



# La Plateforme

*Runtrack Réseau*

Youcef Ouahrhrent

## Job1 :

Afin d'installer Cisco Packet Tracer il faut tout d'abord le télécharger en cliquant ci-dessous :

### Télécharger

LE TÉLÉCHARGEMENT, L'INSTALLATION OU L'UTILISATION DU LOGICIEL CISCO PACKET TRACER CONSTITUE L'ACCEPTATION DU [CONTRAT DE LICENCE DE L'UTILISATEUR FINAL CISCO](#) (le « CLUF ») ET DU [CONTRAT DE LICENCE DE L'UTILISATEUR FINAL SUPPLÉMENTAIRE](#) POUR CISCO PACKET TRACER (le « CLUFS »). SI VOUS N'ACCEPTEZ PAS LES CONDITIONS DU CLUF ET DU CLUFS, VOUS N'ÊTES PAS AUTORISÉ À TÉLÉCHARGER, INSTALLER OU UTILISER LE LOGICIEL.

Les conditions minimales suivantes doivent être remplies pour l'installation et l'exécution de Packet Tracer 8.2 :

1. Cisco Packet Tracer 8.2 (64 bits) :
    - Ordinateur équipé de l'un des systèmes d'exploitation suivants : Microsoft Windows 8.1, 10, 11 (64 bits), Ubuntu 20.04, 22.04 LTS (64 bits) ou MacOS 10.14 ou version ultérieure.
    - Processeur amd64 (x86-64)
    - 4 Go de RAM disponible
    - 1,4 Go d'espace disque disponible
  2. Cisco Packet Tracer 8.2 (32 bits) :
    - Ordinateur équipé de l'un des systèmes d'exploitation suivants : Microsoft Windows 8.1, 10, 11 (32 bits)
    - Processeur compatible x86
    - 2 Go de RAM disponible
    - 1,4 Go d'espace disque disponible
- Afin d'assurer le bon fonctionnement des nouvelles activités et évaluations PTSA, utilisez Cisco Packet Tracer 8.2 64 bits ou une version ultérieure pour le cours CCNA 7.0.2.
  - Cisco Packet Tracer requiert une authentification avec votre adresse e-mail et votre mot de passe lorsque vous l'utilisez pour la première fois et pour chaque nouvelle session du système d'exploitation (voir la note de bas de page 1 ci-dessous).
  - Pour en savoir plus, consultez la [FAQ](#), ainsi que les tutoriels.

#### Bureau Windows, version 8.2.1 (anglais)

[Télécharger la version 64 bits](#)

[Télécharger la version 32 bits](#)

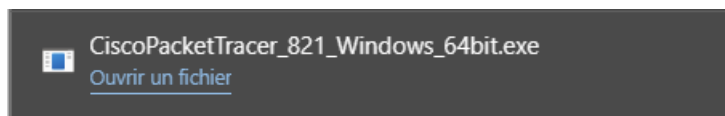
#### Bureau Ubuntu, version 8.2.1 (anglais)

[Téléchargement 64 bits](#)

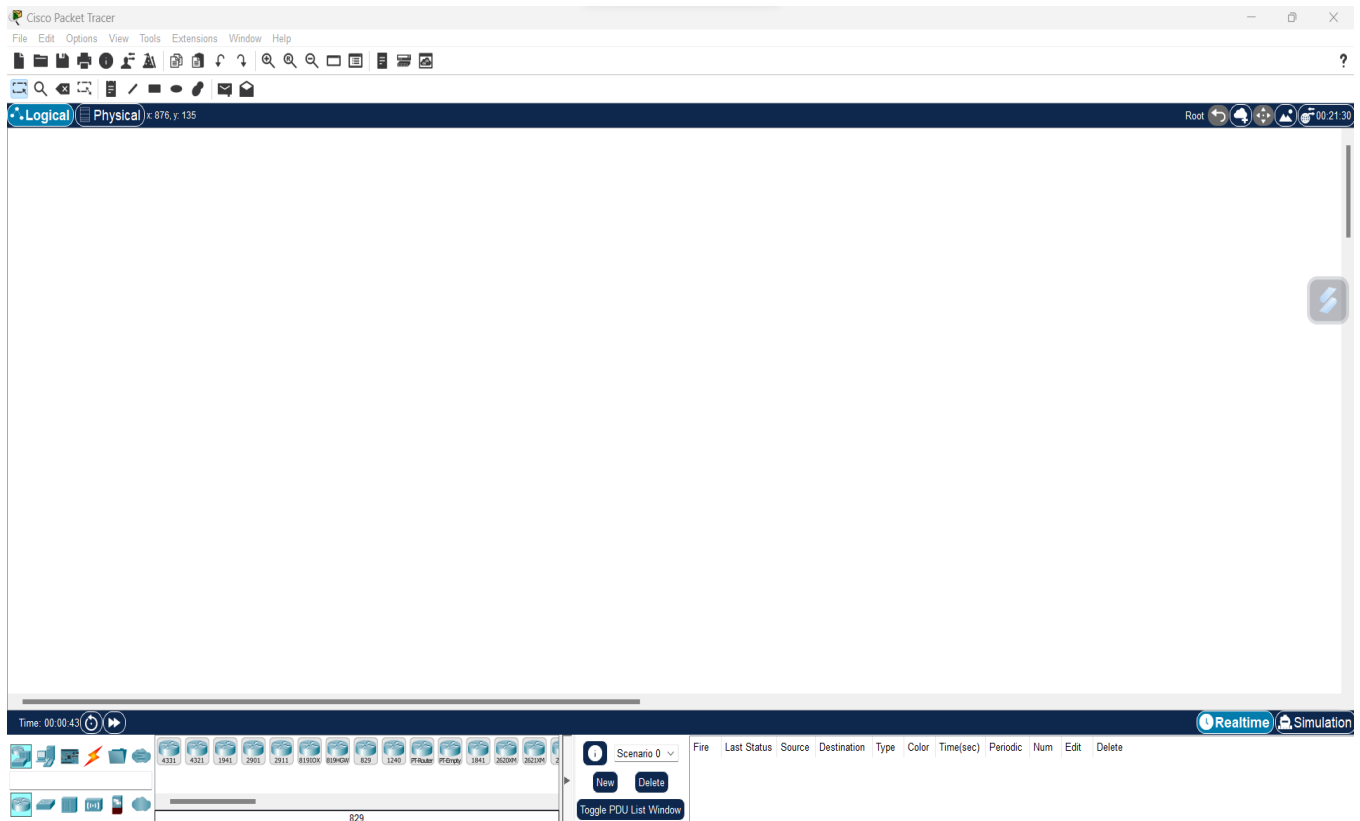
#### MacOS, version 8.2.1 (anglais)

[Télécharger la version 64 bits](#)

Une fois le téléchargement terminée vous ouvrez le fichier et suivez l'installation.



Une fois l'installation terminée il nous faut créer un compte, une fois créer vous devriez normalement avoir accès à Cisco Packet Tracer.



## Job2 :

### →Qu' est-ce qu'un réseau ?

Un réseau est un ensemble d'entités interconnectées qui communiquent entre elles. Ces entités peuvent être des ordinateurs, des périphériques, des personnes ou même des systèmes autonomes. Les réseaux sont utilisés pour partager des informations, des ressources et des services entre les entités connectées. Ils sont omniprésents dans notre monde moderne et jouent un rôle crucial dans les communications, le partage de données et l'accès à Internet.

## →À quoi sert un réseau informatique ?

Un réseau informatique est un ensemble de dispositifs informatiques interconnectés qui communiquent entre eux pour partager des ressources, des données et des informations. Ces réseaux servent à plusieurs fins importantes, notamment :

- **Partage de ressources** : Les réseaux informatiques permettent le partage de ressources telles que des imprimantes, des fichiers, des disques durs, des serveurs, des connexions Internet, et plus encore. Cela permet une utilisation plus efficace des ressources, réduisant ainsi les coûts.
- **Communication** : Les réseaux offrent des moyens de communication efficaces, y compris la messagerie électronique, la messagerie instantanée, la vidéoconférence et la VoIP (voix sur IP). Ils facilitent la communication entre les utilisateurs distants, les organisations et les systèmes informatiques.
- **Accès aux données** : Les réseaux permettent aux utilisateurs d'accéder à des données stockées sur des serveurs ou d'autres périphériques distants. Cela favorise la mobilité et la collaboration, car les utilisateurs peuvent accéder à leurs données de n'importe où.
- **Centralisation de la gestion** : Les réseaux facilitent la gestion centralisée des ressources et des données. Les administrateurs réseau peuvent gérer l'accès aux ressources, les mises à jour logicielles, la sécurité et d'autres aspects depuis un emplacement central.
- **Sauvegarde et récupération des données** : Les réseaux permettent la mise en place de sauvegardes automatiques des données sur des serveurs distants, assurant ainsi la récupération en cas de sinistre ou de perte de données.
- **Sécurité** : Les réseaux jouent un rôle crucial dans la mise en place de mesures de sécurité informatique. Ils permettent de surveiller le trafic, de mettre en œuvre des pare-feu, de gérer l'authentification des utilisateurs et de protéger les données sensibles.
- **Accès à Internet** : Les réseaux locaux (LAN) et étendus (WAN) permettent aux utilisateurs de se connecter à Internet, d'accéder à des informations en ligne, de naviguer sur le web, d'envoyer des courriels, etc.
- **Automatisation des processus** : Les réseaux sont utilisés dans l'automatisation des processus commerciaux et industriels, tels que la surveillance et le contrôle de la production, la gestion des stocks, etc.
- **Partage de connaissances** : Les réseaux sociaux et les plateformes de partage de connaissances en ligne exploitent les réseaux informatiques pour connecter les gens, partager des informations, collaborer sur des projets et échanger des idées.

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

Pour construire un réseau, que ce soit un réseau informatique ou un réseau de communication, vous aurez besoin de divers composants matériels. Les éléments essentiels incluent :

### 1. Dispositifs réseau :

- **Routeurs** : Ils acheminent le trafic entre différentes réseaux. Ils prennent des décisions de routage pour déterminer le chemin optimal pour les données.
- **Commutateurs** : Ils connectent les appareils au sein d'un même réseau local (LAN) et font passer le trafic uniquement entre les appareils nécessaires.
- **Hubs** : Moins courants aujourd'hui, ils diffusent le trafic entrant à tous les appareils connectés, sans tenir compte de la destination.
- **Firewalls** : Ils servent à sécuriser le réseau en filtrant le trafic entrant et sortant pour bloquer les menaces.

## 2. Câblage :

- **Câbles Ethernet** : Ils sont utilisés pour connecter les appareils au réseau filaire. Les câbles Ethernet catégorie 5e, 6 ou 6a sont couramment utilisés pour des débits élevés.
- **Fibres optiques** : Utilisées pour les réseaux à haut débit, elles transmettent la lumière au lieu de signaux électriques.

## 3. Cartes réseau : Les cartes réseau (ou adaptateurs réseau) sont installées dans les ordinateurs et autres dispositifs pour leur permettre de se connecter au réseau. Les cartes sans fil sont utilisées pour les réseaux Wi-Fi.

## 4. Serveurs : Les serveurs sont des ordinateurs puissants qui stockent et partagent des ressources sur le réseau, comme des fichiers, des applications, ou des services.

## 5. Périphériques réseau :

- **Imprimantes réseau** : Elles permettent l'impression depuis n'importe quel ordinateur connecté au réseau.
- **Routeurs sans fil** : Ils ajoutent une connectivité sans fil à un réseau filaire.
- **Points d'accès Wi-Fi** : Utilisés pour étendre la couverture sans fil dans un réseau.

## 6. Modems : Les modems convertissent les signaux numériques des ordinateurs en signaux analogiques pour les transmettre sur des lignes téléphoniques ou câbles, et vice versa.

## 7. Dispositifs de stockage en réseau : Ils permettent le stockage centralisé et partagé de données. Par exemple, les serveurs NAS (Network Attached Storage).

## 8. Équipements de sécurité :

- **Caméras de sécurité réseau** : Utilisées pour surveiller les locaux et les actifs.
- **Systèmes de détection d'intrusion** : Ils aident à protéger le réseau contre les accès non autorisés.

9. **Équipement d'alimentation** : Comprend des onduleurs (pour éviter les coupures de courant), des commutateurs d'alimentation, et des alimentations redondantes pour garantir la disponibilité du réseau.

10. **Rack ou armoire réseau** : Les composants matériels sont souvent logés dans des racks ou armoires spécialement conçus pour l'organisation et la protection.

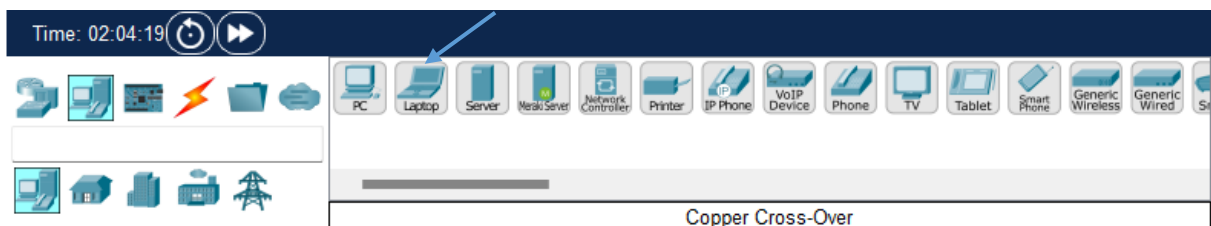
11. **Câblage structuré** : Un système de câblage organisé qui relie tous les composants du réseau de manière systématique. Il inclut des panneaux de brassage, des prises murales, et des chemins de câbles.

Chaque composant remplit un rôle spécifique dans la construction et le fonctionnement d'un réseau. La sélection de ces composants dépend des besoins spécifiques du réseau, de sa taille, de sa complexité et de son budget.

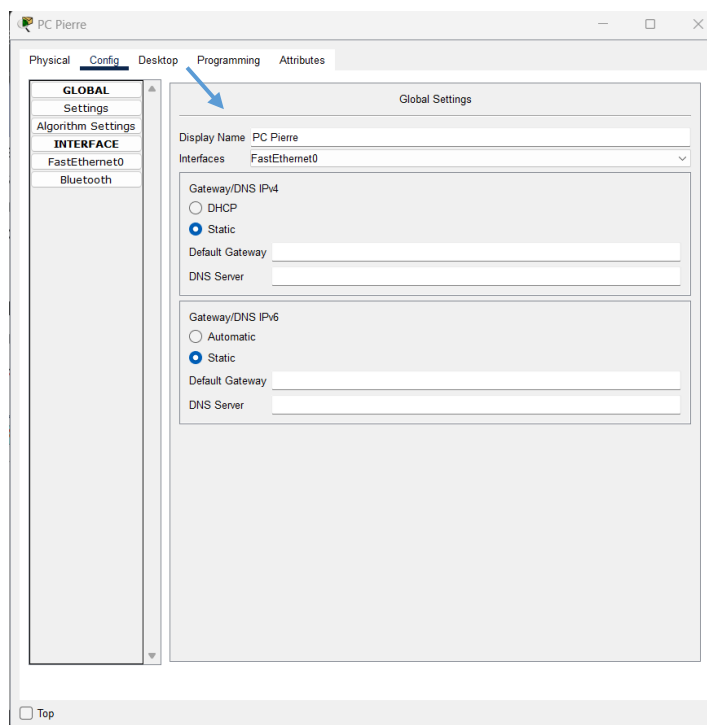
## Job3 :

Pour créer notre premier réseau il nous faut mettre d'abord dans notre zone de travail deux ordinateurs de bureau reliés entre eux par un câble :

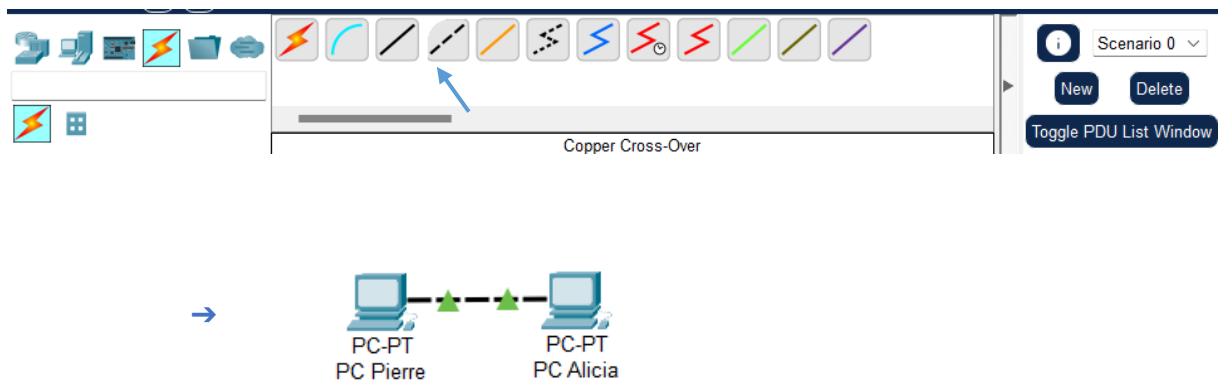
- En bas à gauche, cliquez sur l'icône représentant les ordinateurs, puis on sélectionne le poste de travail classique.



- On ajoute nos deux postes de travail classique à notre zone de travail.
- Pour renommer nos deux postes de travail classique il faut cliquer gauche dessus et on peut le renommer.



Pour les relier on retourne en bas à gauche et on sélectionne  
« Copper Cross-Over »

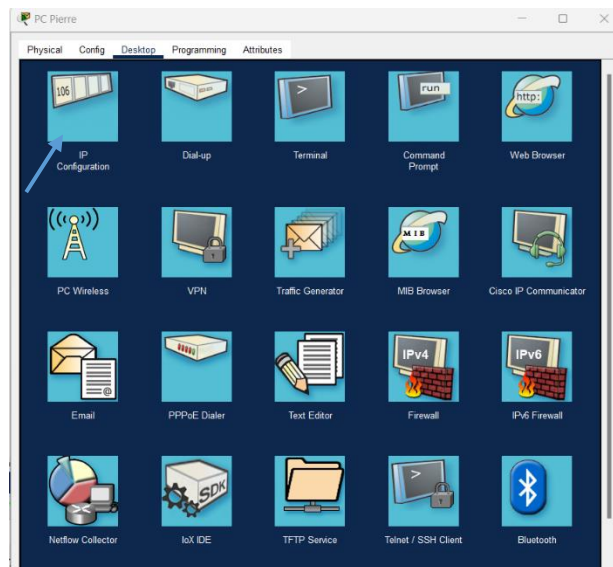


→ Pour relier les deux ordinateurs j'ai choisi un câble croisé car ce câble permet à deux dispositifs de même type de communiquer ensemble.

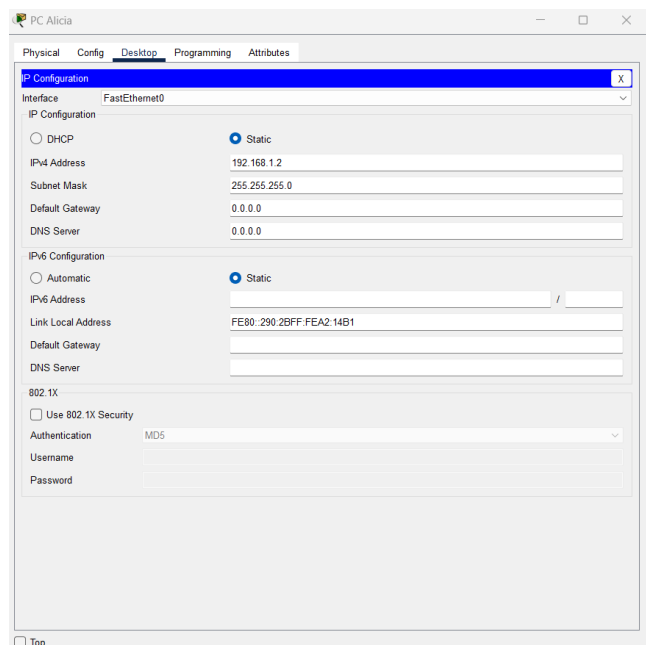
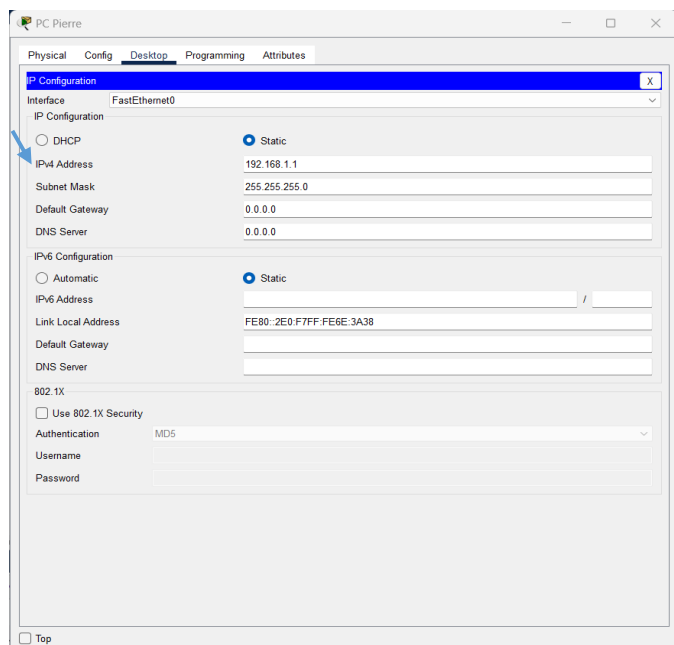


## Job4 :

Pour configurer l'adresse IP des deux ordinateurs il faut cliquer dessus et aller sur « IP Configuration »



Ici on peut ajouter l'adresse IP de l'ordinateur.



On peut voir que « Masque de sous-réseau » se met automatiquement une fois l'adresse IP ajoutée.

## → Qu'est-ce qu'une adresse IP ? et à quoi ça sert.

Une adresse IP, ou adresse Internet Protocol, est un identifiant numérique unique attribué à chaque appareil connecté à un réseau informatique. Elle sert à deux principales choses :

1. **Identifier un appareil** : Les adresses IP permettent d'identifier de manière unique un ordinateur, un smartphone, un serveur ou tout autre dispositif connecté à Internet ou à un réseau local. C'est un peu comme un numéro de téléphone pour les ordinateurs.
2. **Routage des données** : Les adresses IP sont utilisées pour diriger le trafic Internet vers l'appareil approprié. Lorsque vous envoyez des données sur Internet, elles sont découpées en petits paquets, et ces paquets sont acheminés en fonction des adresses IP de destination. En somme, les adresses IP sont essentielles pour permettre la communication et l'échange d'informations entre les appareils connectés à un réseau, qu'il s'agisse d'Internet ou d'un réseau local.

## → Qu'est-ce qu'une adresse MAC ?

Une adresse MAC, ou adresse Media Access Control, est un identifiant unique attribué à une carte réseau ou à un périphérique réseau, comme une carte réseau Ethernet ou une carte Wi-Fi. Cette adresse est généralement constituée de six groupes de chiffres et de lettres hexadécimaux, séparés par des deux-points (par exemple, 00:1A:2B:3C:4D:5E).

L'adresse MAC est utilisée pour identifier de manière unique chaque périphérique sur un réseau local (LAN). Contrairement aux adresses IP, les adresses MAC sont assignées par les fabricants de matériel et ne changent pas, sauf en cas de remplacement du matériel. Les adresses MAC sont essentielles pour le fonctionnement des réseaux locaux, car elles permettent aux routeurs et commutateurs de diriger efficacement le trafic vers les périphériques appropriés.

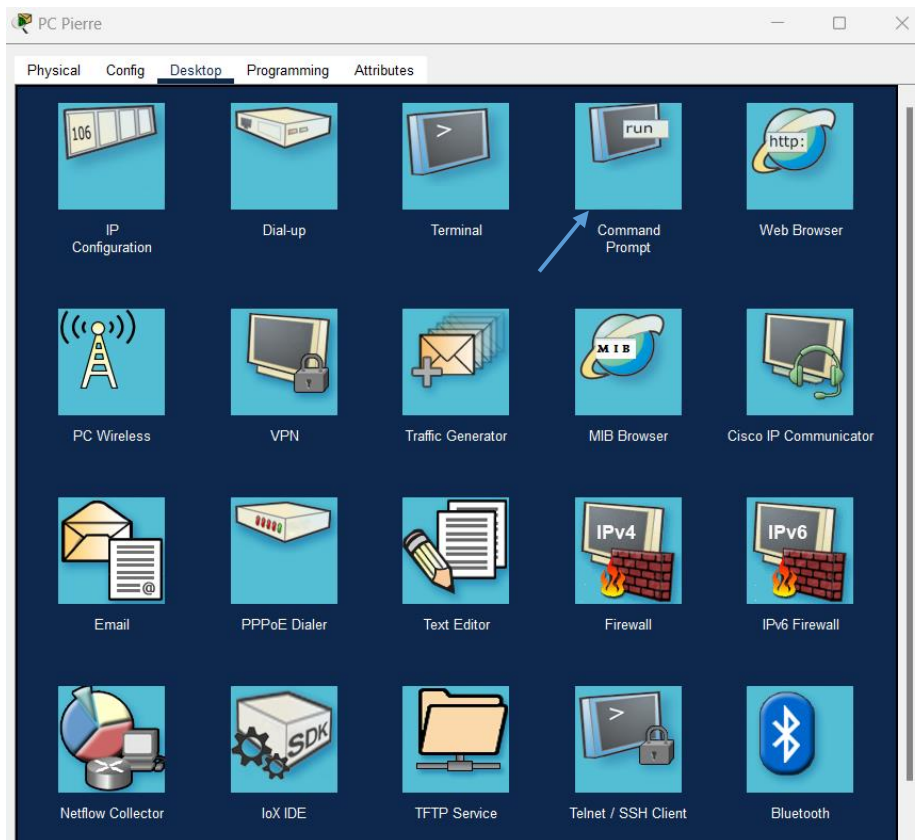
## → Qu'est-ce qu'une IP publique et privée ?

Une adresse IP publique et une adresse IP privée sont deux types d'adresses utilisées pour identifier des appareils sur un réseau, comme Internet.

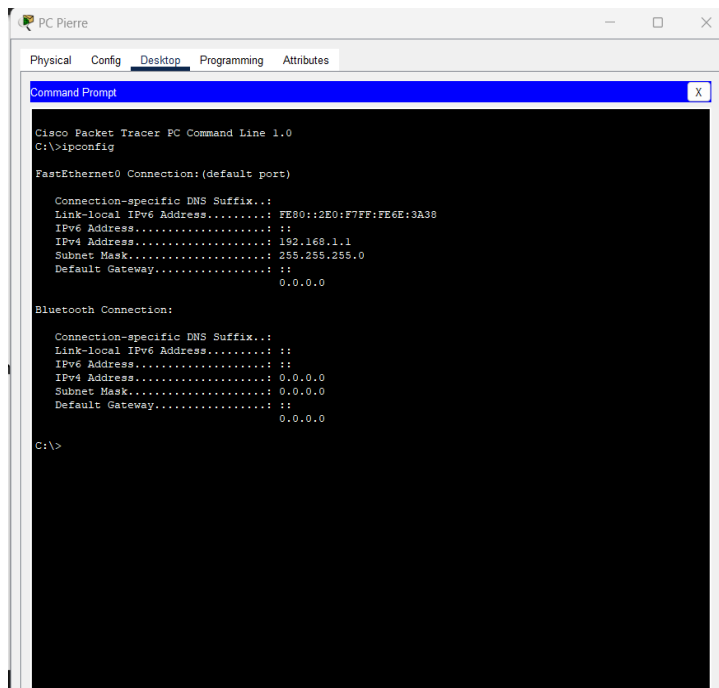
1. **IP Publique** : C'est l'adresse qui est visible depuis Internet. Elle est attribuée à votre routeur ou à votre appareil par votre fournisseur de services Internet (FSI). L'IP publique permet aux appareils de communiquer avec d'autres appareils sur Internet. C'est un peu comme l'adresse de votre maison, connue de tout le monde pour vous envoyer du courrier.
  2. **IP Privée** : C'est l'adresse utilisée à l'intérieur d'un réseau local, comme votre domicile ou votre entreprise. Les appareils connectés à votre routeur reçoivent des IP privées. Ces adresses sont utilisées pour que les appareils se parlent localement, mais elles ne sont pas visibles depuis Internet. C'est un peu comme les numéros de rue à l'intérieur de votre maison, connus uniquement des habitants de la maison pour se repérer.
- En résumé, l'IP publique permet à votre réseau local de communiquer avec Internet, tandis que les IPs privées permettent aux appareils de votre réseau local de communiquer entre eux.

## Job5 :

Pour vérifier que l'IP du « PC de Pierre » est correcte on doit se rendre sur « **Command Prompt** »



Une fois sur le terminal on tape « **ipconfig** » .



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

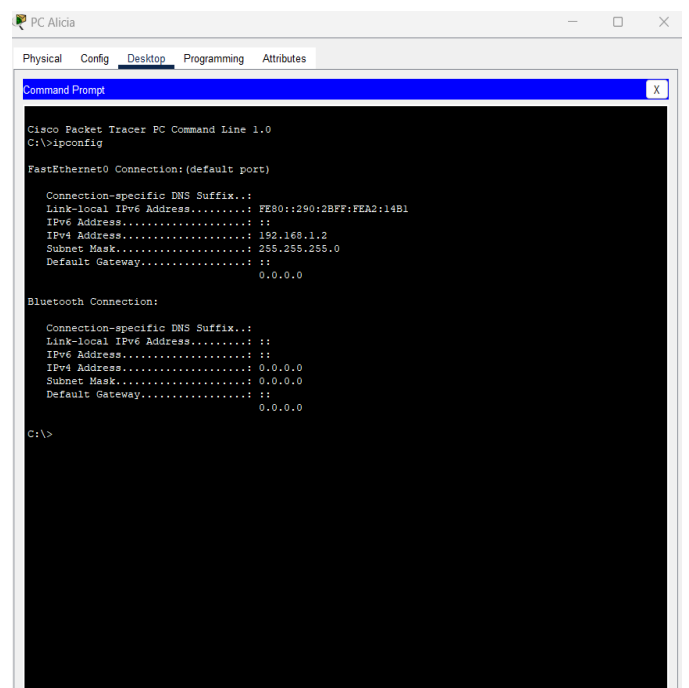
FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F7FF:FE6E:3A38
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::

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 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::290:2BFF:FEA2:14B1
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .:
    0.0.0.0

Bluetooth Connection:

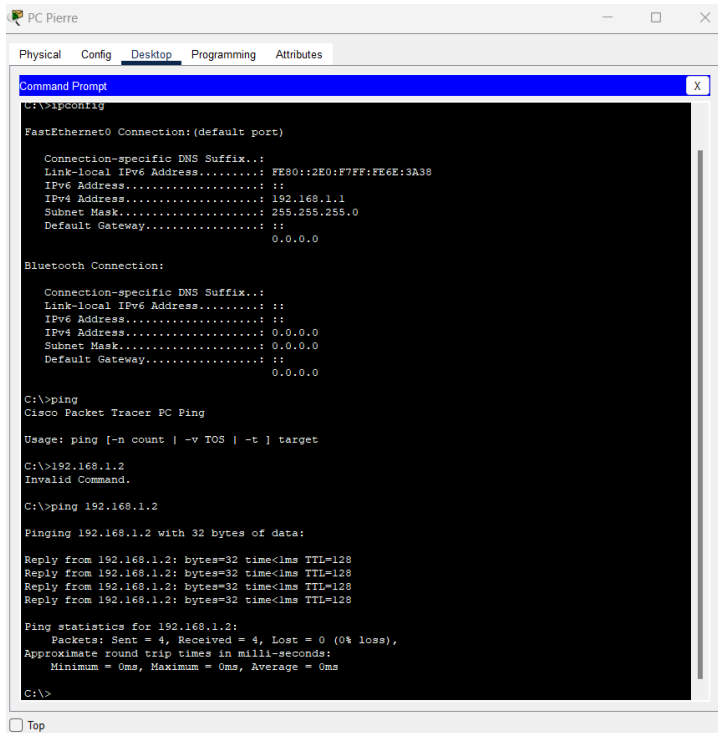
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .:
    0.0.0.0

C:\>
```

## Job6 :

Pour vérifier que la connectivité est bonne entre les deux PC on utilise la commande Ping

- On se rend sur « **Command Prompt** » .
- Pour ping le « **PC Pierre** » tapez la commande suivante Ping « **IP du PC Alicia** ».
- Pour ping le « **PC Alicia** » tapez la commande suivante Ping « **IP du PC Pierre** ».



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F7FF:FE6E:3A38
    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:\>ping
Cisco Packet Tracer PC Ping

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

C:\>ping 192.168.1.2
Invalid Command.

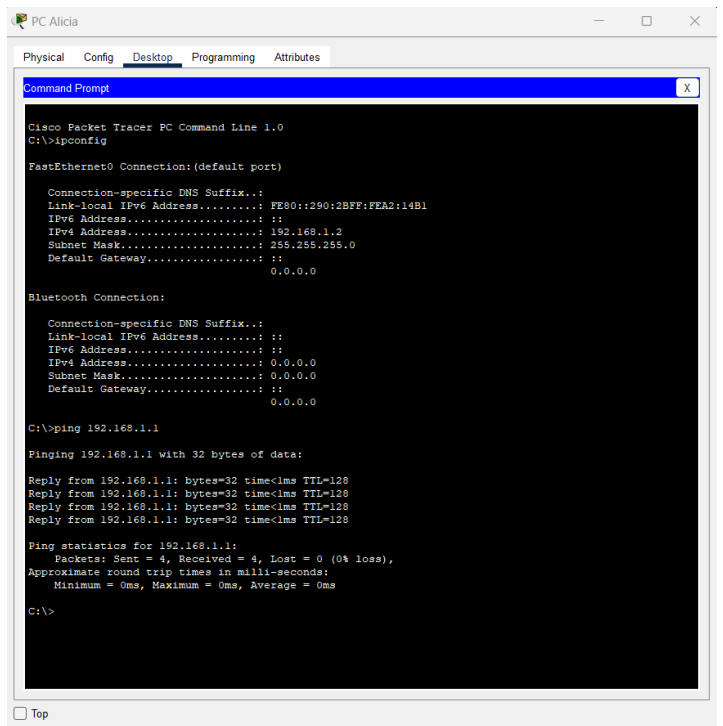
C:\>ping 192.168.1.2

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<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 = 0ms, Average = 0ms

C:\>
```



```
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::290:2BFF:FEA2:14B1
    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:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

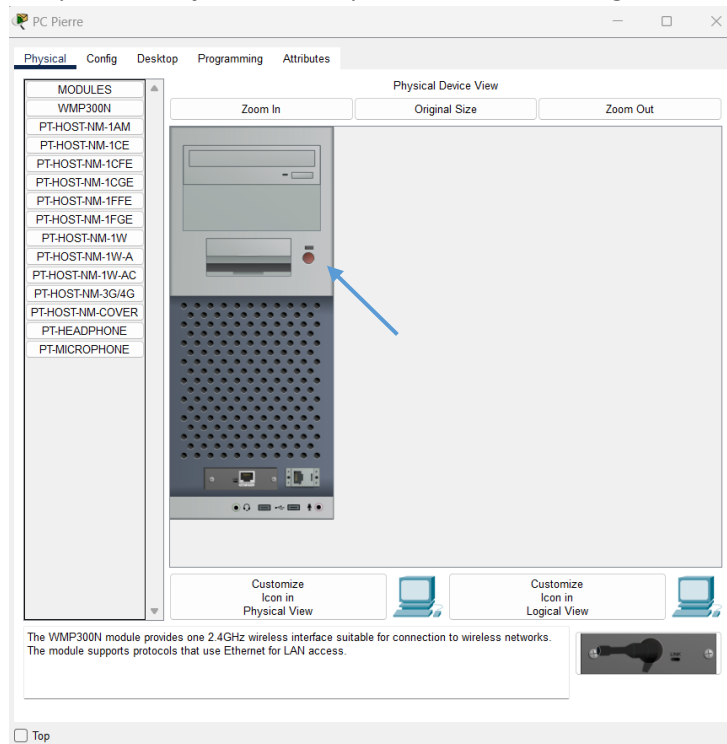
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

## Job7:

Pour éteindre le PC de Pierre il suffit simplement de se rendre sur son PC :

Dans la partie « **Physical** » et cliquez sur le bouton rouge.



On peut voir que lorsqu'un des deux PC est éteint on peut voir :



→ Non le PC de Pierre ne reçoit pas les ping du PC d'Alicia.

Explication :

Etant donnée que l'un des PC est éteint l'autre PC ne peut recevoir les ping .

```
C:\> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

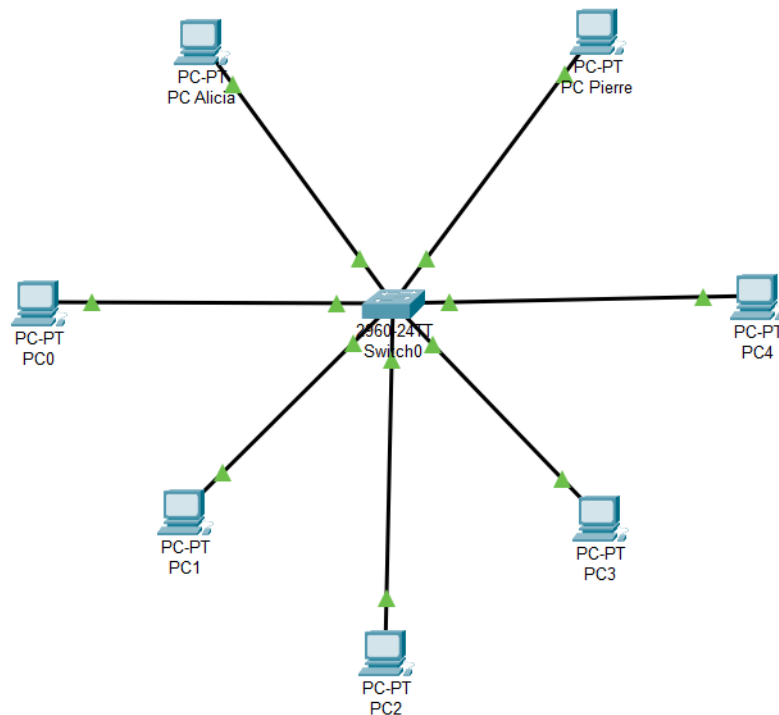
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

## Job8 :

Pour configurer nos cinq ordinateurs sur le même réseau il suffit d'ajouter un « **switch** » qui permettra de connecter nos appareils entre eux.



### La différence entre un hub et un switch ?

Un hub et un switch sont deux types de dispositifs utilisés dans les réseaux informatiques pour connecter plusieurs appareils ensemble. Cependant qu'ils fonctionnent différemment et ont des caractéristiques distinctes.

#### 1. Hub :

- Un hub est un dispositif de la couche physique du modèle OSI, ce qui signifie qu'il fonctionne au niveau le plus bas du modèle de référence OSI.
- Lorsqu'un hub reçoit des données d'un appareil connecté, il les diffuse à toutes les autres interfaces (ports) sans tenir compte de l'adresse de destination. Cela signifie que tous les appareils connectés au hub reçoivent les données, même s'ils ne sont pas destinataires.
- Les hubs sont souvent considérés comme des dispositifs "débiles" car ils ne sont pas capables de gérer efficacement le trafic, ce qui peut entraîner des collisions et une utilisation inefficace de la bande passante. Ils sont rarement utilisés dans les réseaux modernes.

## 2. Switch :

- Un switch fonctionne à un niveau plus élevé que le hub, généralement au niveau de la couche de liaison de données (couche 2 du modèle OSI).
- Contrairement au hub, un switch examine l'adresse MAC (adresse matérielle) de destination des données qu'il reçoit et les transmet uniquement à l'appareil spécifique auquel elles sont destinées. Cela permet de réduire le trafic inutile et les collisions, ce qui rend le réseau plus efficace.
- Les switches sont largement utilisés dans les réseaux modernes, car ils améliorent les performances en isolant le trafic et en permettant une communication plus efficace entre les appareils connectés.

### Fonctionnement d'un hub :

- Le hub reçoit des données d'un appareil connecté et les renvoie à tous les autres appareils connectés au réseau.
- Il fonctionne au niveau de la couche physique du modèle OSI, ce qui signifie qu'il ne comprend pas les adresses IP ni les données, mais se contente de relayer les informations brutes à tous les appareils.

### Avantages d'un hub :

1. **Simplicité** : Les hubs sont simples à configurer et à utiliser, car ils ne nécessitent pas de paramètres complexes.
2. **Coût** : Les hubs sont généralement peu coûteux par rapport à d'autres dispositifs de mise en réseau.
3. **Compatibilité** : Ils peuvent être utilisés avec une variété d'appareils, y compris les plus anciens.

### Inconvénients d'un hub :

1. **Collision de données** : Lorsque plusieurs appareils transmettent des données simultanément, des collisions peuvent se produire, entraînant des perturbations sur le réseau et une perte d'efficacité.
2. **Manque de sécurité** : Les données sont diffusées à tous les appareils connectés, ce qui signifie que toute personne sur le réseau peut potentiellement intercepter des informations sensibles.
3. **Limitations de vitesse** : Les hubs sont limités en termes de vitesse, car ils ne peuvent pas gérer efficacement les réseaux rapides ou gourmands en bande passante.



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

### Avantages d'un switch :

1. **Efficacité de la communication** : Les switches permettent une communication rapide et efficace entre les périphériques connectés, car ils envoient les données uniquement aux appareils destinataires, contrairement aux hubs qui diffusent les données à tous les appareils.
2. **Sécurité accrue** : Les switches isolent le trafic entre les périphériques, améliorant ainsi la sécurité en réduisant le risque d'interception de données par des appareils non autorisés.
3. **Bande passante dédiée** : Chaque port d'un switch dispose de sa propre bande passante, ce qui évite la congestion du réseau et garantit des performances constantes.

### Inconvénients d'un switch :

1. **Coût** : Les switches sont généralement plus chers que les hubs, ce qui peut être un inconvénient pour les petits réseaux ou les budgets limités.
2. **Complexité de configuration** : La configuration d'un switch peut être plus complexe, en particulier pour les réseaux plus importants. Il peut nécessiter des compétences techniques pour optimiser son fonctionnement.
3. **Risques de surcharge** : Si mal configuré, un switch peut être vulnérable à des attaques de saturation, où un grand nombre de données inutiles peuvent provoquer une surcharge du réseau.

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

Un switch gère le trafic réseau en utilisant des adresses MAC (Media Access Control) pour acheminer efficacement les données vers les appareils connectés. Voici une simplification du processus :

1. **Apprentissage des adresses MAC** :  
Lorsqu'un appareil est connecté au switch, ce dernier enregistre l'adresse MAC de cet appareil dans une table de correspondance (table MAC). Cette table indique à quel port du switch chaque adresse MAC est associée.
2. **Réception des trames** :  
Lorsqu'une trame de données (paquet d'informations) arrive sur un port du switch, le switch examine l'adresse MAC source de la trame.
3. **Consultation de la table MAC** :  
Le switch vérifie la table MAC pour trouver l'adresse MAC de destination dans la trame. Si elle est répertoriée, le switch sait sur quel port envoyer la trame.
4. **Transmission sélective** :  
Le switch transmet la trame uniquement sur le port associé à l'adresse MAC de destination, ce qui évite de surcharger le réseau en diffusant la trame à tous les ports. Cela améliore l'efficacité du réseau.
5. **Inconnu ou diffusion** :  
Si l'adresse MAC de destination n'est pas répertoriée dans la table MAC, le switch peut diffuser la trame à tous les ports (sauf le port source), ou il peut laisser tomber la trame s'il est configuré pour ignorer les adresses MAC inconnues.

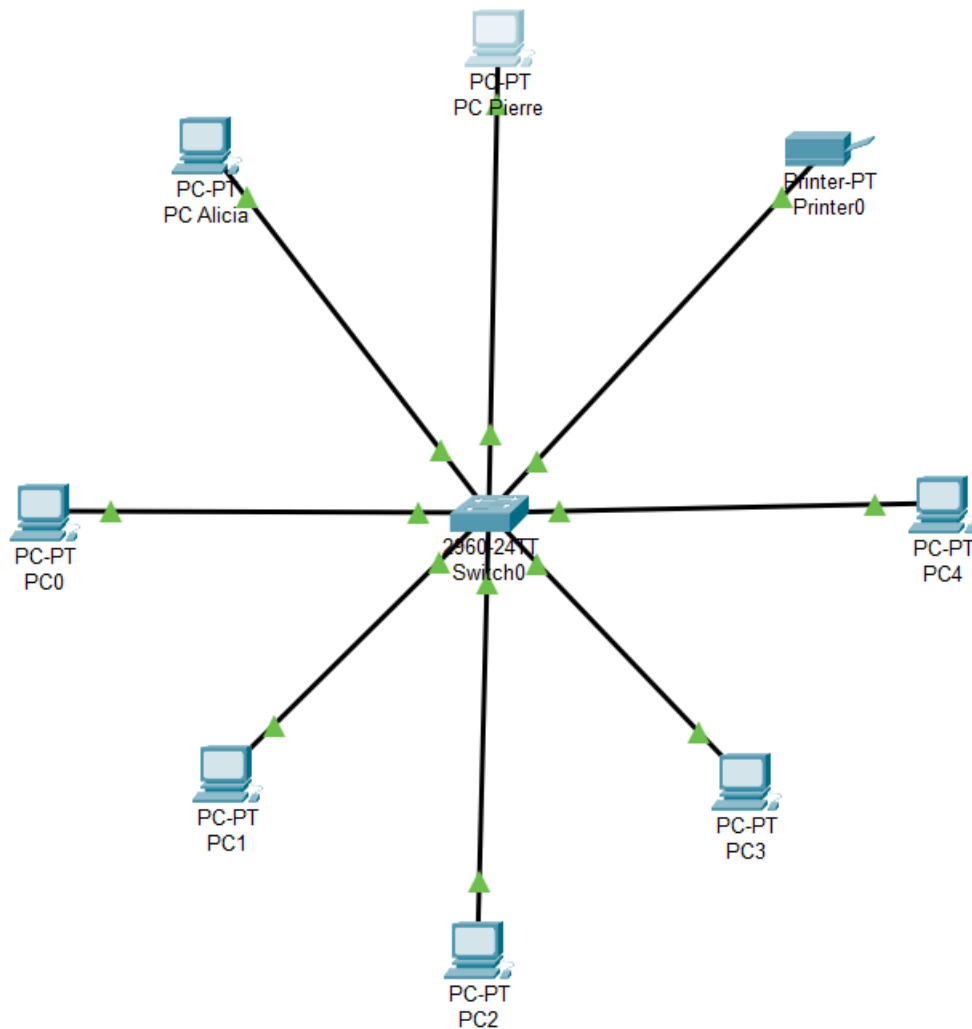
## Job9 :

On ajoute une imprimante à notre réseau :

- Dans la zone en bas à gauche on peut sélectionner l'imprimante.

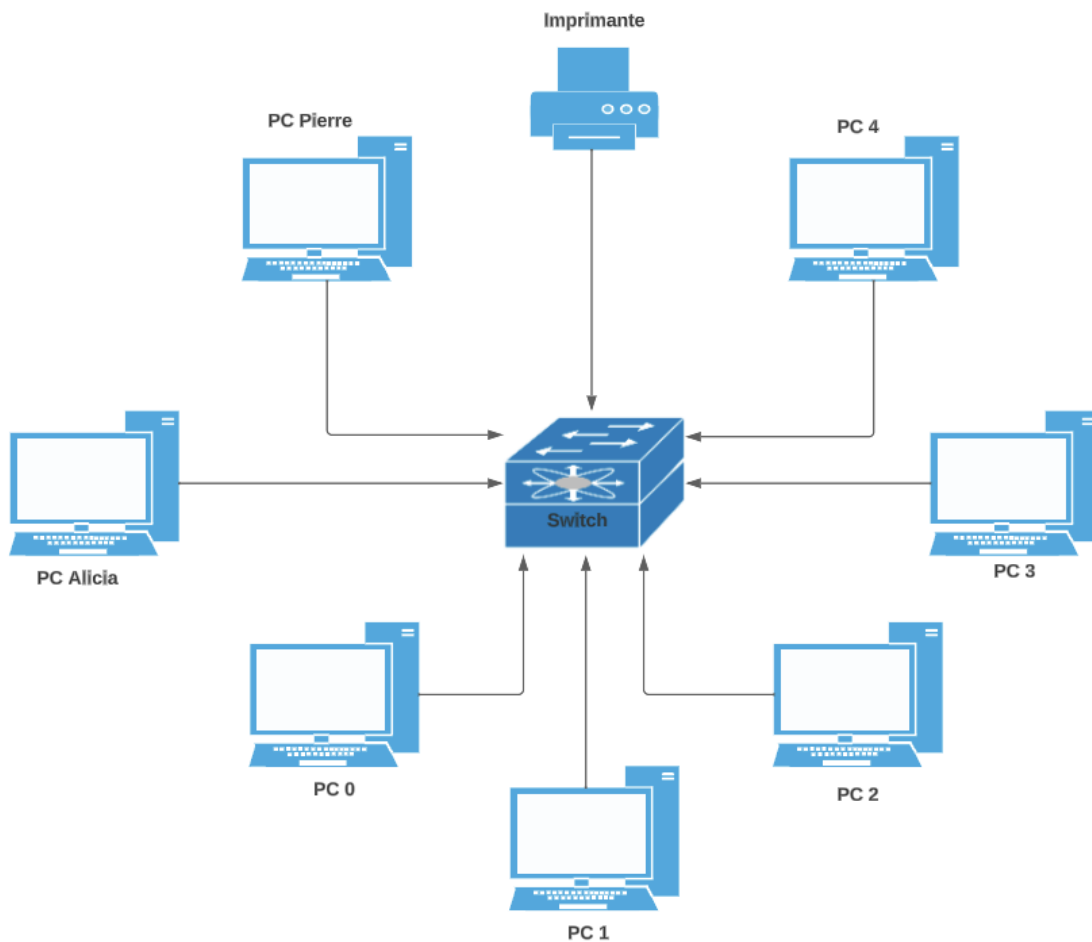


- Une fois ajouter il faut l'intégrer à notre réseau pour se faire on utilise à nouveau un câble.



Pour faire un schéma représentant notre réseau j'ai utilisé comme logiciel « **Lucidchart** ».

**Lucidchart** : permet la création de diagrammes et la visualisation de données, et autres schémas conceptuels.



#### Trois avantages importants d'avoir un schéma :

- Un schéma favorise la compréhension et la mémorisation.
- 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.
- Ils sollicitent tant l'esprit de synthèse (ils permettent d'avoir une vision globale et immédiate du sujet présenté).

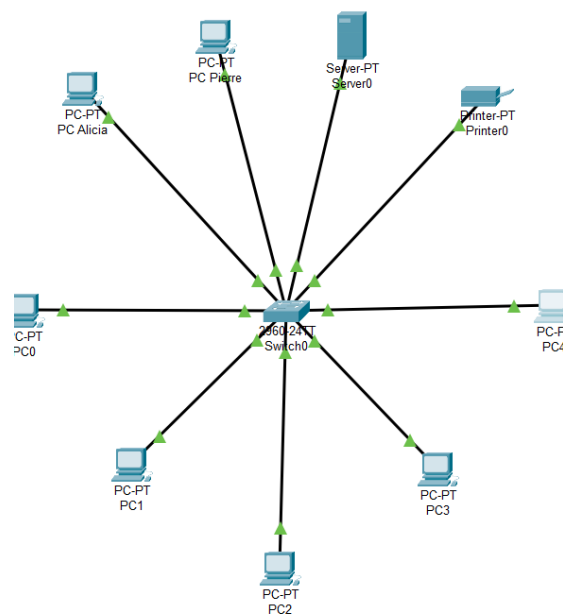
## Job10 :

Pour mettre en place un serveur DHCP qui permet la distribution automatique d'adresse IP il faut :

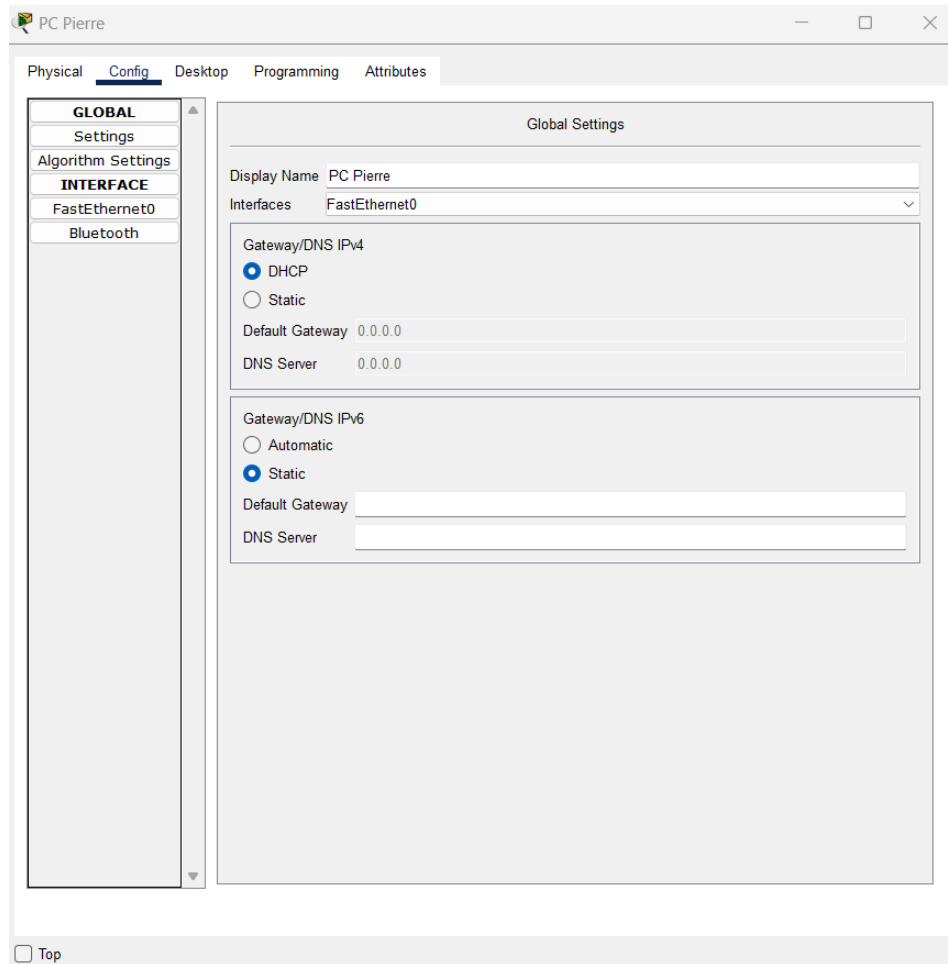
- Dans la zone en bas à gauche on peut sélectionné le serveur.



Une fois ajouter il faut l'intégrer à notre réseau pour se faire on utilise à nouveau un câble.



- Maintenant pour permettre la distribution automatique de l'adresse IP on doit configurer un à un les PC , en changeant bien « **Static** » en « **DHCP** » .



- Puis on va sur le serveur et on active le service en appuyant sur « on » puis pour sauvegarder on clique sur « save ».

The screenshot shows the 'Server0' configuration window with the 'Services' tab selected. On the left, a list of services includes HTTP, DHCP (highlighted), DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area is titled 'DHCP' and contains the following configuration fields:

- Interface: FastEthernet0
- Service: ☒ On ☐ Off
- Pool Name: serverPool
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0
- Start IP Address: 169.254.0.10
- Subnet Mask: 255.255.0.0
- Maximum Number of Users: 246
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below these fields are buttons for 'Add', 'Save', and 'Remove'. At the bottom, a table displays the configured DHCP pool:

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	169.254.0.10	255.255.0.0	246	0.0.0.0	0.0.0.0

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

Une adresse IP statique et une adresse IP attribuée par DHCP sont deux méthodes différentes pour attribuer des adresses IP à des dispositifs sur un réseau informatique. Voici les différences principales entre les deux :

#### 1. Adresse IP statique :

- Une adresse IP statique est configurée manuellement par un administrateur réseau. Cela signifie que l'administrateur doit spécifier une adresse IP spécifique pour chaque dispositif sur le réseau.
- L'adresse IP statique reste inchangée tant que l'administrateur ne la modifie pas explicitement.
- Les adresses IP statiques sont généralement utilisées pour des dispositifs tels que des serveurs, des routeurs, des imprimantes réseau, etc., dont l'adresse IP doit rester constante pour des raisons de stabilité et d'accessibilité.

## 2. Adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) :

- DHCP est un protocole de réseau qui attribue automatiquement des adresses IP aux dispositifs du réseau.
- Les adresses IP attribuées par DHCP sont temporaires et sont généralement empruntées à partir d'un pool d'adresses IP disponibles sur le réseau. Chaque dispositif recevra une adresse IP différente à chaque fois qu'il se connecte au réseau (à moins qu'une réservation DHCP ne soit configurée).
- DHCP est souvent utilisé pour les dispositifs clients tels que des ordinateurs, des téléphones, des tablettes, etc., car il simplifie grandement la gestion des adresses IP et évite les conflits d'adresses.

## Job11 :

Le plan d'adressage :

	Masque	Adresse Sous-réseau	Broadcast	Adresses disponibles	CIDR
1 sous réseau de 12 hôtes	255.255.255.240	10.1.0.0	10.1.0.15	10.1.0.1 – 10.1.0.14	/28
5 sous réseau de 30 hôtes	255.255.255.224	10.2.0.0	10.2.0.31	10.2.0.1 – 10.2.0.30	/27
	255.255.255.224	10.3.0.0	10.3.0.31	10.3.0.1 - 10.3.0.30	/27
	255.255.255.224	10.4.0.0	10.4.0.31	10.4.0.1 - 10.4.0.30	/27
	255.255.255.224	10.5.0.0	10.5.0.31	10.5.0.1 - 10.5.0.30	/27
	255.255.255.224	10.6.0.0	10.6.0.31	10.6.0.1 - 10.6.0.30	/27
5 sous réseau de 120 hôtes	255.255.255.128	10.7.0.0	10.7.0.127	10.7.0.1 - 10.7.0.126	/25
	255.255.255.128	10.8.0.0	10.8.0.127	10.8.0.1 - 10.8.0.126	/25
	255.255.255.128	10.9.0.0	10.9.0.127	10.9.0.1 - 10.9.0.126	/25
	255.255.255.128	10.10.0.0	10.10.0.127	10.10.0.1 - 10.10.0.126	/25
	255.255.255.128	10.11.0.0	10.11.0.127	10.11.0.1 - 10.11.0.126	/25
5 sous réseau de 160 hôtes	255.255.255.0	10.12.0.0	10.12.0.255	10.12.0.1 - 10.12.0.254	/24
	255.255.255.0	10.13.0.0	10.13.0.255	10.13.0.1 - 10.13.0.254	/24
	255.255.255.0	10.14.0.0	10.14.0.255	10.14.0.1 - 10.14.0.254	/24
	255.255.255.0	10.15.0.0	10.15.0.255	10.15.0.1 - 10.15.0.254	/24
	255.255.255.0	10.16.0.0	10.16.0.255	10.16.0.1 - 10.16.0.254	/24

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

Pour le choix d'une adresse de classe A c'est parce que ça permet d'accueillir un nombre d'utilisateurs conséquents.

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

Chacun de ces types d'adresses remplit une fonction spécifique dans son domaine d'application respectif

### 1. Adresse postale :

- Il s'agit de l'adresse physique à laquelle une lettre ou un colis est envoyé.
- Elle comprend généralement le nom du destinataire, le numéro de rue, le nom de la rue, la ville, l'État ou la province, le code postal et éventuellement le pays.
- Les adresses postales sont utilisées pour la livraison de courrier et de colis.

### 2. Adresse IP (Internet Protocol) :

- Une adresse IP est un identifiant numérique attribué à chaque appareil connecté à un réseau informatique, notamment Internet.
- Il existe deux versions principales d'adresses IP : IPv4 (32 bits) et IPv6 (128 bits) en raison de l'épuisement des adresses IPv4.
- Les adresses IP sont utilisées pour router le trafic sur Internet et localiser des dispositifs sur un réseau.

### 3. Adresse email :

- Une adresse email est un identifiant unique permettant d'envoyer et de recevoir des messages électroniques.
- Elle se compose généralement d'un nom d'utilisateur, du symbole "@" et du nom de domaine de l'organisme qui gère la messagerie électronique.
- Les adresses email sont utilisées pour la communication électronique.

### 4. Adresse URL (Uniform Resource Locator) :

- Une URL est une adresse utilisée pour accéder à des ressources en ligne, telles que des sites web, des fichiers, des images, etc.
- Une URL comprend le protocole (comme http ou https), le nom de domaine, le chemin d'accès, et éventuellement des paramètres.
- Les URL sont utilisées pour accéder à des ressources sur Internet.

### 5. Adresse MAC (Media Access Control) :

- Une adresse MAC est un identifiant unique attribué à chaque carte réseau d'un appareil, comme un ordinateur ou un routeur.
- Elle est utilisée au niveau de la couche matérielle du réseau pour acheminer les données entre les appareils.
- Les adresses MAC sont essentielles pour le fonctionnement des réseaux locaux (LAN).










6. Adresse physique (dans le contexte de la géolocalisation) :

- Il s'agit de l'emplacement géographique exact d'un lieu, souvent représenté par des coordonnées géographiques, telles que la latitude et la longitude.
- Les adresses physiques sont utilisées pour la géolocalisation, la navigation, et la cartographie.

## Job12 :

### Modèle OSI

7		C'est la couche la plus haute du modèle OSI, et elle permet aux applications de communiquer avec le réseau. Elle comprend les protocoles et les interfaces utilisateur.	FTP
6		Elle assure la traduction et la conversion des données entre les formats utilisés par les applications.	HTML
5		Cette couche établit, gère et termine les sessions de communication entre deux dispositifs.	SSL/TLS, PPTP
4		Elle s'occupe de la fiabilité de la communication de bout en bout en divisant les données en segments et en s'assurant qu'ils sont correctement reçus.	TCP, UDP

<b>3</b> 	<p>Cette couche est responsable du routage des données à travers un réseau, en prenant en charge l'adressage et la commutation.</p>	<p>IPv4,IPv6,Routeur</p>
<b>2</b> 	<p>Elle gère la communication entre deux nœuds directement connectés et assure la fiabilité de la transmission des données.</p>	<p>Ethernet,MAC,Wifi</p>
<b>1</b> 	<p>Cette couche traite de la transmission physique des données sur un support, comme les câbles, les signaux électriques ou les ondes lumineuses.</p>	<p>Câble RJ45,Fibre optique</p>

## Job13 :

### → Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est en étoile car tous les appareils du réseau sont connectés à un point central, généralement un commutateur ou un concentrateur. Cette topologie présente plusieurs avantages et est couramment utilisée pour de nombreuses applications.

### → Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est la première adresse IP utilisable dans la plage d'adresses IP. Dans ce cas, l'adresse IP du réseau est 192.168.10.0.

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

Le masque de sous-réseau 255.255.255.0 signifie que 8 bits sont réservés pour l'adresse IP (24 bits au total) et 8 bits pour les hôtes. Avec 8 bits pour les hôtes, vous avez  $2^8 - 2$  adresses IP disponibles. Les 2 soustractions sont dues à l'adresse de réseau (192.168.10.0) et à l'adresse de diffusion (192.168.10.255). Donc, il y a  $256 - 2 = 254$  adresses IP disponibles pour les machines sur ce réseau.

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

L'adresse de diffusion d'un réseau est toujours une adresse IP où tous les bits de l'adresse d'hôte sont à 1 dans le masque de sous-réseau. Dans ce cas, le masque de sous-réseau est 255.255.255.0, ce qui signifie que les 8 derniers bits sont réservés pour les hôtes. Par conséquent, l'adresse de diffusion est 192.168.10.255.

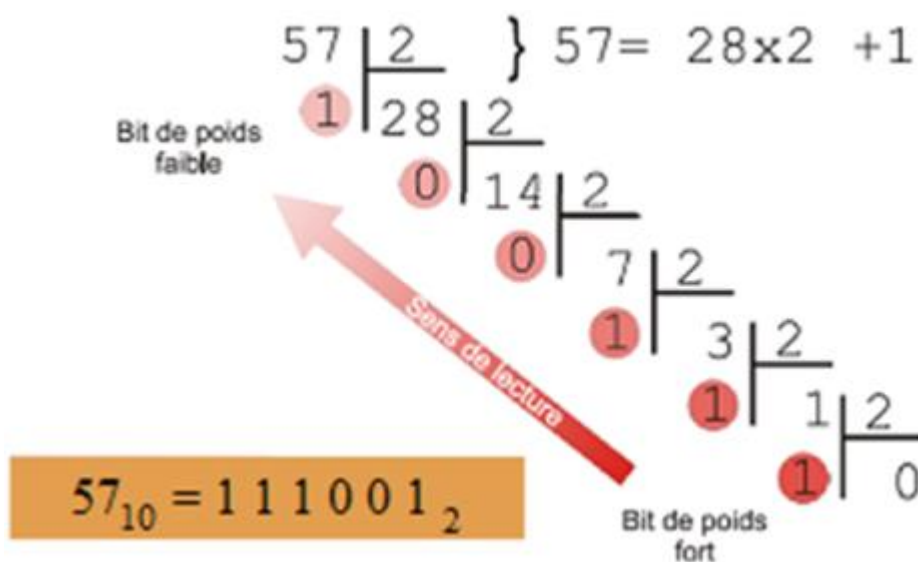
## Job14 :

### Convertir les adresses IP en binaires :

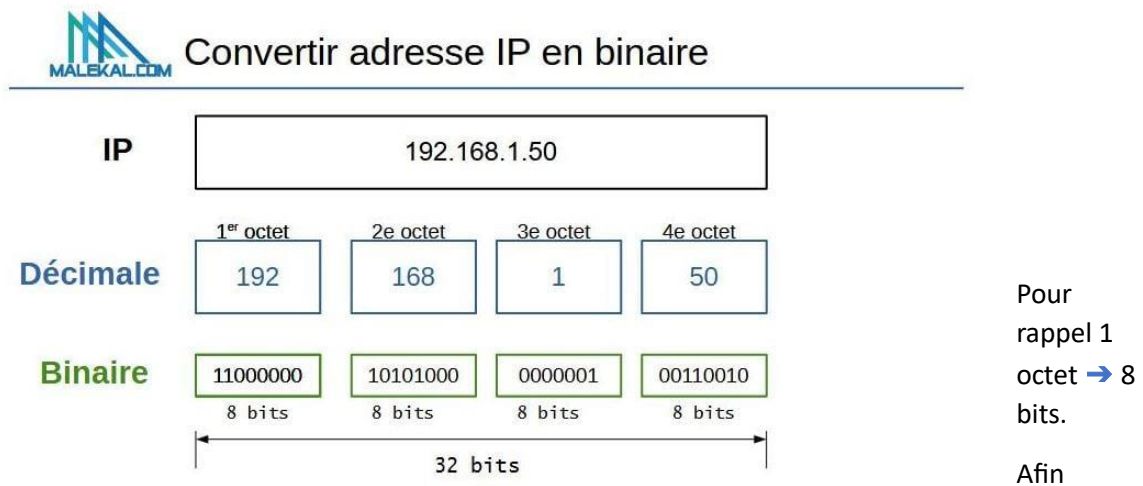
Pour convertir un nombre décimale en binaire :

Prenons par exemple le nombre décimal  $N = 57_{(10)}$  pour savoir à quoi il correspond au nombre binaire :

On peut appliquer une petite astuce :



-Il faut comprendre que chaque chiffre de l'adresse IP se décompose dans un bloc binaire de 8 bits.



d'effectuer la conversion il faut garder en tête ceci :

8e bit	7e bit	6e bit	5e bit	4e bit	3e bit	2e bit	1e bit
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1

« La valeur de chaque bit dans un octet »

En utilisant cette logique on peut calculer la représentation décimale d'un nombre binaire.

Comme 11100011 par exemple.

8e bit (128)	7e bit (64)	6e bit (32)	5e bit (16)	4e bit (8)	3e bit (4)	2e bit (2)	1e bit (1)
1	1	1	0	0	1	1	1

Ducoup  $(11100011)_2 = (128+64+32+4+2+1)=(231)_{10}$

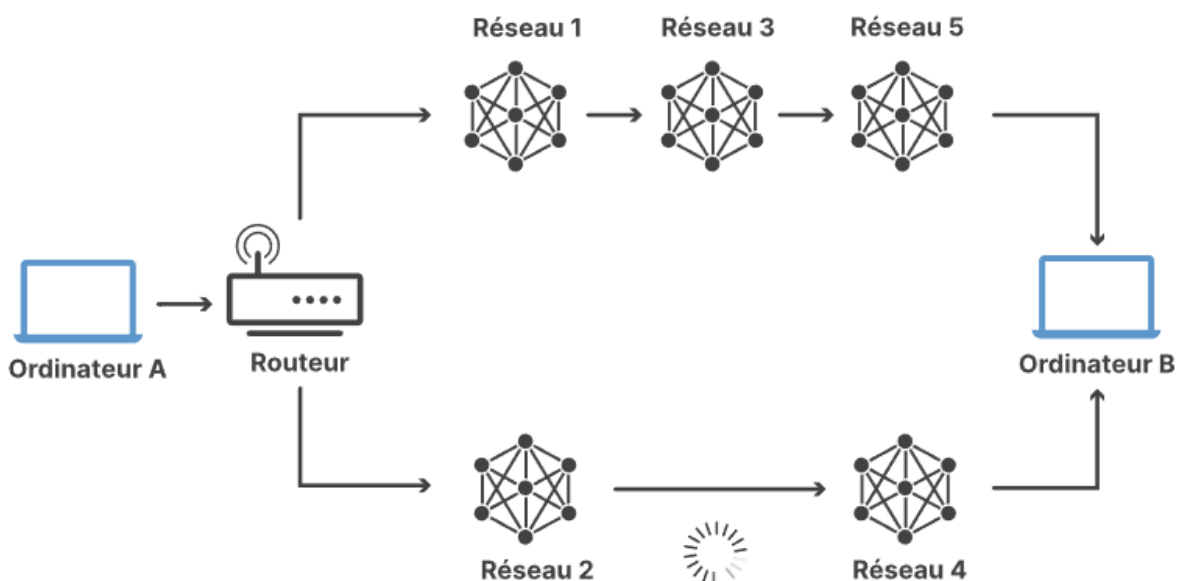
En appliquant ceci sur nos adresses IP on trouve :

- **145.32.59.24** = 10010001.00100000.00111011.00011000
- **200.42.129.16** = 11001000.00101010.10000001.0001000
- **14.82.19.54** = 00001110.01010010.00010011.00110110

## Job15 :

→ Qu'est-ce que le routage ?

Le routage réseau 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. Ces décisions de routage Internet sont prises par des périphériques réseau spécialisés appelés **routeurs**. Examinons l'image ci-dessous. Pour qu'un paquet de données puisse se rendre de l'ordinateur A à l'ordinateur B, doit-il passer par les réseaux 1, 3 et 5 ou les réseaux 2 et 4 ? Le paquet empruntera un chemin plus court via les réseaux 2 et 4, mais les réseaux 1, 3 et 5 pourraient s'avérer plus rapides pour acheminer les paquets. C'est là le genre de choix que les routeurs réseau effectuent en permanence.



## Comment fonctionne le routage ?

Les routeurs s'appuient sur des tables de routage internes pour prendre des décisions concernant l'acheminement des paquets le long des chemins réseau. Une table de routage enregistre les chemins que les paquets doivent emprunter pour atteindre chaque destination dont le routeur est responsable. L'ensemble fonctionne un peu sur le même principe que les horaires ferroviaires que les passagers consultent pour décider quel train prendre. Les tables de routage sont similaires, mais s'attachent aux chemins réseau plutôt qu'aux trains.

Les routeurs fonctionnent de la manière suivante : lorsqu'un routeur reçoit un paquet, il lit les en-têtes\* du paquet pour voir la destination prévue, à l'instar d'un contrôleur qui consulte le billet d'un passager sur un quai pour lui indiquer quel train prendre. Il détermine ensuite où acheminer le paquet en fonction des informations contenues dans ses tables de routage. Les routeurs effectuent ces opérations des millions de fois par seconde, avec des millions de paquets. Lorsqu'un paquet se rend vers sa destination, il peut être acheminé plusieurs fois par différents routeurs.

Les tables de routage peuvent être statiques ou dynamiques.

- Les statiques ne changent pas et sont établies manuellement par un administrateur réseau. Dans les grandes lignes, elles fixent les itinéraires que les paquets de données empruntent sur le réseau, à moins que l'administrateur ne mette à jour les tables de manière manuelle.

- Les tables de routage dynamiques se mettent à jour automatiquement. Les routeurs dynamiques s'appuient sur divers protocoles de routage (voir ci-dessous) pour déterminer les chemins les plus courts et les plus rapides. Ils déterminent également le temps nécessaire aux paquets pour atteindre leur destination (un peu comme Google Maps, Waze et les autres services GPS) afin de déterminer les meilleurs itinéraires en fonction de vos habitudes de trafic et des conditions de circulation actuelles.

Le routage dynamique nécessite une plus grande puissance de calcul, c'est pourquoi les petits réseaux s'appuient plutôt sur le routage statique. En revanche, le routage dynamique se révèle beaucoup plus efficace pour les réseaux de tailles moyenne et grande.

### Qu'est-ce qu'un routeur ?

Un routeur est un équipement réseau physique responsable de l'acheminement des paquets vers leur destination. Les routeurs se connectent à deux ou plusieurs réseaux ou sous-réseaux IP et se transmettent des paquets de données entre eux selon les besoins. Ils sont utilisés pour les particuliers et les bureaux pour établir les connexions au réseau local. Des routeurs plus puissants sont présents partout sur Internet, afin d'aider les paquets de données à atteindre leur destination.

### → Qu'est-ce qu'un gateway ?

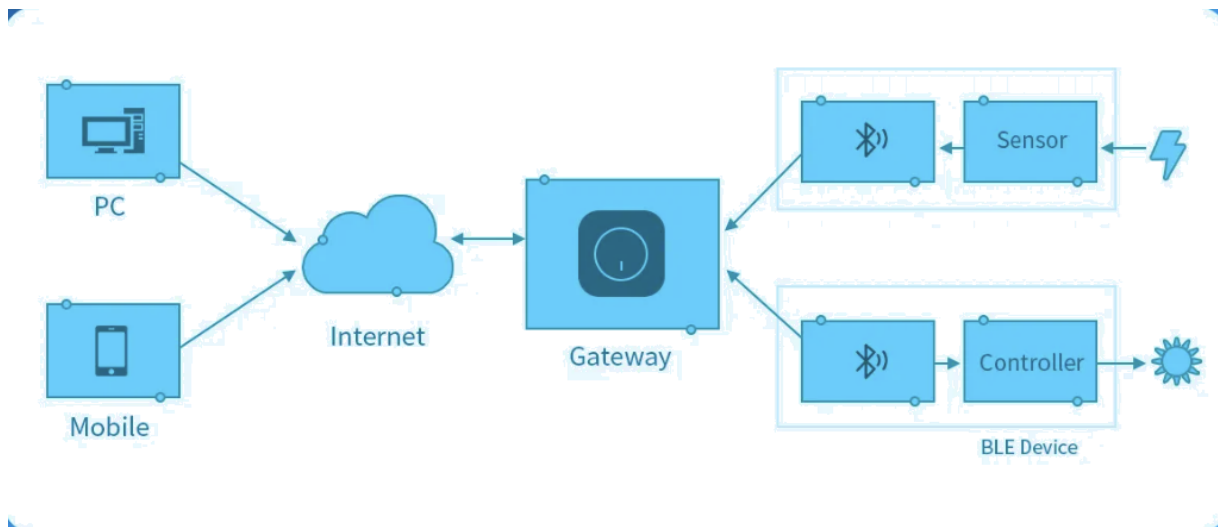
Le terme Gateway est traduit en français par « passerelle » ou « passerelle applicative »

Une Gateway 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. La Gateway la plus connue est ainsi la box Internet.

## Comment fonctionne une gateway ?

Lorsque l'utilisateur d'un réseau souhaite accéder à un réseau utilisant un protocole différent, la Gateway examine la légitimité de sa demande. Si celle-ci respecte les conditions fixées par l'administrateur du réseau visé, alors la Gateway établit une liaison entre les deux réseaux. La passerelle joue ainsi un rôle de pare-feu et participe à la sécurisation des échanges via des protocoles réseau différents.

Sur le plan technique, il existe diverses formes de passerelles : un répéteur est considéré comme une passerelle de niveau 1, un pont comme une passerelle de niveau 2 et un routeur comme une passerelle de niveau 3.





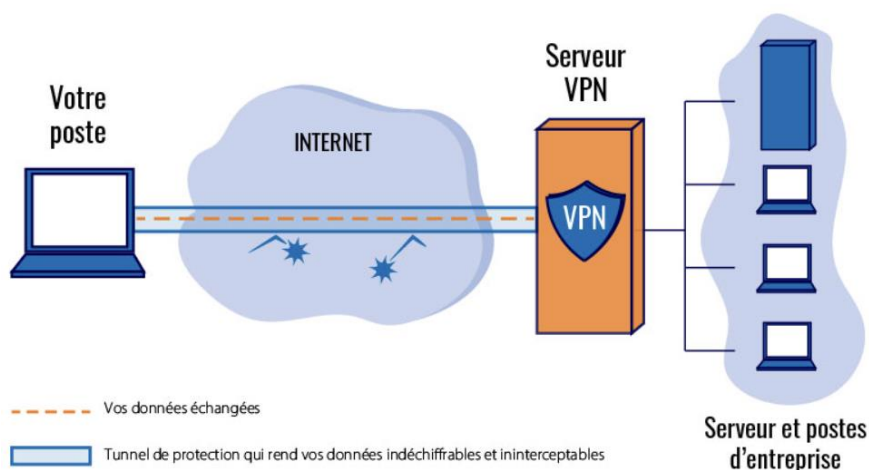
### → Qu'est-ce qu'un VPN ?

VPN signifie Virtual « **Private Network** » en français « **Réseau Privé Virtuel** » .

Le VPN est un logiciel qui s'installe sur plusieurs appareils reliés à Internet. Une fois le VPN activé, un tunnel sécurisé se crée entre vous et le réseau Internet. De cette manière, les informations qui y transitent seront chiffrées. Aussi, précisons que l'activation s'effectue en se connectant à un serveur VPN distant. Ainsi, vous obtiendrez une nouvelle adresse IP d'emprunt et la vôtre sera masquée.

#### Comment un VPN fonctionne-t-il ?

Un VPN masque votre adresse IP en laissant le réseau la rediriger vers un serveur distant spécialement configuré et géré par l'hôte d'un VPN. Cela signifie que si vous surfez en ligne au moyen d'un VPN, le serveur VPN devient la source de vos données. Cela signifie que votre fournisseur d'accès Internet (FAI) et d'autres tiers ne peuvent pas connaître les sites Web que vous visitez ni les données que vous envoyez et recevez en ligne. Un VPN fonctionne comme un filtre qui transforme toutes vos données en « charabia ». Même si quelqu'un venait à mettre la main sur vos données, elles seraient inexploitable.



### → Qu'est-ce qu'un DNS ?

DNS signifiant « **système de noms de domaine** » inventé pour faciliter la recherche d'un site donnée sur Internet , il permet d'associer un nom compréhensible à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique l'adresse IP.

Le nom de domaine et l'adresse IP sont uniques. Le **DNS** permet à votre message d'atteindre son destinataire et non quelqu'un d'autre possédant un nom de domaine similaire