

## *Runtrack Réseau*



### *Job02*

Après l'installation de packet tracer au Job01 .

#### 1\_Définition :

Un réseau informatique est comme une toile d'araignée numérique qui permet aux appareils de se parler et de partager des données, il 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.

#### 2\_A quoi sert un réseau informatique:

Les **réseaux informatiques** sont utilisés pour effectuer un grand nombre de tâches grâce au partage de l'information:

- Accès à Internet .
- Sauvegarde et récupération de données .
- Partage de ressources.
- Communication .
- Accès à distance .

En résumé ,un réseau informatique est un outil essentiel pour connecter des appareils et des utilisateurs, pour la communication, ce qui améliore considérablement l'efficacité et la productivité dans de nombreux domaines.

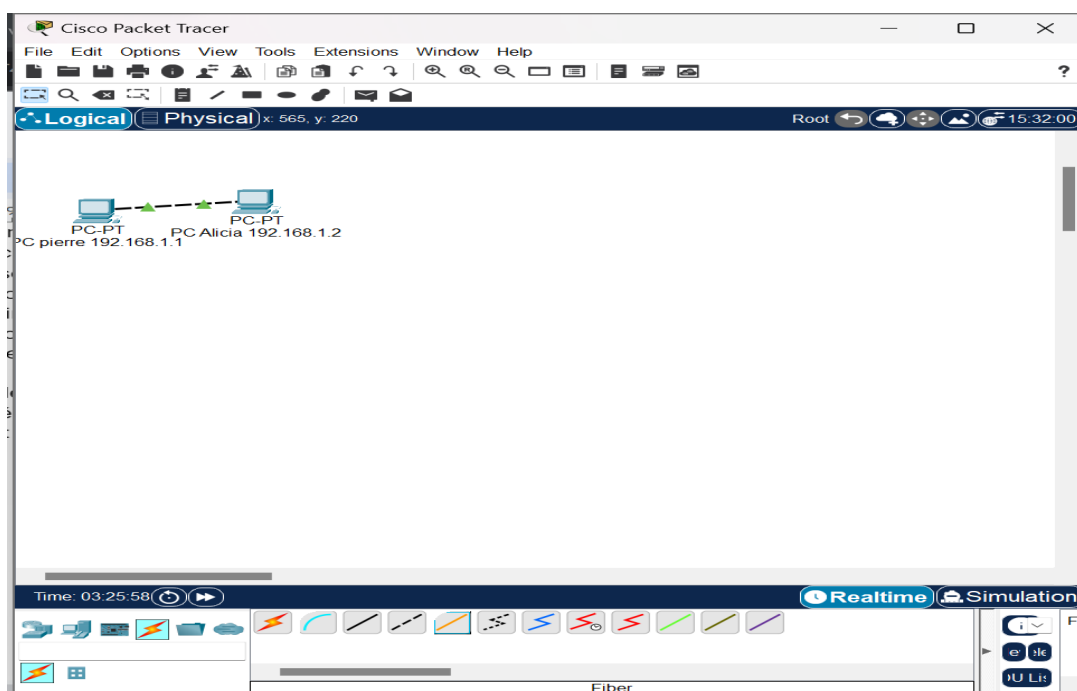
#### 3\_Matériel nécessaire pour construire un réseau :



Pour construire un réseau on a besoin de matériel suivant :

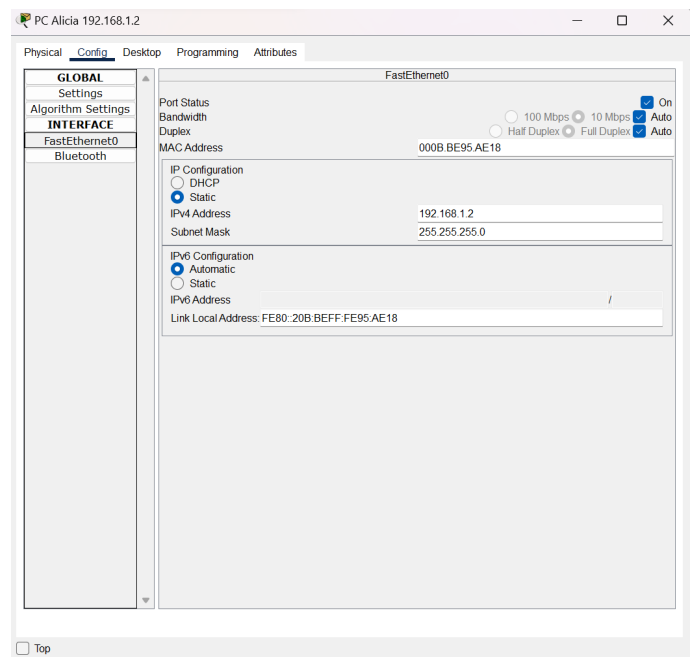
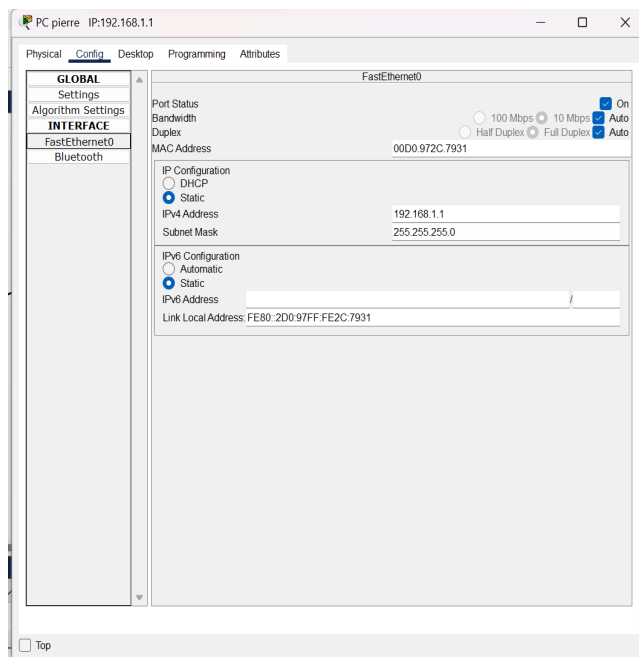
- Des ordinateurs : tels que des ordinateurs de bureau, des ordinateurs portables, des smartphones, des tablettes.  
Ils accèdent au réseau pour partager des informations, des ressources et utiliser les services.
- Une box : Le rôle d'une box dans un réseau informatique est essentiel, car elle exécute plusieurs fonctions clés notamment : wifi , sécurité ,connexion internet ....
- Un serveur : il remplit plusieurs fonctions critiques pour permettre la communication, le stockage de données et l'accès aux ressources dans un réseau.
- Un serveur dhcp et dns : Deux serveurs garantissent que les appareils peuvent se connecter au réseau et accéder aux ressources en utilisant des noms conviviaux. Le serveur DHCP attribue des configurations réseau aux appareils est des adresses IP. et le serveur DNS assure la résolution des noms de domaine en adresses IP .
- Un routeur : un composant clé pour l'acheminement du trafic, la gestion de la connectivité entre différents réseaux et la sécurité dans un réseau informatique. Il garantit que les données sont acheminées de manière efficace et sécurisée entre les dispositifs connectés au réseau .
- Un switch : Faciliter la communication entre les appareils connectés au sein d'un même réseau local en acheminant les données de manière efficace, en améliorant la bande passante, en segmentant le réseau et en réduisant la diffusion de données inutiles.

## Job03



➡ Pour connecter directement les deux ordinateurs sans passer par un routeur ou un commutateur, on utilise un câble croisé. Les broches à chaque extrémité du câble sont inversées, ce qui permet aux deux dispositifs de communiquer directement.

## Job04



### Définition et rôle d'une adresse IP :

"Internet Protocol Address" en anglais, est une étiquette numérique attribuée à chaque dispositif connecté à un réseau informatique qui utilise le protocole Internet (IP).

L'adresse IP est une sorte de code qui permet l'identification de chaque terminal connecté au réseau internet, sont en jeu pour assurer la communication et l'acheminement des informations et sert principalement à identifier de manière unique chaque dispositif ou point d'accès sur un réseau informatique, notamment sur Internet.

### Définition d'une adresse MAC :

L'adresse MAC ( **Media Access Control**) est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est sensée être unique au monde.

Les adresses MAC sont gravées en usine dans le matériel et sont permanentes. Elles servent à identifier de manière unique chaque interface réseau sur un réseau local.

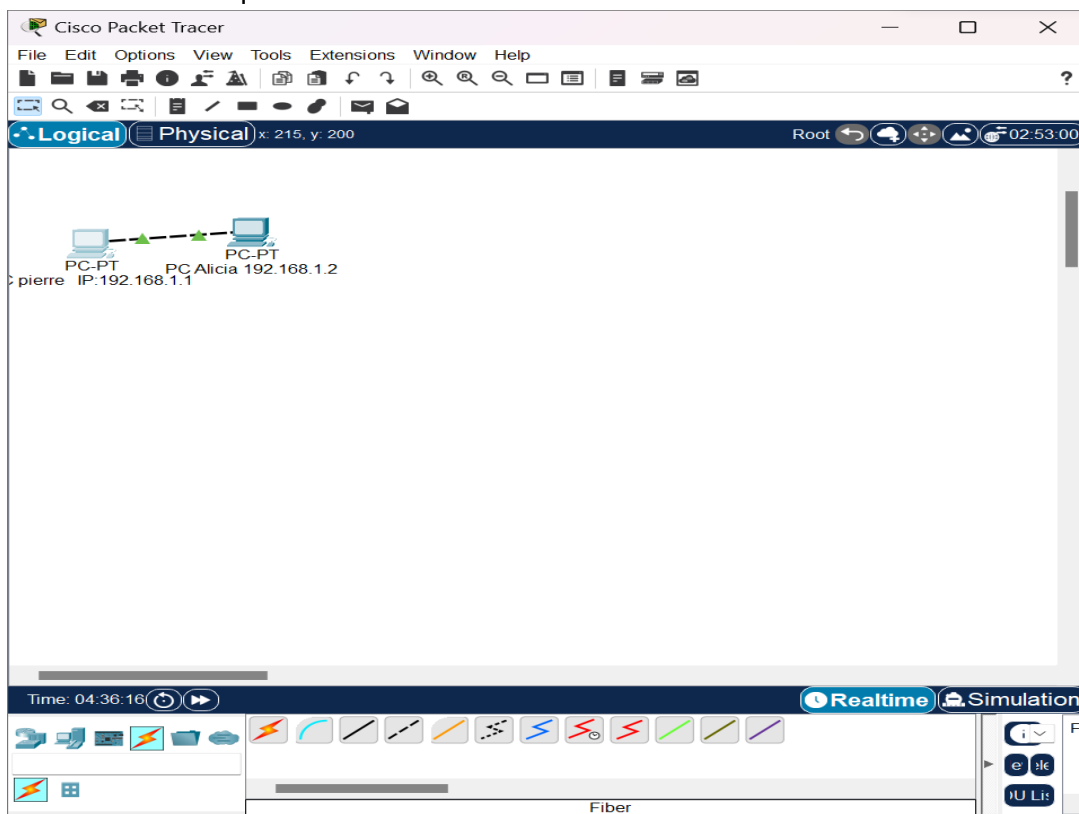
### IP publique et privée :

Une adresse **IP publique** nous identifie auprès du réseau Internet, de telle sorte que toutes les informations que nous recherchons puissent nous 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 .

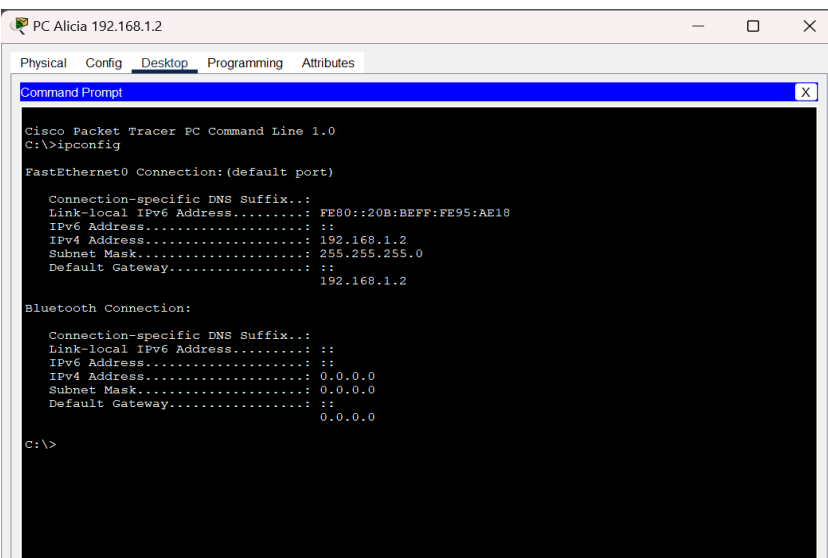
### L'adresse de ce réseau :

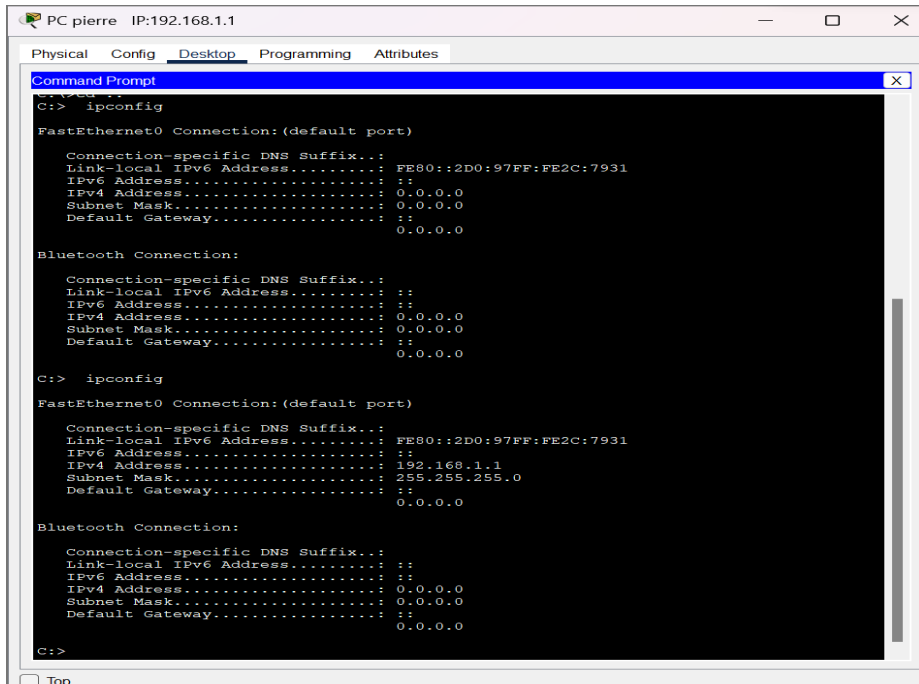
C'est l'adresse masque de sous-réseau : **255.255.255.0**



**Job05**

**PC Alicia .**





```
PC pierre IP:192.168.1.1
Physical Config Desktop Programming Attributes
Command Prompt
C:\> ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::2D0:97FF:FE2C:7931
    IPv6 Address...: ::
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    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:\> ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: FE80::2D0:97FF:FE2C:7931
    IPv6 Address...: ::
    IPv4 Address...: 192.168.1.1
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
    0.0.0.0

Bluetooth Connection:

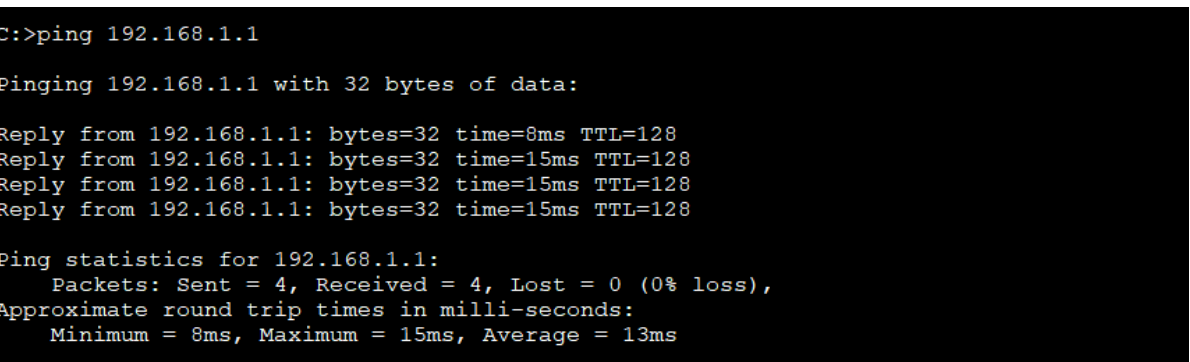
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: ::
    IPv6 Address...: ::
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    Default Gateway...: ::
    0.0.0.0

C:\>
```

*PC Pierre.*

La ligne de commande utilisée pour vérifier l'id des machines : Ipconfig

## Job06



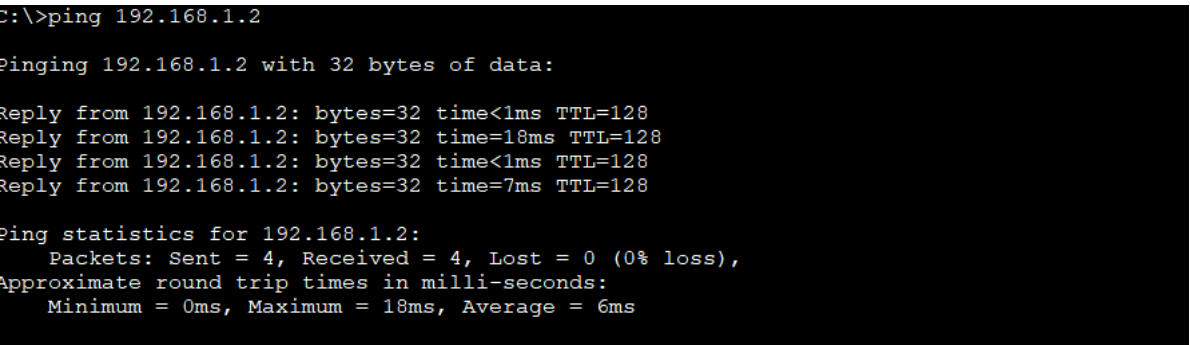
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=8ms TTL=128
Reply from 192.168.1.1: bytes=32 time=15ms TTL=128
Reply from 192.168.1.1: bytes=32 time=15ms TTL=128
Reply from 192.168.1.1: bytes=32 time=15ms 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 = 8ms, Maximum = 15ms, Average = 13ms
```

*Pc Pierre .*



```
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
Reply from 192.168.1.2: bytes=32 time=18ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms 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 = 0ms, Maximum = 18ms, Average = 6ms
```

*Pc Alicia.*



**La ligne de commande permettant le ping entre deux PC :** `ping` [adresse IP de PC Pierre ou pc Alicia]

---

## **Job07**

```
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:\>
```

⇒ Si le PC de Pierre est éteint, il ne sera pas en mesure de répondre aux paquets PING envoyés par Alicia et ,il ne peut pas répondre aux requêtes PING car il n'est pas actif sur le réseau .  
Donc Alicia ne recevra pas de réponse aux paquets PING, car le PC cible est inactif sur le réseau.

---

## **Job08**

### **La différence entre un hub et un switch :**

Un hub et un switch sont deux dispositifs utilisés pour interconnecter des appareils au sein d'un réseau. La principale différence entre un hub et un switch réside dans la manière dont ils gèrent le trafic sur un réseau. Un hub doit en plus partager sa bande passante avec chacun de ses ports. En comparaison, un commutateur (switch) conserve un registre des adresses MAC (Media Access Control) de tous les appareils qui y sont connectés.

### **Comment fonctionne un hub , ses avantages et inconvénients :**

Un hub transfère toutes les données à tous les appareils connectés, sans distinction, en mode semi-duplex. Tous les ports d'un hub fonctionnent à la même vitesse et partagent un même domaine de collision.

Contrairement à d'autres périphériques réseau, un hub ne peut pas cibler ou exclure spécifiquement des destinataires. Cela signifie que lors du transfert de données, tous les appareils reçoivent toutes les données, même si elles ne leur sont pas destinées. Cela peut provoquer une congestion, empêchant d'autres appareils d'envoyer des données simultanément, car les demandes sont traitées séquentiellement.

### **Inconvénients :**

- - La technologie des hubs est obsolète et vulnérable.
- - Elle provoque des pertes de vitesse et offre peu de flexibilité pour le transfert de données.
- - Les systèmes de hubs sont vulnérables aux failles de sécurité car le trafic de données n'est pas isolé.
- - Les problèmes de sécurité et de protection des données concernent tous les appareils connectés à un hub.

### **Avantages :**

- - Les hubs sont de moins en moins utilisés aujourd'hui en raison de leur manque de flexibilité et de la perte de vitesse qu'ils entraînent.
- - Ils peuvent encore être utiles pour les réseaux plus anciens.
- - Ils peuvent être utilisés pour diffuser du contenu multimédia vers plusieurs appareils.
- - Les hubs sont adaptés à des analyses réseau, car ils ne nécessitent pas de miroirs de port supplémentaires pour la lecture et l'analyse des données.

## **Les avantages et inconvénients d'un switch :**

### **Avantages :**

- Les switches augmentent la capacité de transfert de données accessible de l'organisation.
- Réduction Ils réduisent la charge exceptionnelle sur les ordinateurs hôtes individuels.
- Les switches améliorent les performances de l'organisation.
- Les réseaux utilisant des switches ont moins d'impacts sur le réseau grâce à la création de zones d'impact pour chaque connexion.
- Les switches peuvent être directement associés aux postes de travail.
- Ils augmentent la bande passante disponible du réseau.
- Les réseaux utilisant des switches ont moins de collisions de trames.
- Les données vont uniquement à leur destination, ce qui renforce la sécurité.

### **Inconvénients :**

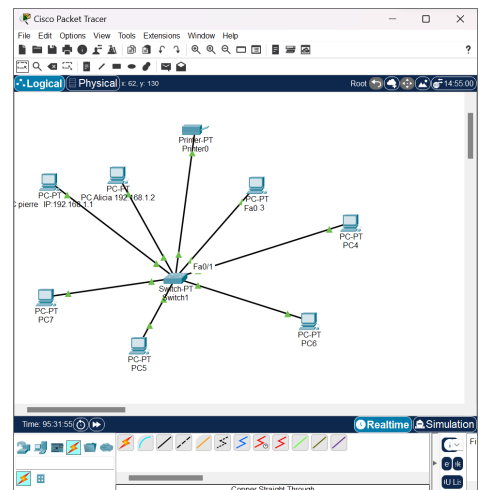
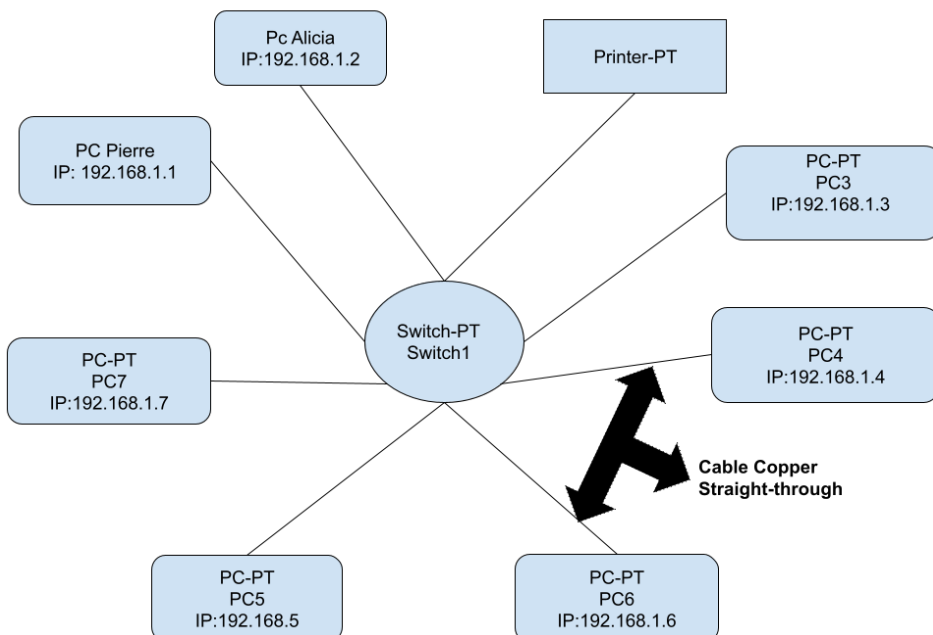
- Les switches sont plus coûteux que les hubs.
- Les problèmes de disponibilité du réseau sont difficiles à suivre avec une architecture basée sur des switches.
- Le trafic de diffusion peut être problématique.
- Si les switches sont mal configurés, ils peuvent être vulnérables à des attaques de sécurité, telles que le spoofing d'adresse IP ou la capture de trames Ethernet.

- Une planification et une configuration appropriées sont nécessaires pour traiter le trafic de multidiffusion.
- Les composants mécaniques du switch peuvent s'user avec le temps.
- Les switches nécessitent un contact physique pour être actionnés.

### Comment un switch gère-t-il le trafic réseau :

Un switch gère un réseau en filtrant le trafic en fonction des adresses MAC, éliminant les collisions, créant des segments logiques, priorisant le trafic, permettant l'analyse du trafic, prévenant les boucles réseau, connectant différents réseaux, offrant des fonctionnalités de redondance, et en organisant efficacement le transfert de données pour améliorer les performances et la sécurité du réseau local.

#### ***Job09***



### Avantages importants d'avoir un schéma :

- Un schéma de réseau offre une documentation visuelle facilitant la compréhension pour les utilisateurs et les administrateurs.
- Ils permettent de visualiser les relations entre les différents éléments d'un concept de manière claire et concise.
- Il montre clairement la structure actuelle du réseau et les possibilités d'extension.





## **Job10**

### **La différence entre une adresse IP statique et une adresse IP attribuée par DHCP:**

Les adresses IP statiques conservent une adresse IP permanente pour chaque dispositif réseau, mais nécessitent une configuration manuelle et une gestion précise pour éviter les conflits d'adresses. Le DHCP est un protocole qui automatise l'attribution des adresses IP, facilitant la tâche des administrateurs en évitant la configuration manuelle répétitive. Il est particulièrement utile pour gérer de nombreux appareils, comme les points d'accès sans fil, de manière efficace et économique. Le DHCP offre des avantages tels que la réduction des coûts et de la maintenance par rapport aux adresses IP statiques, tout en nécessitant moins d'efforts administratifs.

---

## **Job11**

### **→ Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A :**

La sélection d'une adresse de classe A telle que 10.0.0.0 a été déterminée par sa capacité à offrir une vaste étendue d'adresses, ce qui s'avère particulièrement avantageux pour satisfaire les exigences de ce réseau composé de 21 sous-réseaux distincts.

La distinction fondamentale entre les diverses classes d'adresses repose principalement sur l'ampleur de l'espace d'adressage disponible et sur la structure de leur format.

### **→ le plan d'adressage :**

#### **❖ 1 sous-réseau de 12 hôtes :**

<b><u>CDIR</u></b>	Masque de Sous-réseau	adresse de sous-réseau	Plage d'Adresse IP	Adresse de Diffusion
<b><u>/28</u></b>	255.255.255.240	10.1.0.0	10.0.0.1- 10.0.0.14	10.0.0.15

#### **❖ 5 sous-réseaux de 30 hôtes :**

<b><u>CDIR</u></b>	Masque de sous-réseau	adresse de sous-réseau	Plage d'Adresse IP	Adresse de Diffusion
<b>/27</b>	255.255.255.224	10.2.0.0	10.2.0.1 - 10.2.0.30	10.2.0.31
<b>/27</b>	255.255.255.224	10.3.0.0	10.3.0.1 - 10.3.0.30	10.3.0.31
<b>/27</b>	255.255.255.224	10.4.0.0	10.4.0.1 - 10.4.0.30	10.4.0.31
<b>/27</b>	255.255.255.224	10.5.0.0	10.5.0.1 - 10.5.0.30	10.5.0.31
<b>/27</b>	255.255.255.224	10.6.0.0	10.6.0.1 - 10.6.0.30	10.6.0.31

❖ **5 sous-réseaux de 120 hôtes :**

<b><u>CDIR</u></b>	Masque de sous-réseau	adresse de sous-réseau	Plage d'Adresse IP	Adresse de Diffusion
<b>/25</b>	255.255.255.128	10.7.0.0	10.7.0.1 à 10.7.0.126	10.7.0.127
<b>/25</b>	255.255.255.128	10.8.0.0	10.8.0.1 à 10.8.0.126	10.8.0.127
<b>/25</b>	255.255.255.128	10.9.0.0	10.9.0.1 à 10.9.0.126	10.9.0.127
<b>/25</b>	255.255.255.128	10.10.0.0	10.10.0.1 à 10.10.0.126	10.10.0.127
<b>/25</b>	255.255.255.128	10.11.0.0	10.11.0.1 à 10.11.0.126	10.11.0.127

❖ **5 sous-réseaux de 160 hôtes :**

<b><u>CDIR</u></b>	Masque de sous-réseau	Adresse de sous-réseau	Plage d'Adresse IP	Adresse de Diffusion
<b>/24</b>	225.225.255.0	10.12.0.0	10.12.0.0 à 10.12.0.254	10.12.0.254
<b>/24</b>	225.225.225.0	10.13.0.0	10.13.0.0 à 10.13.0.254	10.13.0.254
<b>/24</b>	225.225.225.0	10.14.0.0	10.14.0.0 à 10.14.0.254	10.14.0.254
<b>/24</b>	225.225.225.0	10.15.0.0	10.15.0.0 à 10.15.0.254	10.16.0.254
<b>/24</b>	225.225.225.0	10.16.0.0	10.16.0.0 à 10.16.0.254	10.16.0.254

## ***Job12***

### **Couche OSI :**

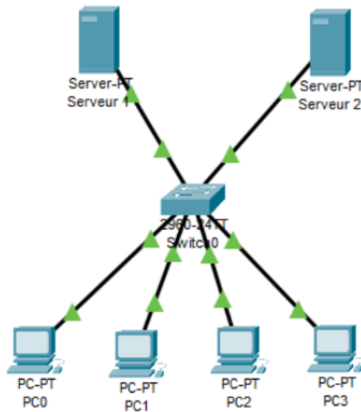
Le modèle OSI " **Open Systems Interconnection** ", représente un cadre conceptuel essentiel pour la communication et le transfert de données entre systèmes réseau. Son objectif principal est de décomposer la communication en plusieurs composants pour établir des normes et des règles cohérentes au sein des applications et de l'infrastructure réseau. Composé de sept couches empilées du bas vers le haut, le modèle OSI joue un rôle fondamental dans la structuration des échanges de données.

<b><i>Couche OSI</i></b>	<b><i>description des rôles</i></b>	<b><i>matériels et protocoles associés</i></b>
<b>1</b> _ La couche physique.	Responsable de l'équipement qui facilite le transfert des données, comme les câbles et les routeurs installés sur le réseau.	Fibre optique, câble RJ45, Wi-Fi
<b>2</b> _ La couche de liaison de données.	Responsable du transfert des informations sur le même réseau. Transforme les paquets reçus de la couche réseau en trames. Responsable du contrôle des erreurs et du flux pour garantir la réussite de la transmission.	Ethernet, MAC, câble RJ45, Wi-Fi
<b>3</b> _ La couche réseau.	Chargée de décomposer les données sur l'appareil de l'expéditeur et de les réassembler sur l'appareil du destinataire lorsque la transmission s'effectue sur deux réseaux différents .	IPv4, IPv6, routeur
<b>4</b> _ La couche de transport	La couche transport du modèle OSI divise les données en segments plus petits pour une transmission efficace sur le réseau. Chacun de ces segments est accompagné d'informations d'en-tête cruciales pour le réassemblage. De plus, des mécanismes de contrôle d'erreur garantissent l'intégrité des données et la réémission en cas de perte de paquets.	TCP, UDP
<b>5</b> _ La couche session.	Chargée de s'assurer que le fichier est transféré dans son intégralité et que la retransmission est établie si les données sont incomplètes.	PPTP, SSL/TLS, FTP
<b>6</b> _ La couche de présentation.	Responsable de l'encodage et du décodage des informations afin qu'elles puissent être affichées en clair. Responsable de la compression et de la décompression des données lorsqu'elles passent d'un appareil à un autre	SSL/TLS, HTML
<b>7</b> _ La couche	Elle communique directement avec l'utilisateur.	FTP, HTML, PPTP,



d'application.	Fournit des services de réseau aux applications..	SSL/TLS
----------------	---	---------

## Job13



- PC0 : **192.168.10.6**
- PC1 : **192.168.10.7**
- PC2 : **192.168.10.8**
- PC3 : **192.168.10.9**
- Serveur 1 : **192.168.10.100**
- Serveur 2 : **192.168.10.200**

Avec un masque de sous-réseau :  
**255.255.255.0**

### → L'architecture de ce réseau est :

La configuration de ce réseau suit une architecture en étoile la topologie la plus courante actuellement, dans laquelle chaque appareil, qu'il s'agisse d'un PC ou d'un serveur, est connecté directement au réseau local (LAN) par le biais d'un commutateur ou d'un routeur central.

Cette disposition assure que chaque appareil est directement relié au commutateur/routeur principal, ce qui simplifie la gestion et la communication au sein du réseau.

### → L'adresse IP du réseau :

J'ai calculé l'adresse IP du réseau en utilisant l'adresse IP du PC0 (192.168.10.6) et le masque de sous-réseau (255.255.255.0). L'adresse IP du réseau est la première adresse possible dans la plage d'adresses définie par le masque de sous-réseau. Dans ce cas, le masque de sous-réseau 255.255.255.0 signifie que les 24 premiers bits de l'adresse IP sont réservés pour le réseau, et les 8 bits restants sont disponibles pour les hôtes.

Donc, pour trouver l'adresse IP du réseau, j'ai "masqué" les 24 premiers bits de l'adresse IP du PC0 avec des zéros, ce qui donne **192.168.10.0**. C'est donc l'adresse IP du réseau auquel appartiennent PC0, PC1, PC2, PC3, Serveur 1 et Serveur 2.

### → le nombre des machines que l'on peut brancher sur ce réseau:

Le masque de sous-réseau 255.255.255.0 s'agit d'un masque de sous-réseau de la classe C donc il peut allouer 24 bits pour l'adresse réseau et 8 pour les adresses des machines .

Donc on a  $2^8 - 2$  ( IP 0 et 255 de la plage sont réservés )

Donc le nombre des machines que ce réseau peut avoir est : **254 Machines.**



## → L'adresse de diffusion de ce réseau :

On peut brancher sur ce réseau 254 machines et on a le masque de sous-réseau est 255.255.255.0, ce qui signifie que les trois premiers octets (192.168.10) correspondent à l'adresse réseau, et le dernier octet (0) est réservé pour les adresses des machines. Donc, l'adresse de diffusion pour ce réseau serait **192.168.10.255**.

---

## **Job14**

## → Les adresses IP converties en binaire :

✓ 145.32.59.24 :

- 145 en binaire : 10010001
- 32 en binaire : 00100000
- 59 en binaire : 00111011
- 24 en binaire : 00011000

Adresse IP en binaire : **10010001.00100000.00111011.00011000**

✓ 200.42.129.16 :

- 200 en binaire : 11001000
- 42 en binaire : 00101010
- 129 en binaire : 10000001
- 16 en binaire : 00010000

Adresse IP en binaire : **11001000.00101010.10000001.00010000**

✓ 14.82.19.54 :

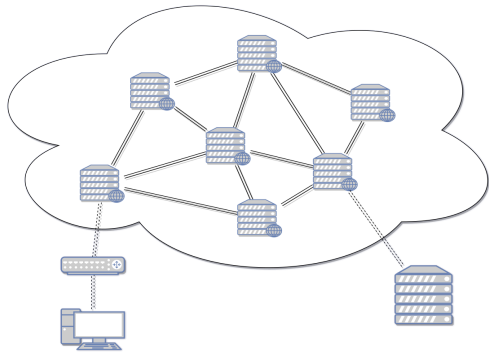
- 14 en binaire : 00001110
- 82 en binaire : 01010010
- 19 en binaire : 00010011
- 54 en binaire : 00110110

Adresse IP en binaire : **00001110.01010010.00010011.00110110**

---

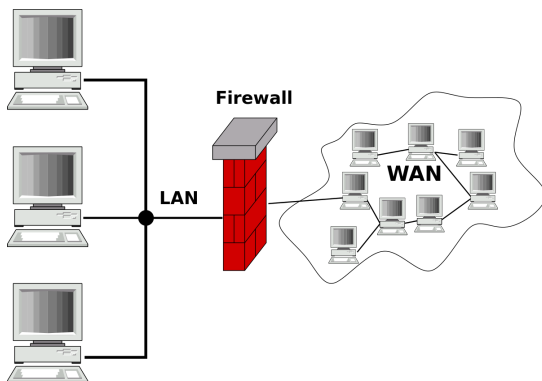
## Job15

### Le routage :



Le routage est le procédé de détermination du trajet optimal au sein d'un réseau. Un réseau informatique se compose de diverses machines, connues sous le nom de nœuds, qui sont reliées entre elles par des chemins ou des liaisons. Lorsqu'il faut établir une communication entre deux nœuds dans un réseau complexe, il existe plusieurs itinéraires possibles. Le routage consiste à choisir le chemin optimal en se basant sur des règles préétablies, afin d'assurer une transmission efficace des données.

### UN Gateway :



Une passerelle applicative est un système, à la fois matériel et logiciel, qui établit la connexion entre deux réseaux informatiques ou de télécommunications présentant des caractéristiques différentes. Son rôle principal consiste généralement à relier un réseau local à Internet, et un exemple bien connu de passerelle applicative est une box Internet.

### UN VPN :



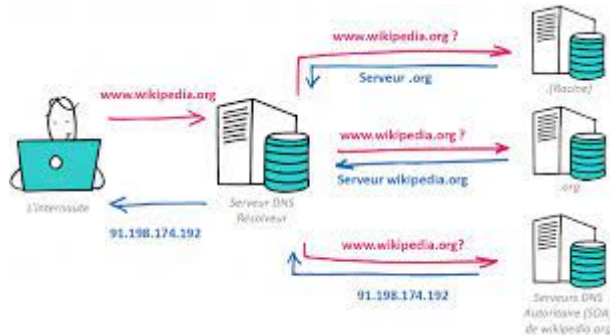
Un VPN, ou Réseau Privé Virtuel, représente la capacité d'établir une connexion réseau sécurisée lorsqu'on utilise des réseaux publics. Les VPN cryptent le flux de données sur Internet et masquent votre

identité en ligne.

Cela complique la

tâche des tiers qui souhaitent surveiller vos activités en ligne ou accéder à vos données, car le chiffrement est appliqué en temps réel.

## UN DNS:



Le système de noms de domaine (DNS) a été conçu pour simplifier la recherche de sites web sur Internet. Il fonctionne en associant un nom facilement compréhensible à une adresse IP. Cette association relie ainsi un identifiant logique, le nom de domaine, à une adresse physique, l'adresse IP.

Les noms de domaine et les adresses IP sont uniques. Le rôle du DNS est d'acheminer vos communications vers le bon destinataire, en garantissant qu'elles n'atteignent pas quelqu'un d'autre ayant un nom de domaine similaire. De plus, le DNS vous permet de saisir des noms de domaine conviviaux comme "www.exemple.com" au lieu de devoir mémoriser de longues adresses IP, facilitant ainsi l'accès aux sites web appropriés.