

# Runtrack Réseau

## Job 1

### 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](#)

## Téléchargement de cisco

## Job 2

### → Qu'est qu'un réseau ?

Un réseau informatique est une infrastructure composée d'un ensemble d'appareils interconnectés permettant le partage de ressources, d'informations et de services entre des ordinateurs, des périphériques et des utilisateurs. Ces appareils peuvent être des ordinateurs, des serveurs, des routeurs, des commutateurs, des points d'accès Wi-Fi, des périphériques de stockage...

## → À quoi sert un réseau informatique ?

L'objectif principal d'un réseau informatique est de faciliter la communication et le partage de données entre les différents composants du réseau. Les réseaux informatiques peuvent être locaux (LAN), étendus (WAN), métropolitains (MAN) ou globaux (Internet). Voici quelques composants clés d'un réseau informatique :

- ❖ **Nœuds (ou hôtes)** : Ce sont les appareils connectés au réseau, tels que les ordinateurs, les serveurs, les imprimantes, les téléphones, etc.
- ❖ **Connexions** : Ce sont les liens physiques ou logiques qui permettent la communication entre les nœuds, tels que les câbles, les fibres optiques, les ondes radio, etc.
- ❖ **Équipements réseau** :
  - **Routeurs** : Ils dirigent le trafic entre différents réseaux.
  - **Commutateurs** : Ils dirigent le trafic au sein d'un réseau local en fonction des adresses matérielles (MAC).
  - **Points d'accès Wi-Fi** : Ils permettent aux appareils sans fil de se connecter au réseau.
  - **Firewalls** : Ils sécurisent le réseau en contrôlant le trafic entrant et sortant.
- ❖ **Protocoles réseau** : Ce sont des règles et des conventions qui régissent la communication entre les nœuds du réseau. Des exemples incluent TCP/IP, UDP, HTTP, FTP, etc.



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

Pour construire un réseau informatique, plusieurs composants matériels sont nécessaires. Chacun de ces composants remplit des fonctions spécifiques pour permettre le bon fonctionnement et la connectivité du réseau. Voici les principaux composants matériels et leurs fonctions :

### ❖ Serveurs :

- **Fonction** : Stockage centralisé, traitement de données, partage de ressources.
- **Description** : Les serveurs sont des ordinateurs puissants qui stockent et gèrent des données, des applications et des services pour les utilisateurs du réseau. Ils peuvent être des serveurs de fichiers, des serveurs d'applications, des serveurs de messagerie, etc.

### ❖ Ordinateurs (nœuds) :

- **Fonction** : Utilisation des services du réseau, accès aux ressources partagées.
- **Description** : Les ordinateurs, également appelés nœuds, sont les appareils finaux du réseau tels que les ordinateurs de bureau, les ordinateurs portables, les tablettes et les smartphones. Ils utilisent le réseau pour accéder aux services et aux ressources partagées.

#### ❖ Switches (commutateurs) :

- **Fonction** : Acheminement efficace des données entre les appareils du réseau.
- **Description** : Les commutateurs sont des dispositifs qui dirigent le trafic réseau en fonction des adresses MAC (Media Access Control). Ils permettent une communication directe entre les appareils connectés sur le réseau local (LAN).

#### ❖ Routeurs :

- **Fonction** : Acheminement des données entre différents réseaux.
- **Description** : Les routeurs sont des appareils qui connectent différents réseaux, dirigeant le trafic en fonction des adresses IP. Ils facilitent la communication entre les appareils situés dans des réseaux distincts.

#### ❖ Câbles et connecteurs :

- **Fonction** : Transmission des données entre les appareils du réseau.
- **Description** : Les câbles (comme les câbles Ethernet) et les connecteurs (comme les prises RJ45) sont utilisés pour établir des connexions physiques entre les appareils du réseau, permettant ainsi le transfert de données.



#### ❖ Points d'accès Wi-Fi :

- **Fonction** : Fourniture d'accès réseau sans fil.
- **Description** : Les points d'accès Wi-Fi permettent aux appareils sans fil de se connecter au réseau, offrant ainsi une connectivité réseau sans fil dans une zone donnée.

#### ❖ Firewalls (pare-feux) :

- **Fonction** : Sécurisation du réseau en contrôlant le trafic entrant et sortant.
- **Description** : Les pare-feux sont des dispositifs qui filtrent le trafic réseau pour protéger le réseau contre les menaces potentielles en autorisant ou en bloquant certains types de trafic en fonction de règles prédéfinies.

#### ❖ Modems :

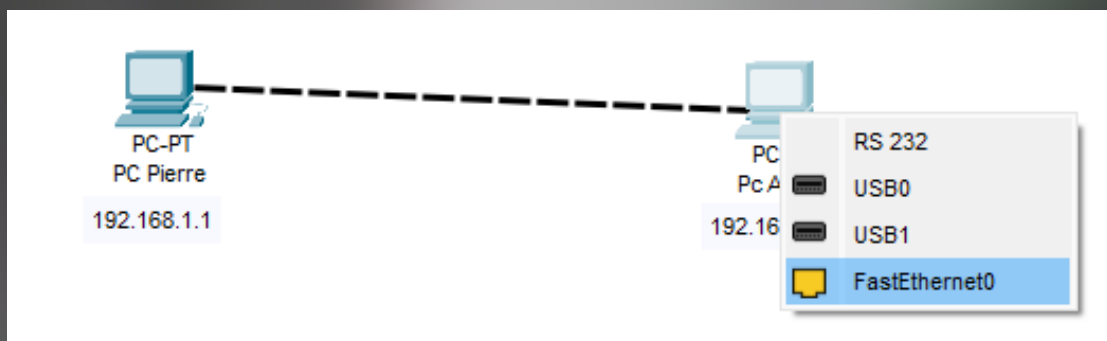
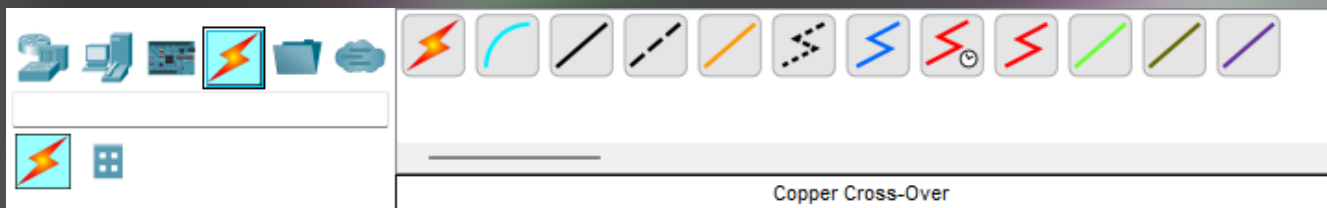
- **Fonction** : Établissement de la connexion au fournisseur de services Internet (FSI).
- **Description** : Les modems traduisent les signaux numériques en signaux analogiques pour établir une connexion au FSI via des technologies telles que DSL, câble ou fibre optique.

Ces composants matériels sont essentiels pour établir et maintenir un réseau informatique fonctionnel, permettant ainsi la communication, le partage de ressources et l'accès à l'information au sein d'une organisation ou d'un groupe d'utilisateurs.

## Job 3

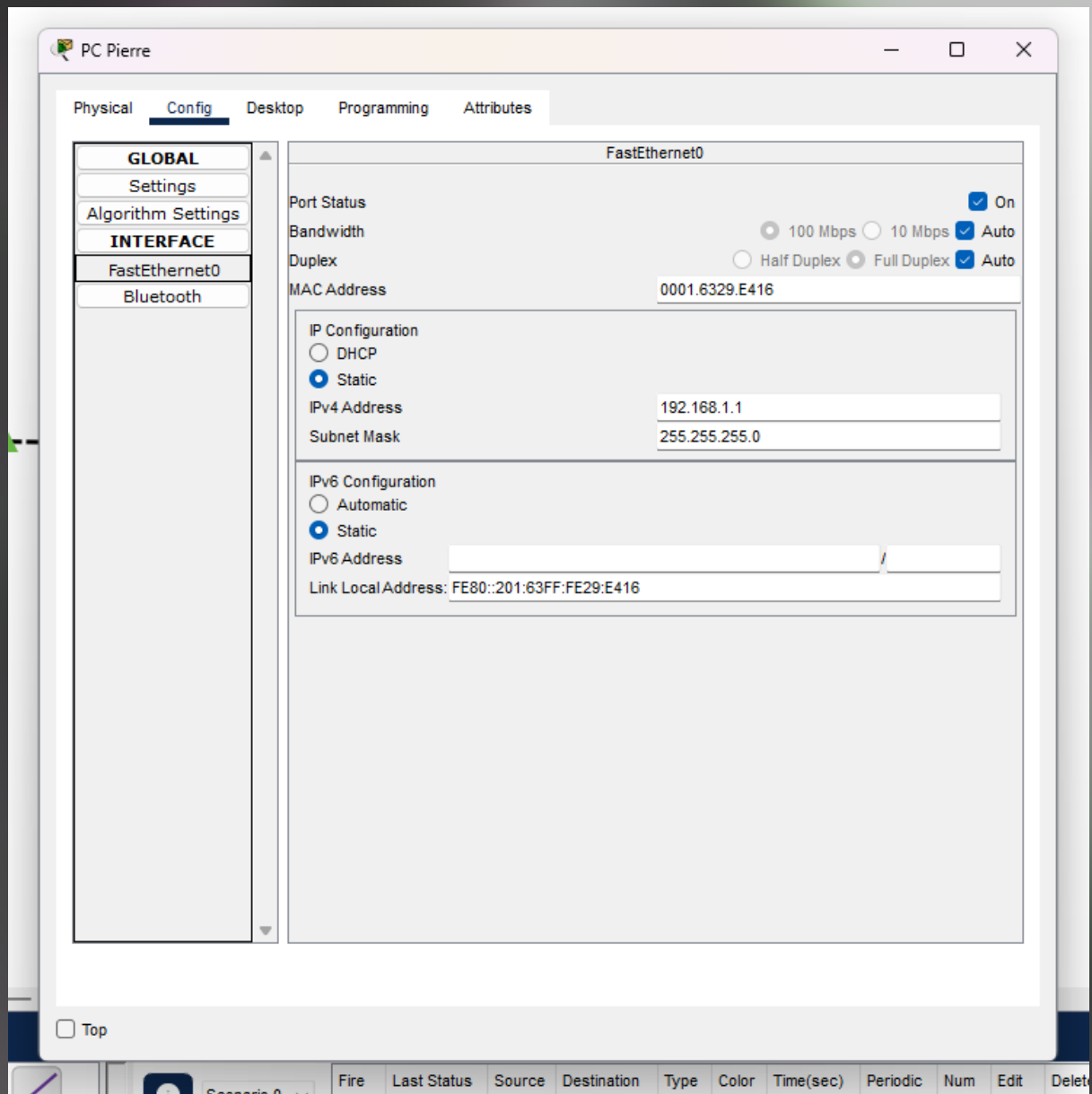
→ Quels câbles avez-vous choisis pour relier les deux ordinateurs ?

J'ai choisie le câble Cross-Over car le câble crossover (ou câble croisé en français) est un choix approprié pour relier deux ordinateurs directement sans passer par un routeur ou un commutateur intermédiaire. Ce type de câble est spécialement conçu pour permettre la communication entre deux appareils similaires, tels que deux ordinateurs, en inversant les broches du câble.



**Liaison du PC Pierre au PC Alicia via un cable crossover  
connecter sur chacun des ports fast Ethernet**

## Job 4



### → Qu'est-ce qu'une adresse IP ?

Une adresse IP, abréviation d'"adresse de protocole Internet" en anglais, est un identifiant numérique unique attribué à chaque appareil connecté à un réseau informatique qui utilise Internet Protocol (IP) pour la communication. Cette adresse permet d'identifier et de localiser de manière unique chaque appareil sur un réseau, qu'il s'agisse d'un ordinateur, d'un smartphone, d'une tablette, d'un serveur, ou tout autre appareil connecté à Internet.



L'adresse IP est généralement représentée sous forme de série de chiffres séparés par des points, par exemple : 192.168.121.41. Il existe deux principales versions d'adresses IP en usage :

➤ **IPv4 (Internet Protocol version 4) :**

Utilise une série de quatre nombres décimaux séparés par des points, par exemple, 192.168.142.125. Chaque nombre peut varier de 0 à 255.

➤ **IPv6 (Internet Protocol version 6) :**

Utilise une notation hexadécimale constituée de huit groupes de quatre chiffres, séparés par des deux-points, par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 a été introduit pour répondre à l'épuisement des adresses IPv4 et permettant ainsi de générer un nombre beaucoup plus grand d'adresses uniques pour faire face à la croissance exponentielle d'appareils connectés à Internet.

Lorsque vous envoyez des données sur Internet (comme visiter un site web, envoyer un e-mail, etc.), votre appareil utilise son adresse IP pour être identifié et pour que les données soient correctement acheminées vers la destination désirée.

→ **À quoi sert un IP ?**

Lorsque vous envoyez des données sur Internet (comme visiter un site web, envoyer un e-mail, etc.), votre appareil utilise son adresse IP pour être identifié. Pour chaque appareil connecté à Internet est attribuée une adresse IP pour faciliter l'acheminement efficace des données vers et depuis cet appareil dans le réseau mondial.



## → Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est un identifiant unique attribué à chaque carte réseau d'un appareil connecté à un réseau informatique. Contrairement à l'adresse IP, qui est liée à la couche réseau et peut être modifiée, l'adresse MAC est spécifique au matériel et est associée à la carte réseau elle-même.

L'adresse MAC est généralement attribuée par le fabricant de la carte réseau et est utilisée pour identifier de manière unique chaque carte réseau dans le monde. Elle est composée de 12 caractères alphanumériques, généralement séparés par des deux-points ou des tirets, par exemple, "00:1A:2B:3C:4D:5E".

Contrairement aux adresses IP, les adresses MAC ne sont pas rentables à travers Internet. Elles sont utilisées pour la communication au sein d'un réseau local. L'adresse MAC est souvent appelée "adresse physique" car elle est gravée dans le matériel de la carte réseau et est unique pour chaque carte.

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

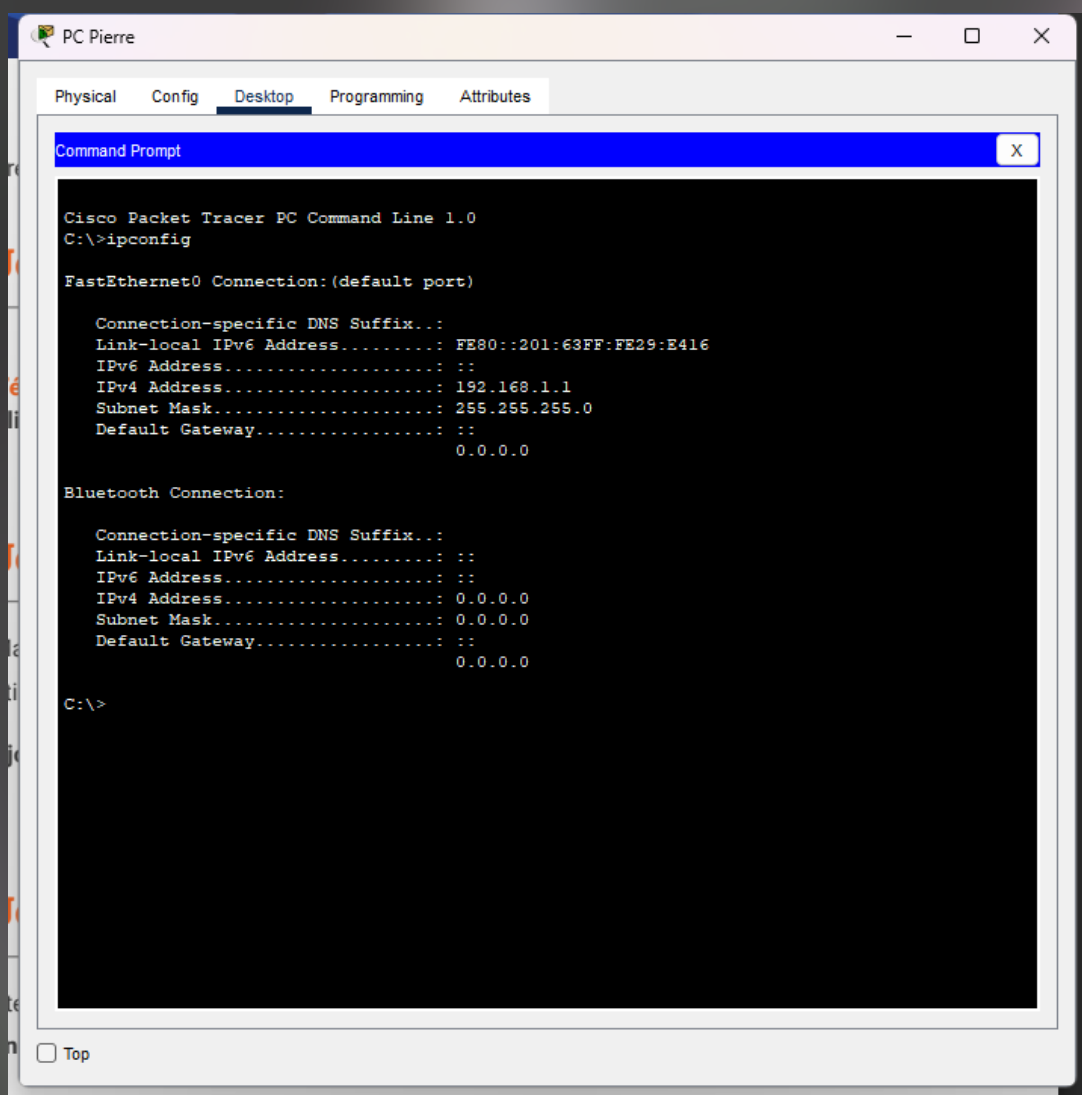
La différence entre une IP publique et privée est en fonction de son accessibilité et de l'emplacement du réseau auquel elle est associée voici les caractéristiques de chacune d'elles :

- **Adresse IP publique** : Une adresse IP publique est accessible depuis Internet. Elle peut être atteinte depuis n'importe quel autre point sur Internet, ce qui signifie que les serveurs, les ordinateurs et les appareils qui utilisent des adresses IP publiques peuvent être contactés directement depuis le réseau mondial. Les adresses IP publiques sont généralement routables sur Internet. Elles sont attribuées par des autorités centrales et doivent être uniques pour garantir la connectivité et l'identification uniques à l'échelle mondiale.
- **Adresse IP privée** : Une adresse IP privée est utilisée à l'intérieur d'un réseau privé, tel qu'un réseau domestique ou un réseau d'entreprise. Ces adresses ne sont pas routables sur Internet et sont conçues pour être utilisées localement au sein du réseau privé. Elles ne peuvent pas être atteintes directement depuis Internet. Les adresses IP privées permettent de conserver des adresses IP publiques, car de nombreux appareils peuvent partager une seule adresse IP publique à travers un routeur utilisant la technique de translation d'adresse réseau (NAT - Network Address Translation).

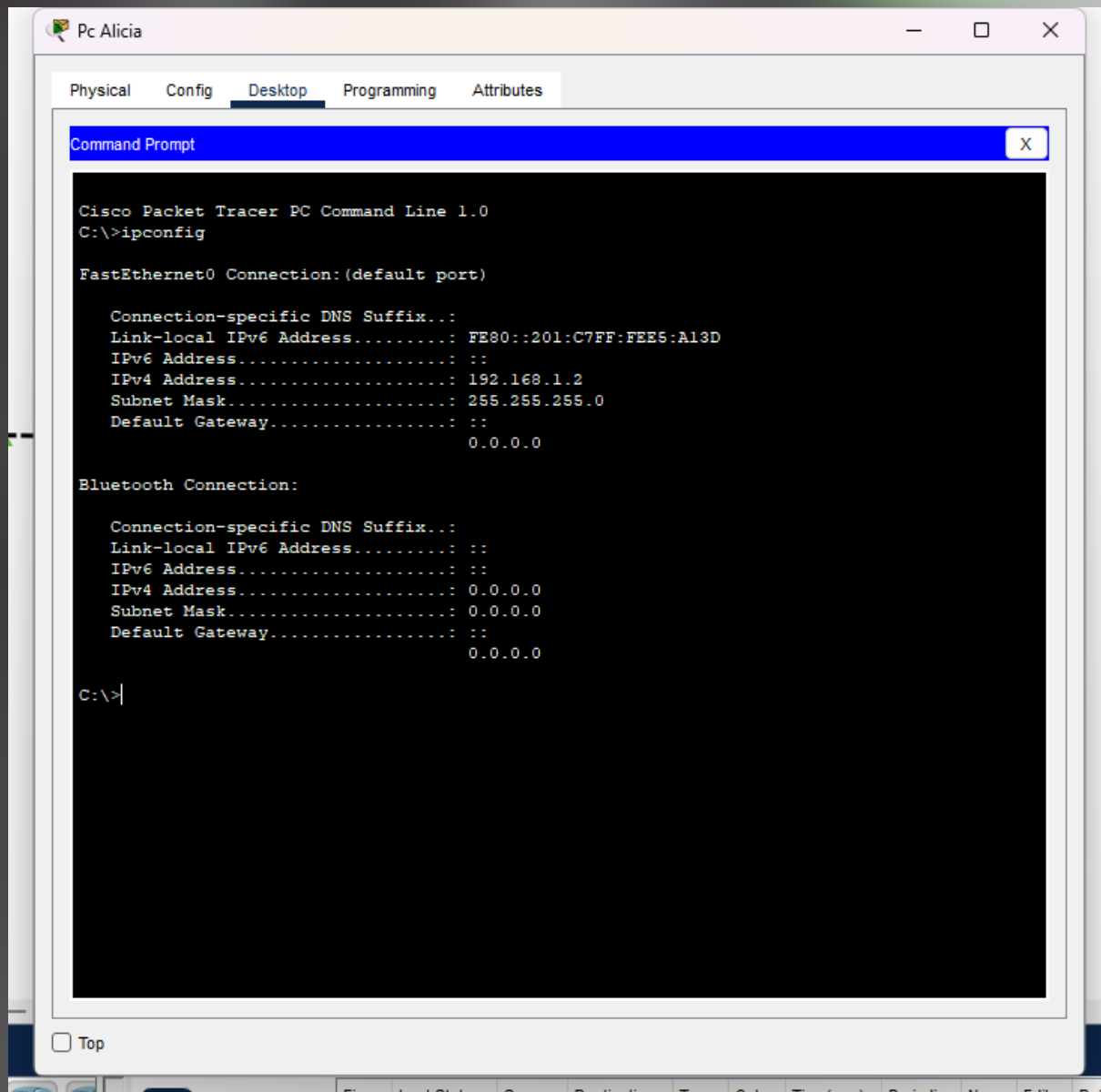
## → Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau sera 192.168.1.0 le zéro étant pour désigner le réseau lui-même et l'adresse suivante étant 192.168.1.1 sera attribuée aux machines.

## Job 5







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

On utilise la commande ipconfig afin de connaître l'adresse ip de chaque machine.

## Job 6

```
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=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms 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 = 2ms, Maximum = 2ms, Average = 2ms

C:\>|
```

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

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

C:\>
```

### Requêtes ping entre le pc de Pierre et Alicia

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

La commande permettant de ping entre les machines est le ping; on envoie des paquets à une autre machine et celle-ci va nous les renvoyer testant ainsi la disponibilité de la machine et la connexion entre les deux machines.



## Job 7

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Ping statistics for 192.168.1.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>
```

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

Si le PC de Pierre est éteint, il ne peut pas recevoir de paquets, y compris ceux envoyés par le PC d'Alicia. Lorsque le PC de Pierre est éteint, ses interfaces réseau, y compris l'interface à laquelle le PC d'Alicia envoie les paquets, sont inactives. Par conséquent, les paquets envoyés par le PC d'Alicia ne peuvent pas être reçus ou traités par le PC de Pierre car ses interfaces réseau sont désactivées lorsqu'il est hors tension.

## Job 8

```
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=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms 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 = 4ms, Maximum = 8ms, Average = 5ms

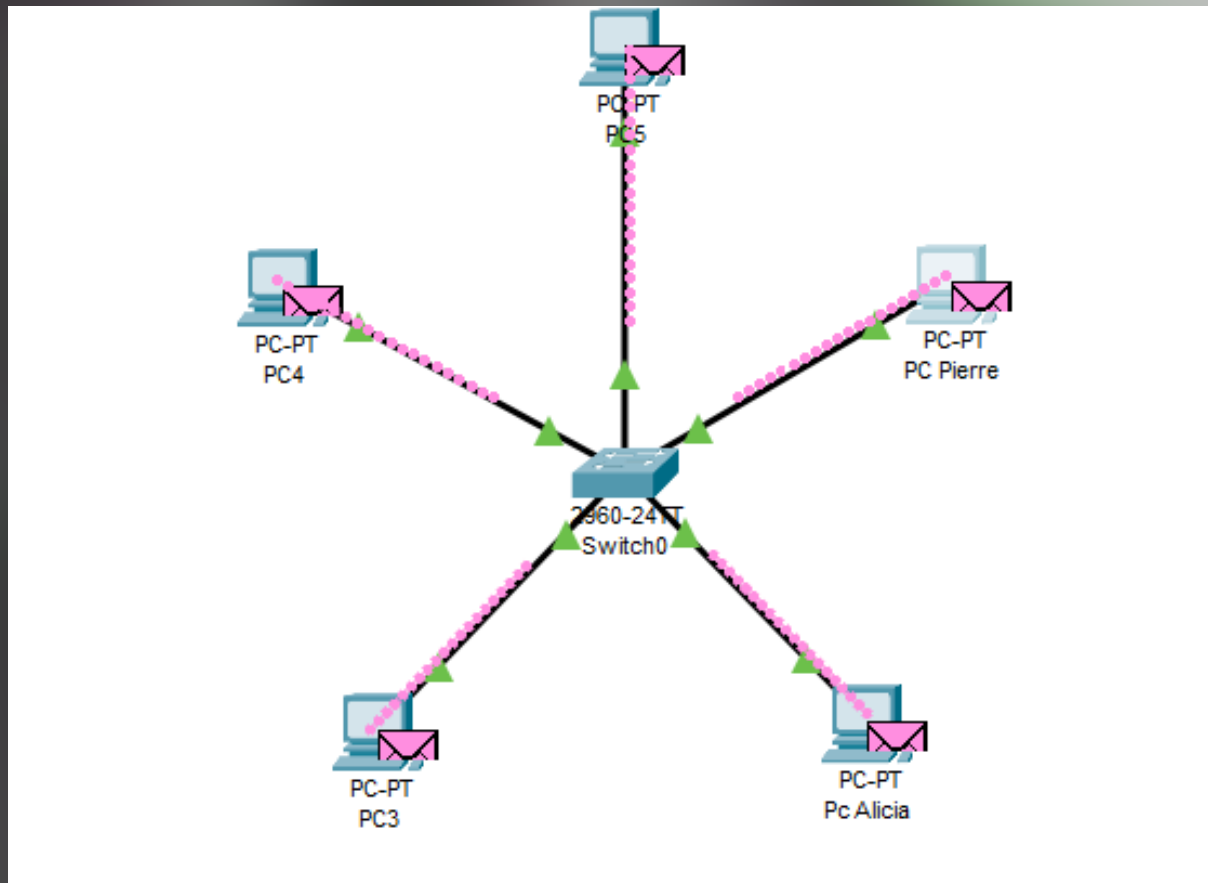
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=8ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128
Reply from 192.168.1.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>
```



## Mon réseau sur cisco

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

Un hub et un switch sont tous deux des périphériques utilisés dans les réseaux informatiques pour interconnecter des périphériques tels que des ordinateurs, des imprimantes, des routeurs, etc. Cependant, ils fonctionnent de manière différente et ont des caractéristiques distinctes :



❖ Hub (concentrateur) :

- Un hub est un périphérique de réseau de la couche physique qui permet de connecter plusieurs périphériques au sein d'un réseau local (LAN).
- Lorsqu'un périphérique envoie des données à un hub, le hub la diffuse à tous les autres ports connectés, quels que soient le destinataire et la source des données.
- Le hub n'est pas intelligent (ne possède pas de capacités d'intelligence ou de traitement complexe, contrairement à un switch) et fonctionne en mode half-duplex, ce qui signifie qu'il ne peut pas recevoir et transmettre des données simultanément sur un même port.

❖ Switch (commutateur) :

- Un switch est un périphérique de réseau de la couche liaison de données qui permet de connecter plusieurs périphériques au sein d'un réseau local (LAN).
- Lorsqu'un périphérique envoie des données à un switch, ce dernier détermine le port vers lequel les données doivent être transmises en fonction de l'adresse MAC du destinataire, puis transmet les données uniquement à ce port, évitant ainsi la diffusion à tous les ports.
- Les switches sont plus intelligents que les hubs et peuvent fonctionner en mode full-duplex, ce qui signifie qu'ils peuvent recevoir et transmettre des données simultanément sur un même port.

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

Un hub est un périphérique de réseau utilisé pour connecter plusieurs appareils au sein d'un réseau local (LAN). Il fonctionne à la couche physique du modèle OSI (couche 1) et agit comme un amplificateur de signal. Voici comment il fonctionne et quels sont ses avantages et inconvénients :

### ❖ Fonctionnement d'un hub :

- Réception de données : Lorsqu'un hub reçoit des données sur un port, il amplifie et transmet ces données à tous les autres ports du hub.
- Diffusion : Le hub diffuse les données reçues à tous les appareils connectés, quel que soit le destinataire. Cela signifie que toutes les machines connectées au hub voient le trafic, même si la donnée n'est destinée qu'à une seule d'entre elles.
- Half-duplex : Les hubs fonctionnent en mode half-duplex, ce qui signifie que les données peuvent être transmises dans un seul sens à la fois sur un port donné.

### ❖ Avantages d'un hub :

- Simplicité : Les hubs sont simples à installer et à configurer, ce qui les rend conviviaux pour les utilisateurs novices.



- Coût : Les hubs sont souvent moins chers que les switches, ce qui en fait une option économique pour les petits réseaux.
- Facilité d'extension : L'ajout de nouveaux appareils au réseau est simple avec un hub, car il suffit de les connecter à un port disponible.

❖ Inconvénients d'un hub :

- Collision de données : Étant donné que les données sont diffusées à tous les ports, cela peut entraîner des collisions de données, ce qui réduit l'efficacité du réseau.
- Bande passante partagée : La bande passante du hub est partagée entre tous les appareils connectés, ce qui peut entraîner des ralentissements lorsque plusieurs appareils tentent de communiquer simultanément.
- Manque de sécurité : Étant donné que les données sont diffusées à tous les ports, la sécurité est compromise car n'importe quel appareil peut voir tout le trafic du réseau.
- Faible performance : En raison de la nature de la diffusion et des collisions potentielles, les performances d'un hub sont généralement inférieures à celles d'un switch.

En résumé, bien que les hubs soient simples et peu coûteux, ils ont des limites en termes de performances, de sécurité et de gestion du trafic, ce qui fait que les switches sont préférés dans la plupart des environnements réseau modernes.

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

Un switch est un périphérique de réseau qui connecte plusieurs appareils au sein d'un réseau local (LAN). Il fonctionne à la couche liaison de données du modèle OSI (couche 2) et est plus sophistiqué qu'un hub. Voici les avantages et inconvénients d'un switch :

### ❖ Avantages d'un switch :

- **Efficacité de la bande passante** : Un switch transmet les données uniquement au port vers lequel le destinataire est connecté, évitant ainsi la diffusion inutile à tous les ports. Cela optimise l'utilisation de la bande passante et améliore les performances du réseau.
- **Faible collision de données** : Les collisions de données sont réduites car le switch utilise des tables d'adresses MAC pour diriger le trafic spécifiquement vers le port du destinataire.
- **Full-duplex** : Les switches permettent le fonctionnement en mode full-duplex, ce qui signifie qu'ils peuvent recevoir et transmettre des données simultanément sur un même port, améliorant ainsi l'efficacité du réseau.
- **Sécurité améliorée** : Étant donné que les données sont transmises spécifiquement au port du destinataire, les autres appareils du réseau ne peuvent pas les intercepter, renforçant ainsi la sécurité.



- **Gestion du trafic** : Les switches permettent une gestion plus fine du trafic en utilisant des fonctionnalités telles que le VLAN (Virtual LAN), le contrôle d'accès basé sur les ports et la qualité de service (QoS).
- **Adaptabilité et extensibilité** : Les switches peuvent être configurés et personnalisés en fonction des besoins spécifiques du réseau, et il est facile d'ajouter de nouveaux appareils et de les intégrer au réseau.

❖ **Inconvénients d'un switch :**

- **Coût** : Les switches sont généralement plus coûteux que les hubs en raison de leur sophistication et de leurs fonctionnalités avancées.
- **Complexité de configuration** : Configurer un switch peut être plus complexe que configurer un hub en raison de la diversité des fonctionnalités et des options disponibles.
- **Dépendance de l'alimentation électrique** : Les switches nécessitent de l'alimentation électrique pour fonctionner, ce qui signifie qu'ils sont inutilisables en cas de panne de courant, contrairement aux hubs passifs.

Dans l'ensemble, malgré leur coût supérieur et leur configuration plus complexe, les switches offrent des avantages significatifs en termes de performances, de sécurité et de gestion du trafic par rapport aux hubs, ce qui en fait un choix préféré dans la plupart des réseaux modernes.

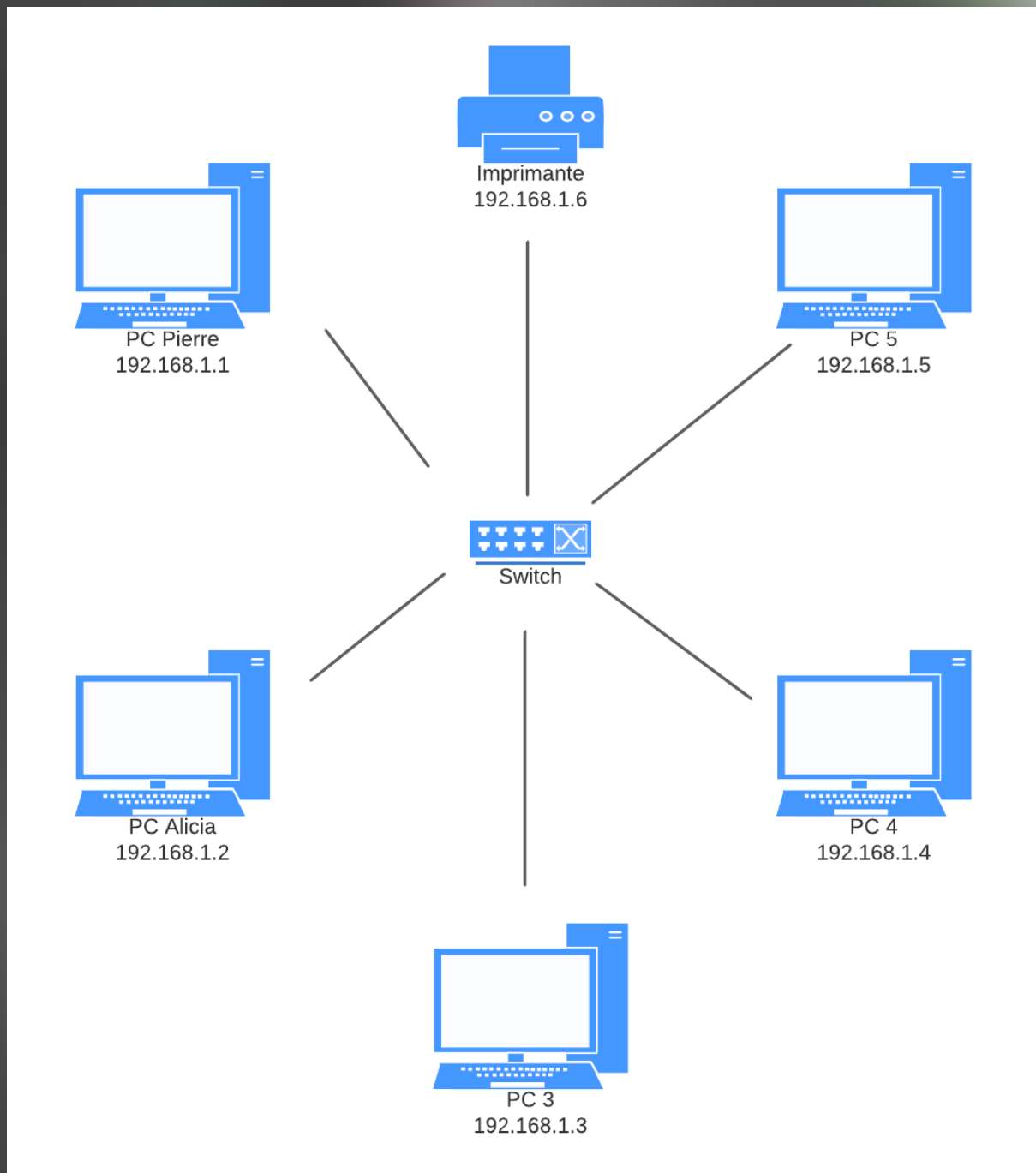
## → Comment un switch gère-t-il le trafic réseau ?

- ❖ Un switch gère le trafic réseau de manière intelligente en utilisant des tables d'adresses MAC (Media Access Control) et en basant ses décisions sur ces adresses. Voici comment cela fonctionne :
  - Lorsqu'un switch reçoit des données sur un port, il enregistre l'adresse MAC du périphérique source de ces données dans une table d'adresses MAC.
  - Le switch enregistre une table d'adresse MAC qui répertorie les adresses MAC et les ports auxquels elles sont associées.
  - Lorsqu'une trame de données est reçue par le switch, il regarde l'adresse MAC de destination dans l'en-tête de la trame. Il consulte ensuite sa table d'adresse MAC pour trouver le port associé à cette adresse MAC.
  - Le switch transmet la trame uniquement sur le port associé à l'adresse MAC de destination, minimisant ainsi la diffusion inutile de données à tous les ports comme c'est le cas avec un hub.
  - Si le switch ne connaît pas encore l'adresse MAC de destination, il diffuse la trame à tous les ports sauf celui d'origine. Lorsque la réponse est reçue, le switch met à jour sa table d'adresses MAC avec l'adresse MAC du nouveau périphérique associé au port correspondant.
  - Pour maintenir l'efficacité de la table d'adresses MAC, le switch applique un mécanisme d'aging où les entrées de la table expirent après un certain temps si elles ne sont pas utilisées. Cela permet d'éliminer les entrées obsolètes.

Grâce à ce processus de gestion du trafic basé sur les adresses MAC, optimisent l'utilisation de la bande passante et renforcent la sécurité du réseau en ne transmettant les données qu'aux destinataires appropriés. Cela contribue à des performances réseau améliorées et à une utilisation plus efficace des ressources.



## Job 9



```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=8ms TTL=128
Reply from 192.168.1.6: bytes=32 time=4ms TTL=128
Reply from 192.168.1.6: bytes=32 time=4ms TTL=128
Reply from 192.168.1.6: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>|
```

## Requête ping sur l'imprimante

### ❖ Avantages d'un Schéma :

- Avoir un schéma simplifie l'analyse et la compréhension du réseau donné.
- Cela rend la configuration du réseau plus claire et esthétique.
- Refaire la configuration et ainsi vérifier ou remarque si jamais il y as des erreurs



## Job 10

The screenshot shows the 'Server' configuration window with the 'Services' tab selected. The 'DHCP' service is configured for the 'FastEthernet0' interface. The 'Service' is turned 'On'. The configuration includes a pool named 'serverPool' with a default gateway of 0.0.0.0, DNS server of 0.0.0.0, and a start IP address of 192.168.1.0 with a subnet mask of 255.255.255.0. The maximum number of users is set to 256. The TFTP and WLC addresses are also 0.0.0.0. A table at the bottom lists the configured DHCP pool.

**SERVER**

Physical Config **Services** Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

**DHCP**

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 192 168 1 0

Subnet Mask: 255 255 255 0

Maximum Number of Users: 256

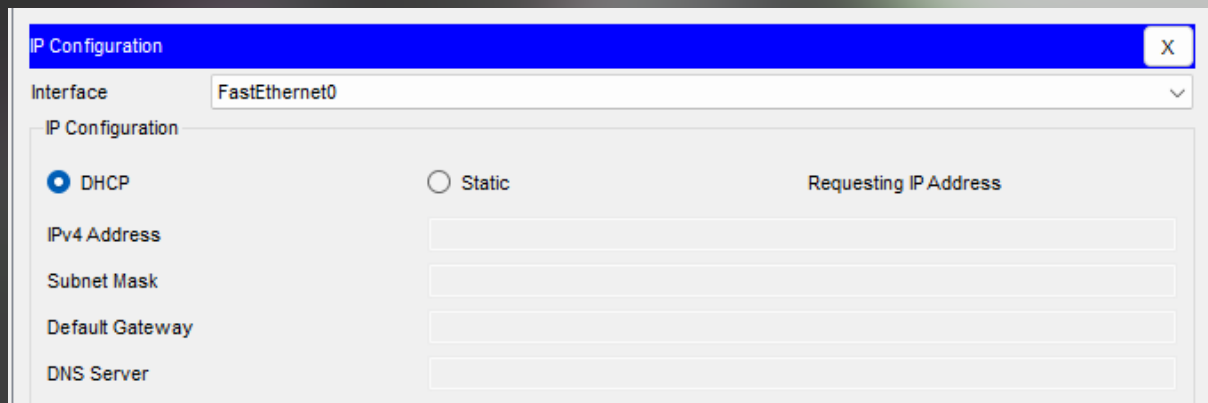
TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

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	192.168....	255.255....	256	0.0.0.0	0.0.0.0

☐ Top

Mise en place du serveur DHCP



IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static Requesting IP Address

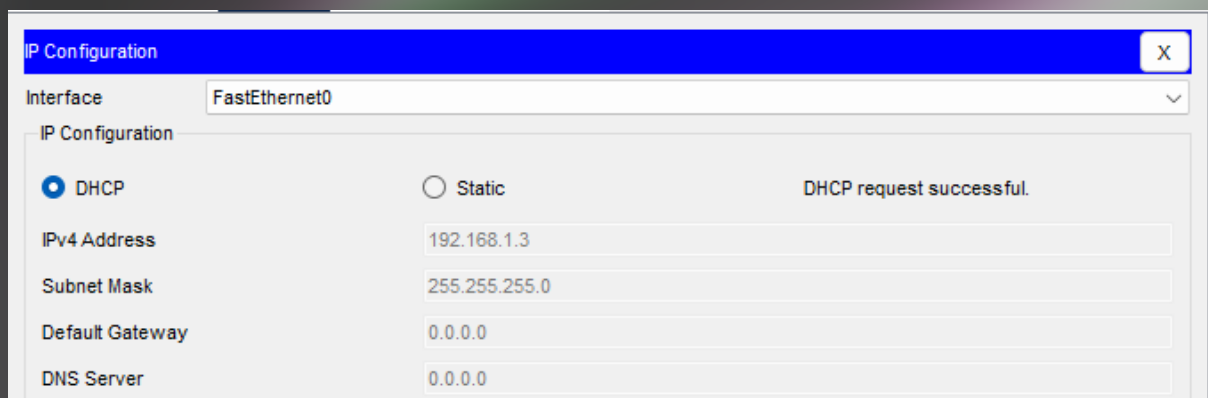
IPv4 Address:

Subnet Mask:

Default Gateway:

DNS Server:

**Demande d'adresse ip de la machine au serveur**



IP Configuration

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address: 192.168.1.3

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

**Adresse ip attribuée par le serveur**

**→ 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 affecter des adresses IP à des périphériques dans un réseau. Voici les différences entre les deux :



### ❖ Adresse IP statique :

- Une adresse IP statique est configurée manuellement par un administrateur réseau ou par l'utilisateur.
- L'attribution d'une adresse IP statique reste constante et ne change pas, sauf si elle est modifiée manuellement.
- Elle est souvent utilisée pour des périphériques tels que des serveurs, des imprimantes réseau, des routeurs, etc., dont l'adresse IP doit rester fixe pour des raisons de gestion et d'accès.

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

- Le DHCP est un protocole qui permet d'attribuer automatiquement des adresses IP et d'autres configurations réseau à des périphériques.
- L'adresse IP attribuée par DHCP peut changer à chaque fois que le périphérique se connecte au réseau ou lorsqu'il renouvelle sa location DHCP.
- Elle est généralement utilisée pour des périphériques tels que des ordinateurs, des téléphones, des tablettes, etc., qui ont besoin d'une adresse IP temporaire et peuvent partager les adresses IP disponibles dans le pool DHCP.

Une adresse IP statique est définie manuellement et reste constante, tandis qu'une adresse IP attribuée par DHCP est assignée automatiquement et peut changer au fil du temps. Le choix entre les deux dépend des besoins et des exigences spécifiques du réseau et des périphériques.

## Job 11

### → Plan d'adressage

Un masque de sous réseau est composé de 32 bits (11111111.11111111.11111111.11111111). Si on veut un certain nombre d'hôtes, on va calculer le nombre de bits qu'on doit attribuer aux hôtes. On nous donne comme base une adresse de classe A en 10.0.0.0.

Pour le premier on nous demande 1 sous réseau de 12 hôtes :

L'adresse commencera donc à 10.0.0.0 et se terminera à 10.0.0.15 ce qui fera donc 16 hôtes moins 2 (réserve pour le loopback et la passerelle) donc 14 hôtes. On nous demande effectivement 12 hôtes mais le calcul se fait en bits donc si on regarde le masque de sous réseau sera 255.255.255.240 ce qui donne binaire 11111111.11111111.11111111.11110000 il y a donc 4 bits réservés pour les hôtes.

Donc la plage d'adresses pour 12 hôtes sera : 10.0.0.0 à 10.0.0.15/28

Si on calcule cela donne 2 puissance 4 qui donne 16. Si l'on prend seulement 3 bits cela nous donne 2 puissance 3 qui nous donne seulement 8 donc on ne peut pas mettre 12 hôtes mais seulement 6 on prend donc le bits d'après qui nous amène à 16.

Pour le sous réseau de 30 hôtes on fait la même chose on retire un bit (11111111.11111111.11111111.11100000) ce qui rajoute une puissance de 2 donc (2 puissance 5 = 32) donc 32 hôtes moins 2 qui nous donne 30.

Et ainsi de suite on prendra le nombre de bits supérieur ou égal au nombre d'hôtes voulu.

Pour le reste des réseaux demander on aura pour les 120 hôtes :  $2^7 = 128$ , donc 7 bits pour les hôtes. Et pour celui de 160 hôtes :  $2^8 = 256$ , donc 8 bits pour les hôtes.



— — — — —	Plage d'adresses	Masque de sous-réseau et Nombre de bits
Sous-réseaux de 30 hôtes	10.0.0.16 à 10.0.0.47	255.255.255.224  11111111.11111111.11111111.11110000  /27 (5 bits)
	10.0.0.48 à 10.0.0.79	
	10.0.0.80 à 10.0.0.111	
	10.0.0.112 à 10.0.0.143	
	10.0.0.144 à 10.0.0.175	
Sous-réseaux de 120 hôtes	10.0.0.176 à 10.0.0.255	255.255.255.128  11111111.11111111.11111111.11100000  /25 (7 bits)
	10.0.1.0 à 10.0.1.127	
	10.0.1.128 à 10.0.1.255	
	10.0.2.0 à 10.0.2.127	
	10.0.2.128 à 10.0.2.255	
Sous-réseaux de 160 hôtes	10.0.3.0 à 10.0.3.255	255.255.255.0  11111111.11111111.11111111.00000000  /24 (8 bits)
	10.0.4.0 à 10.0.4.255	
	10.0.5.0 à 10.0.5.255	
	10.0.6.0 à 10.0.6.255	
	10.0.7.0 à 10.0.7.255	

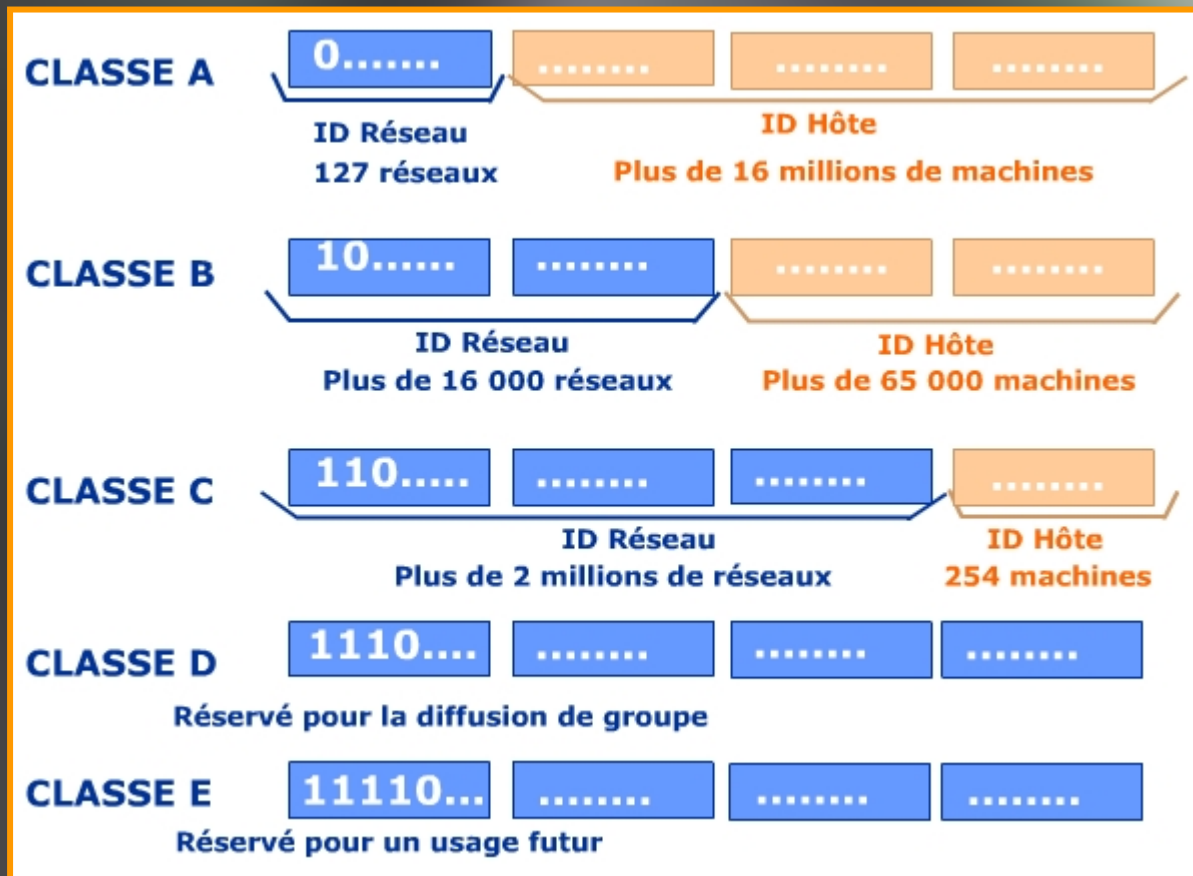
## Plage d'adresses

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

On a choisi une adresse de class A afin de pouvoir avoir un maximum d'utilisateurs  
L'adresse IP 10.0.0.0 est simplement une adresse privée couramment utilisée dans les réseaux locaux pour des intranets, des réseaux d'entreprise et d'autres réseaux internes. L'utilisation de cette plage d'adresse 10.0.0.0 -10.255.255.255 est une pratique courante pour la création de réseaux privés.

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

Il y a plusieurs classes de réseaux :



La différence entre chaque classe est le nombre de bits accordé à chaque partie du masque de sous réseau en fonction de ce que l'on veut par exemple en classe A on aura seulement 1 octet pour les réseaux donc 127 réseaux car seulement 7 bits disponible dans l'octet mais par contre pour les hôtes on aura 3 octets.

Pour à l'inverse une classe C communément utilisée pour les box que l'on a chez nous on aura 3 octets pour les réseaux donc approximativement 2 millions de réseaux et seulement 1 octet pour les utilisateurs ce qui fait 254 machines ce qui est largement suffisant dans le cadre d'une box de maison.



## Job 12

— — — — —	—	Unité de données	COUCHES	DESCRIPTION
Couches Hautes	7	Donnée	Application	Fournit des interfaces aux applications réseau
	6	Donnée	Présentation	Gère la représentation et la syntaxe des données
	5	Donnée	Session	Établit, gère et termine les sessions
	4	Segment	Transport	Divise les données en segments et assure le contrôle de flux
Couches matérielles	3	Paquet	Réseau	Effectue le routage et le transfert de paquets
	2	Trame	Liaison	Gère les trames et le contrôle d'accès au support
	1	Bit	Physique	Transmet des bits sur le support physique

**Modèle OSI (Open Systems Interconnection)**

## **1. Couche physique :**

- Ethernet (câble RJ45)
- Fibre optique
- Wifi (technologie sans fil)

## **2. Couche liaison de données :**

- MAC (Media Access Control)
- Ethernet (liaison Ethernet avec câble RJ45)

## **3. Couche réseau :**

- IPv4
- IPv6
- Routeur
- Wi-Fi (routage sans fil)

## **4. Couche transport :**

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

## **5. Couche session :**

- PPTP (Point-to-Point Tunneling Protocol)

## **6. Couche présentation :**

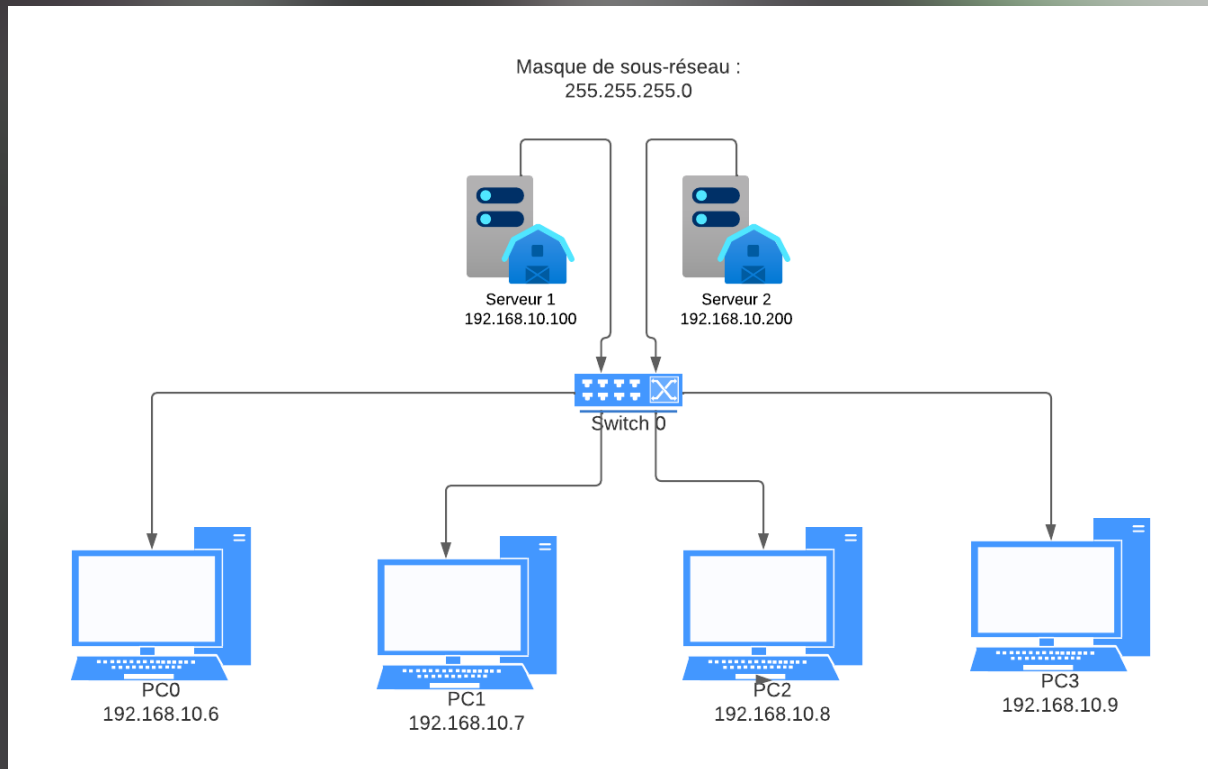
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- HTML (Hypertext Markup Language)

## **7. Couche application :**

- FTP (File Transfer Protocol)



## Job 13



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

C'est une architecture en étoile, dans cette configuration, tous les périphériques sont connectés à un concentrateur ou un commutateur central. Les périphériques ne sont pas directement connectés les uns aux autres. C'est une architecture simple à gérer, mais si le concentrateur central échoue, l'ensemble du réseau peut être affecté.

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

Pour ce réseau l'adresse IP du réseau est déterminée en prenant les trois premiers octets de n'importe quelle adresse IP fournie, puis en fixant le dernier octet à 0. Donc, l'adresse IP du réseau ci-dessus est : 192.168.10.0.

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

- Adresse du réseau (192.168.10.0) : Utilisée pour identifier le réseau.
- Adresse de diffusion (192.168.10.255) : Utilisée pour envoyer des données à tous les périphériques sur le réseau.

Donc, le nombre réel d'adresses IP disponibles pour les machines est de 254.

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

Pour ce réseau l'adresse de diffusion du réseau est déterminée en prenant les trois premiers octets de n'importe quelle adresse IP fournie, puis en fixant le dernier octet à 255. Donc, l'adresse de diffusion du réseau ci-dessus est : 192.168.10.255.

## Job 14

### Conversion des IP en binaire :

→ 145.32.59.24 en binaire est : 10010001.00100000.00111011.00011000

→ 200.42.129.16 en binaire est : 11001000.00101010.10000001.00010000

→ 14.82.19.54 en binaire est : 00001110.01010010.00010011.00110110



## Job 15

### → Qu'est-ce que le routage ?

Le routage est le processus de détermination du chemin optimal qu'un paquet de données doit emprunter pour atteindre sa destination à partir de son point de départ dans un réseau informatique ou de télécommunications. C'est essentiel pour acheminer efficacement les données d'un endroit à un autre en tenant compte de divers facteurs tels que la charge du réseau, les performances et les politiques de routage. Des protocoles de routage, comme BGP, OSPF et RIP, sont utilisés pour prendre ces décisions de manière automatisée.

### → Qu'est-ce qu'un gateway ?

Une passerelle, souvent appelée "gateway" en anglais, est un dispositif réseau permettant la communication entre deux réseaux différents. Elle traduit les protocoles, filtre le trafic, gère les accès et facilite la connexion entre ces réseaux hétérogènes. En résumé, c'est une interface qui facilite la communication entre des systèmes qui utilisent des normes différentes.

### → Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel, est un outil qui permet de sécuriser et anonymiser la connexion Internet. Il crée un tunnel crypté entre l'utilisateur et un serveur, masquant ainsi son adresse IP et chiffrant les données échangées. Cela garantit la confidentialité des activités en ligne, sécurise les connexions sur les réseaux publics (comme le Wi-Fi dans les cafés) et permet d'accéder à des contenus restreints géographiquement. Un VPN assure donc la confidentialité et la sécurité de la navigation sur Internet.

### → Qu'est-ce qu'un DNS ?

Le DNS (Domain Name System) est un système informatique qui traduit les noms de domaine en adresses IP, permettant ainsi aux ordinateurs de se connecter entre eux sur Internet. En d'autres termes, il transforme les adresses web faciles à retenir (comme "google.com") en adresses IP compréhensibles par les ordinateurs, indispensables pour acheminer le trafic sur le réseau.