes (2^4 = 16 adresses, dont 2 sont réservées pour l'adresse réseau et l'adresse de diffusion)
Masque de sous-réseau : 225.225.225.240/28
Pool address : 10.0.0.0/28.

- **5 sous-réseaux de 30 hôtes**

On a besoin de 30 hôtes, ce qui nécessite 5 bits pour les hôtes (2^5 - 2 = 30 adresses disponibles).
Masque de sous-réseau : 255.255.255.224/27.
Pool address : 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

- **5 sous-réseaux de 120 hôtes**

Pour 120 hôtes, on aura besoin de 7 bits pour les hôtes (2^7 - 2 = 126 adresses disponibles).
Masque de sous-réseau : 255.255.255.128/25
Pool address : 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

- **5 sous-réseaux de 160 hôtes**

Pour 160 hôtes, cela nécessite 8 bits pour les hôtes (2^8 - 2 = 254 adresses disponibles).
Masque de sous-réseau : 255.255.255.0/24
Pool address : 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

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

C'est pour des raisons de flexibilité et de disponibilité d'adresses IP et de facilité de gestion, ce qui en fait un choix judicieux pour un réseau nécessitant de nombreux sous-réseaux de tailles variables.

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

Les adresses IP peuvent être classées en différentes catégories en fonction de leur plage d'adresses et de leur utilisation. Les principales catégories d'adresses IP sont les adresses de **classe A, de classe B, de classe C**, de classe D et de classe E. Par conséquent, celles des **classes A, B et C** sont les plus utilisées:

Classe A :
Les adresses de ces réseaux sont a.0.0.0 avec a compris entre 1 et 126 bornes incluses (le premier bit des adresses IP des ces réseaux est 0).
Le masque est 255.0.0.0
Un tel réseau peut contenir 224-2 machines soit 16 millions environ.

Classe B :
Les adresses de ces réseaux sont a.b.0.0 avec a compris entre 128 et 191 bornes incluses et b compris entre 0 et 255.(les 2 premiers bits des adresses IP de ces réseaux sont 10).
Un tel réseau peut contenir 216 -2 = 65 534 machines.

Classe C :
Les adresses de ces réseaux sont a.b.c.0 avec a compris entre 192 et 223 bornes incluses et b et c compris entre 0 et 255 (les 3 premiers bits des adresses IP de ces réseaux sont 110).
Un tel réseau peut contenir 28-2 = 254 machines.

Classe	Plage d'adresses	Détail	Partie réseau /hôte	Masque de sous-réseau par défaut
Classe A	1 .0.0.1 – 126 .255.255.254	Prend en charge 16 millions d'hôtes sur chacun des 127 réseaux	N .HHH	255 .0.0.0
Classe B	128.1.0.1 – 191.255.255.254 _	Prend en charge 65 000 hôtes sur chacun des 16 000 réseaux	NN .HH	255.255.0.0 _
Classe C	192.0.1.1 – 223.255.254.254 _	Prend en charge 254 hôtes sur chacun des 2 millions de réseaux	NNN .H	255.255.255.0 _

JOB 12

NUM	COUCHE	RÔLE	PROTOCOLE
7	***Application***	La couche application comprend les protocoles conçus pour les utilisateurs finaux. Elle permet la communication entre les applications et fournit des services de haut niveau tels que le courrier électronique, la navigation web, etc.	**HTML, FTP, SSL/TLS, PPTP**
6	***Présentation***	Elle est responsable de la traduction, de la compression et du chiffrement des données. Elle s'occupe de la représentation des données pour l'application.	**SSL/TLS**
5	***Session***	Cette couche gère l'ouverture, la fermeture et la gestion des sessions de communication. Elle assure la coordination et la synchronisation des échanges entre les applications.	**PPTP, FTP**
4	***transport***	La couche transport est responsable du contrôle de la fiabilité et du flux de données entre deux hôtes. Elle gère la segmentation, la réassemblage, la vérification de l'intégrité des données, et assure un contrôle de flux.	**UDP, TCP**
3	***Réseau***	Cette couche est responsable de l'acheminement des paquets de données à travers un réseau. Elle gère la détermination du meilleur chemin (routage) et les adresses logiques.	**routeur,IPv4, IPv6,**
2	***Liaison***	Elle décompose les données à transmettre en trames pour les transmettre à la couche physique et s'occupe de la gestion des connexions entre deux nœuds adjacents, la détection d'erreurs, le contrôle d'accès au support de transmission et le MAC (Media Access Control).	**Ethernet, MAC, Wi-Fi, câble RJ45**
1	***physique***	Elle englobe les aspects matériels de la communication, tels que les signaux électriques, les câbles, les interfaces, et les technologies de transmission. C'est l'endroit où le flux binaire brut est physiquement transmis sur un support physique.	**câble RJ45 , Fibre optique**

JOB 13

➔ *Quelle est l'architecture de ce réseau ?*

L'architecture de ce réseau est une adresse IP de classe C, car le masque de sous-réseau 255.255.255.0 est typique des réseaux de classe C. De surcroît, le premier intervalle d'octets est situé entre 192 et 223 ce qui correspond également à une adresse de classe C.

➔ *Indiquer quelle est l'adresse IP du réseau ?*

L'adresse IP du réseau est ***192.168.10.0***

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

En se basant sur le masque de sous réseau 255.255.255.0 , on dispose de 8 bits pour les adresses d'hôtes ce qui donne un total de 2^8 = 256 adresses IP uniques dans le sous réseau. Cependant, certaines adresses sont réservées, donc le nombre d'adresses d'hôtes disponibles est un de moins que 256. Dans ce cas, vous pouvez brancher jusqu'à 255 machines (de 1 à 254) sur ce réseau.

➔ *Quelle est l'adresse de diffusion de ce réseau ?*

L'adresse de diffusion de ce réseau est l'adresse IP la plus élevée possible dans le sous-réseau. L'adresse de diffusion est 192.168.10.255, car le dernier octet est à 255.

JOB 14

Convertissez les adresses IP suivantes en binaires :

- **145.32.59.24 = 10010001.0010000.00111011.00011000**
- **200.42.129.16 = 11001000.00101010.10000001.00010000**
- **14.82.19.54 = 00001110.01010010.00010011.00110110**

JOB 15

➔ *Qu'est-ce que le routage ?*

Le routage réseau est le processus de sélection d'un chemin à travers un ou plusieurs réseaux, que ce soit un réseau local (LAN), un réseau étendu (WAN), ou même Internet. Le routage consiste à déterminer le meilleur chemin ou l'itinéraire à suivre pour que les données atteignent leur destination de manière efficace.

➔ *Qu'est-ce qu'un gateway ?*

Un "gateway" (en français, une passerelle) est un dispositif matériel ou un logiciel qui agit comme un intermédiaire entre deux réseaux informatiques ou systèmes différents pour faciliter la communication et l'échange de données entre eux. La plupart du temps, la passerelle applicative a pour mission de relier un réseau local à Internet. La gateway la plus connue est la box Internet.

➔ *Qu'est-ce qu'un VPN ?*

Un VPN (Virtual Private Network) est un outil de sécurité et de confidentialité en ligne qui permet de créer une connexion sécurisée et chiffrée entre votre appareil (comme un ordinateur,

un smartphone ou une tablette) et un serveur distant. Il décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de 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, tel que www.google.com.b