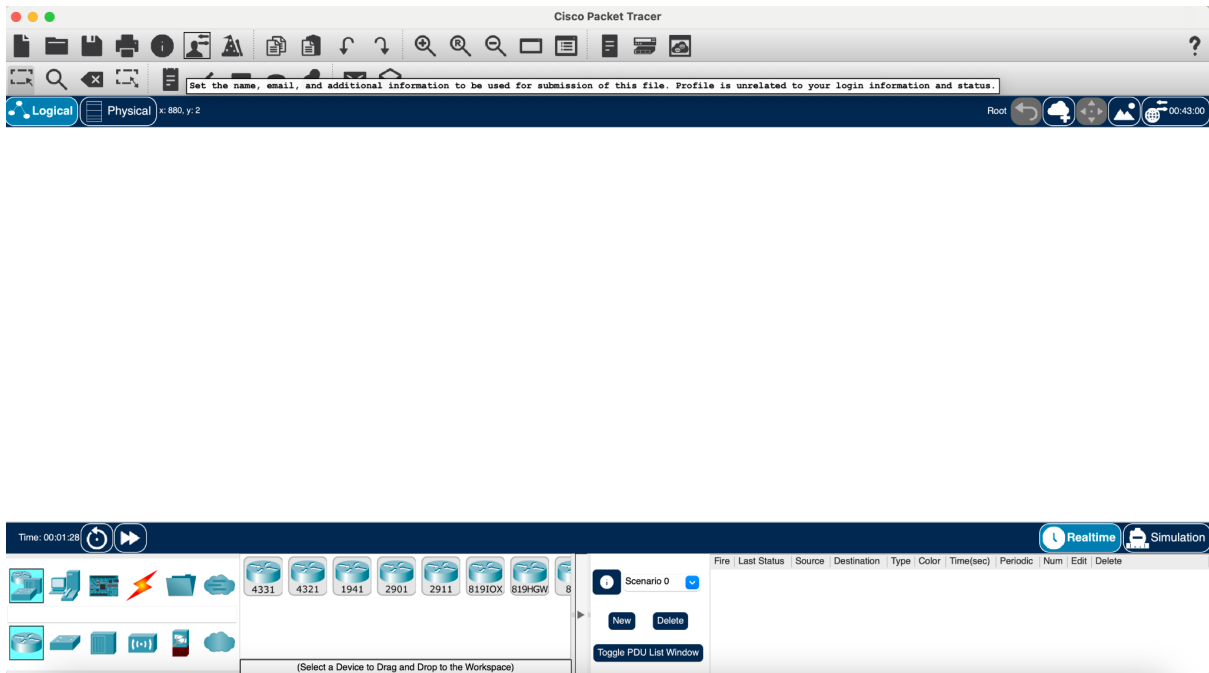


# JOB 1



# JOB 2

## Qu'est-ce qu'un réseau ?

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

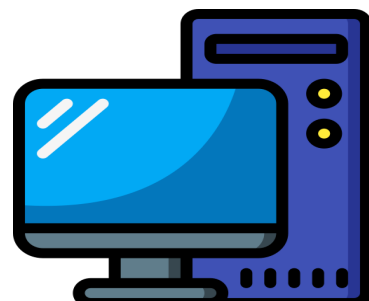
## À quoi sert un réseau informatique ?

Un réseau informatique sert à permettre la communication et le partage d'informations entre différents appareils informatiques. Cela peut inclure des ordinateurs, des serveurs, des périphériques et d'autres équipements. Les réseaux informatiques peuvent être utilisés à diverses fins comme le partage de ressources, la communication, l'accès à Internet.

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

- Ordinateur

Les ordinateurs dans un réseau jouent le rôle de clients (demandant des services), de serveurs (fournissant des



services), de nœuds de transit (dirigeant le trafic), de stockage partagé, de participants à des calculs distribués, et peuvent agir en tant que terminaux distants pour un accès à distance. Ils facilitent la communication et le partage de ressources entre les membres du réseau.

#### - Serveur

Le serveur dans un réseau a pour rôle principal de fournir des services, des données ou des ressources aux clients. Il répond aux demandes des clients, qu'il s'agisse de fournir des pages Web, des fichiers, des services d'impression, des courriels, ou d'autres fonctions spécifiques. Le serveur gère souvent des tâches critiques pour le réseau et assure la disponibilité des informations requises par les utilisateurs du réseau. En résumé, le serveur est le fournisseur centralisé de services et de ressources dans un réseau.



#### - Un Routeur

Le routeur, du moins le dispositif de réseau informatique que l'on appelle généralement routeur, est l'élément de matériel réseau qui permet la communication entre votre réseau domestique local – comme vos ordinateurs personnels et d'autres dispositifs connectés – et l'internet.

Un routeur est la première ligne de sécurité contre l'intrusion dans un réseau. En activant le plus haut niveau de sécurité sur le routeur, vous activez des éléments tels que le pare-feu. Ainsi, c'est le meilleur moyen de protéger votre système informatique et vos informations contre les attaques. La plupart de ces matériels se connectent à d'autres périphériques réseau uniquement avec des câbles réseau grâce à ses ports Ethernet. Ils ne nécessitent pas de pilotes pour fonctionner sous Windows, Mac ou d'autres systèmes d'exploitation. Cependant, ceux qui se connectent à un ordinateur par USB ou FireWire nécessitent généralement des pilotes pour fonctionner correctement. Les routeurs font souvent office de serveurs DHCP dans les petits réseaux d'entreprise ; en émettant des adresses IP uniques.



#### - Un Concentrateur (Hub)

Un hub est un dispositif en réseau qui permet de mettre plusieurs ordinateurs en contact. Définition pas très précise, puisque tout dispositif en réseau (ou presque) a le même but. Bref, ce qu'il faut retenir est qu'un hub est très bête, enfin, moins intelligent que les autres. Ce qu'il fait est tout simple : il reçoit des données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une



interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés). Attention, une interface permet la réception ET la diffusion. Comme vous pouvez le voir sur la photo ci-dessous, le hub n'a pas juste deux interfaces physiques, où on entre par la gauche et on ressort à droite, non ! L'interface de réception est logique. Exemple : j'ai un hub à 4 ports, avec 4 ordinateurs connectés. J'ai le port 1, 2, 3, 4 (ici, interface = port). Si l'ordinateur 4 (au port 4) veut communiquer avec les autres, moi le hub, je reçois les données au port 4 (c'est mon port de réception) et je renvoie les données aux ports 1, 2, et 3 : ce sont les ports de diffusion.

Le concentrateur permet de relier plusieurs ordinateurs entre eux, mais on lui reproche le manque de confidentialité.

## OU (meilleure option)

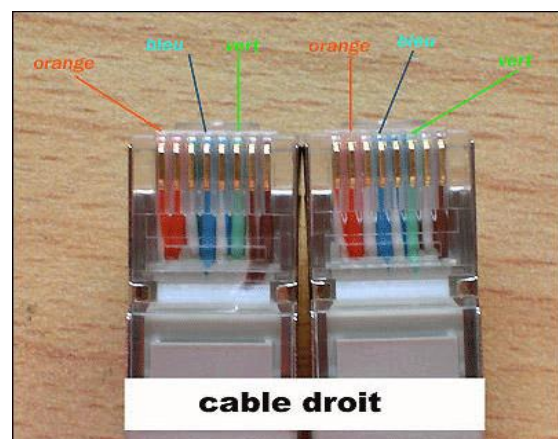
### - Un Commutateur (Switch)

Le commutateur (ou switch) et le routeur sont 2 appareils fondamentalement différents, et pourtant, leurs rôles se ressemblent tellement ! Au-delà de leur architecture, il faut comprendre leur différence au niveau d'un réseau. Le commutateur : juste une histoire d'échange de données. Un commutateur fonctionne à peu près comme un hub, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Si l'ordinateur 1 envoie des données à l'ordinateur 2, seul ce dernier les recevra et pas les autres connectés. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le switch se base sur les adresses physiques (adresses MAC) des cartes réseau. Pour faire une analogie avec la vie réelle, une adresse MAC est un peu comme une adresse postale. C'est une suite de 6 nombres hexadécimaux, par exemple 00-16-D4-C7-6E-D3. Un commutateur transmet donc des données aux autres ordinateurs en se basant sur leurs adresses MAC. Les transmissions sont plus confidentielles, les autres ne savent rien des données ne leur étant pas destinées. Son utilisation reste limitée aux réseaux locaux.



### - Câbles

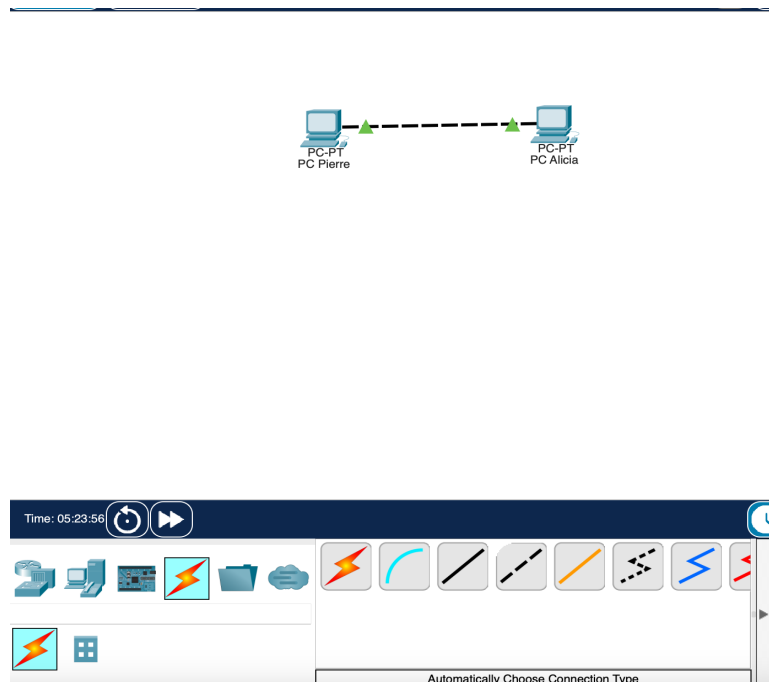
Il existe deux types de câble Ethernet : les câbles Ethernet droits et les câbles Ethernet croisés. Ces derniers permettent de relier directement entre eux deux ordinateurs alors que les câbles droits servent à relier un ordinateur à un autre appareil comme un hub



ou un switch que nous allons vous présenter dans ce chapitre.

Nous nous dirigeons donc vers des câbles Ethernet de raccordement droits

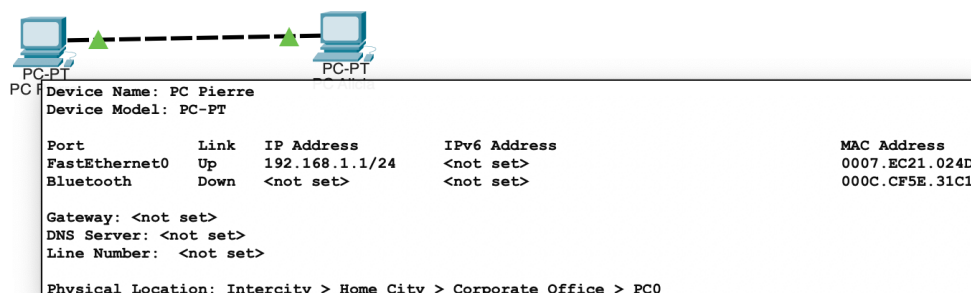
## JOB 3

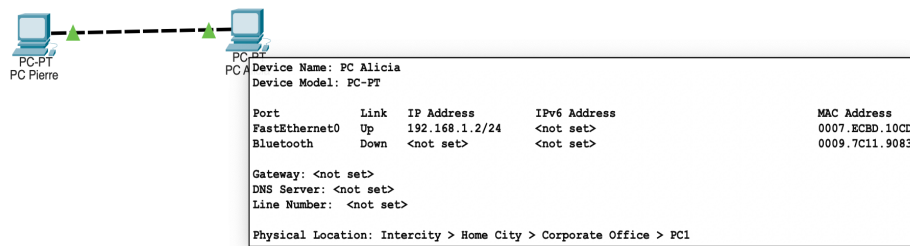


**Comme vous avez pu le constater, il existe des câbles croisés, droits... Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.**

J'ai utilisé un raccordement croisé car c'est le raccordement que l'on utilise pour connecter deux dispositifs de même type.

## JOB 4





## Qu'est-ce qu'une adresse IP ?

L'adresse IP est une adresse unique qui permet l'identification d'un appareil sur internet. IP signifie Internet Protocol, il correspond à un ensemble de règles établissant la gestion des données sur internet. L'adresse IP est donc un numéro d'identification attribué de façon permanente ou provisoire à un appareil sur internet. Ce numéro d'immatriculation est défini par l'ICANN (Internet Corporation for Assigned Names and Numbers), association qui gère les adresses IP au niveau mondial.

## À quoi sert un IP ?

Elle permet de le relier à un réseau informatique, c'est la base du système permettant l'acheminement des données sur internet. L'adresse IP permet à deux machines de s'identifier et de dialoguer entre elles, en échangeant des données sur Internet. De fait, tout appareil faisant partie d'un réseau interne ou externe nécessite une adresse IP pour communiquer avec les autres appareils et recevoir des paquets de données de leur part.

## Qu'est-ce qu'une adresse MAC ?

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

L'adresse MAC peut être modifiée dans certains cas. Cependant, cela reste assez rare car elle est activée dès la fabrication en usine.

Elle se présente sous la forme suivante : XX.XX.XX.XX.XX.XX. Les 12 caractères utilisés sont alphanumériques : de 0 à 9 et de A à F. Les 6 premiers chiffres (XX.XX.XX) permettent d'identifier le fabricant de l'appareil.

La fonctionnalité première d'une adresse MAC est l'identification de chaque périphérique.

Elle est utilisée sur la plupart des types de réseaux en vogue de nos jours, traditionnels (ethernet par exemple) ou mobile (Wi-Fi, Bluetooth...). L'adresse MAC étant unique, elle est souvent utilisée dans le filtrage de connexion à une borne WiFi par exemple. C'est en effet le moyen le plus efficace de bloquer l'accès à un appareil, plutôt que de bloquer une adresse IP qui pourra facilement être modifiée.

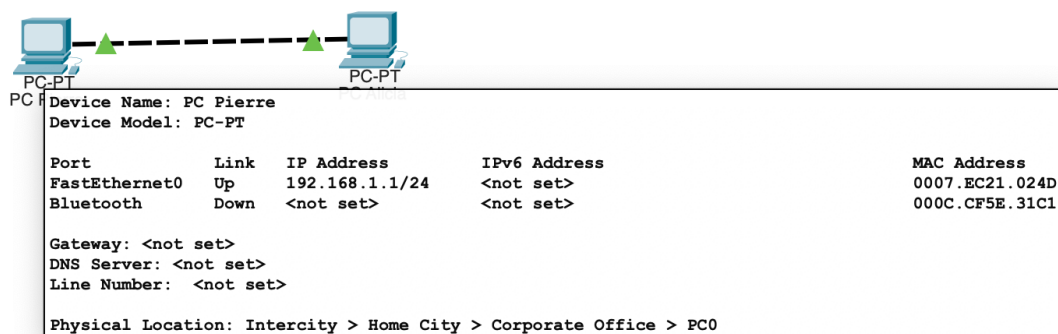
## Qu'est-ce qu'une IP publique et privée ?

La principale différence entre les adresses IP publiques et privées se situe au niveau de leur portée et du réseau auquel elles sont connectées. Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

Les adresses IP privées sont générées automatiquement tandis que les adresses IP publiques sont assignées par les FAI.

## Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau est 192.168.1.0



## JOB 5

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

J'ai utilisé la commande ipconfig.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::207:ECFF:FE21:24D
    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
```

## JOB 6

J'ai utiliser la commande: ping "Ip de Alicia"

```
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<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 = 2ms, Average = 0ms

C:\>
```

## JOB 7

```
Cisco Packet Tracer PC Command Line 1.0
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),
```

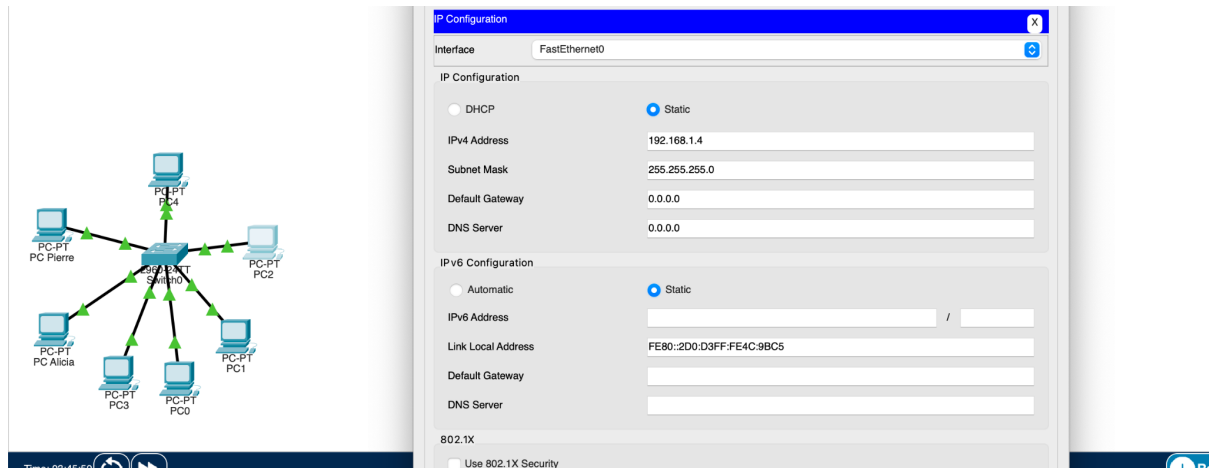
Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

Non, car lorsque l'on effectue un ping d'une machine A vers une machine B, et que l'on obtient **une réponse positive**, cela signifie que d'un point de vue du réseau, la



**machine A peut atteindre la machine B (route aller) et que la machine B peut atteindre la machine A** or étant donné que la machine de pierre est éteinte celle-ci ne peut ni communiquer avec la machine d'Alice ni recevoir des requêtes de la part d'Alice.

## JOB 8



Voilà le réseau chacun des ordinateurs est relié au switch par des câbles Ethernet de raccordement droit. Pour configurer les nouveaux pc sur le même sous-réseau, j'ai configuré les IP étant donné que celles de Pierre et Alicia sont 192.168.1.1 et 192.168.1.2 j'ai alloué les IP de 192.168.1.2 à 192.168.1.7 pour les nouveaux pc et avec le même masque de sous-réseau pour chacun des PC soit 255.255.255.0

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

Un commutateur fonctionne à peu près comme un hub, sauf qu'il est plus discret et intelligent. Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Si l'ordinateur 1 envoie des données à l'ordinateur 2, seul ce dernier les recevra et pas les autres connectés contrairement au hub qui lui enverra à toutes les autres machines connectées. Afin de déterminer l'ordinateur à qui il faut renvoyer les données, le switch se base sur les adresses physiques (adresses MAC) des cartes réseau.

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

**Avantages :** Les concentrateurs réseau sont le type le plus simple de dispositif de connexion pour les réseaux locaux (LAN) et offrent des avantages distincts pour les réseaux domestiques. Fonction Un concentrateur de réseau offre une connectivité



simple pour un réseau domestique qui n'a pas besoin de commutation complexes à gérer les taux élevés de trafic . Coût: un concentrateur de réseau simple est nettement moins cher qu'un commutateur ou un routeur . Certains coûtent moins de 30 \$. Partagée Accès Internet Un concentrateur de réseau permet une seule connexion Internet pour être partagée entre plusieurs ordinateurs. évolutivité concentrateurs réseau peuvent avoir quatre, cinq, huit ou 16 ports à laquelle les ordinateurs peuvent être connectés. Beaucoup de concentrateurs de réseau ont également un port "uplink" qui permet à l'utilisateur de connecter plusieurs hubs de sorte que plus d'ordinateurs peuvent être connectés au réseau. Network Monitoring raison concentrateurs de réseau transmettent toutes les données reçues de tous les périphériques connectés , ils permettent facile, peu coûteux de surveillance de l'ensemble du réseau . compatibilité ascendante Un concentrateur réseau est le moins cher et le plus facile façon de connecter certains types de périphériques réseau plus âgés, en particulier ceux qui ne supportent 10BASE2 ports, à un réseau moderne.

**Inconvénients** : La technologie qui se cache derrière les hubs est donc considérée comme étant vulnérable et obsolète. En plus de la perte de vitesse mentionnée ci-dessus et du manque de flexibilité relatif au transfert de données et à la sélection des récepteurs, un système de hubs est souvent assez vulnérable face aux failles de sécurité. Comme un tel système ne peut être mis en quarantaine, le trafic de données n'est pas protégé. Les potentiels problèmes de sécurité ou les éventuelles préoccupations liées à la protection des données concernent forcément tous les hôtes connectés.

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

#### **Avantages des Switchs :**

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

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

Incrémenter la présentation – Ils incrémentent la présentation de l'organisation.

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

Simple – Les commutateurs peuvent être directement associés aux postes de travail.

Augmente la bande passante – Il augmente la bande passante disponible du réseau.

Moins de collisions de trames – Les réseaux qui utilisent des commutateurs auront moins de collisions de trames

Plus sécurisé – Étant donné que le commutateur est isolé, les données n'iront qu'à la destination.

### **Inconvénients des switchs :**

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

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

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

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

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

Les composants mécaniques peuvent s'user – Les composants mécaniques du commutateur peuvent s'user avec le temps.

Le contact physique est obligatoire – Doit avoir un contact physique avec l'objet à actionner.

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

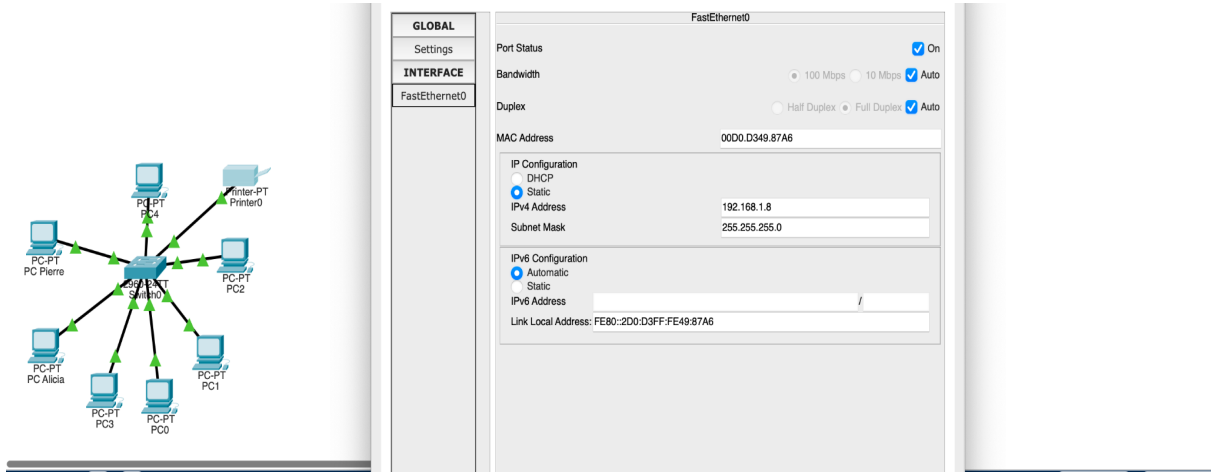
Un switch gère le trafic réseau en utilisant des adresses MAC (Media Access Control). Chaque appareil connecté à un switch a une adresse MAC unique. Lorsqu'un périphérique envoie des données, le switch examine l'adresse MAC de destination de chaque trame de données pour déterminer à quel port envoyer la trame.

Le switch maintient une table de correspondance entre les adresses MAC et les ports du réseau. Lorsqu'une trame arrive au switch, il enregistre l'adresse MAC source et le port sur lequel la trame est arrivée dans sa table. Ainsi, il sait comment atteindre chaque adresse MAC sur le réseau.

Lorsqu'une trame est destinée à une adresse MAC particulière, le switch la transmet uniquement au port associé à cette adresse, plutôt que de la diffuser à tous les ports comme le ferait un hub. Cela permet d'optimiser le trafic réseau et d'améliorer les performances.

En résumé, un switch utilise des adresses MAC pour diriger le trafic uniquement vers les ports nécessaires, réduisant ainsi la congestion du réseau et améliorant son efficacité.

## JOB 9



J'ai ajouté mon imprimante à mon réseau en utilisant un câble de raccordement droit, et je lui ai alloué une ip et le même masque de sous réseau que sur les autres machines du réseau.

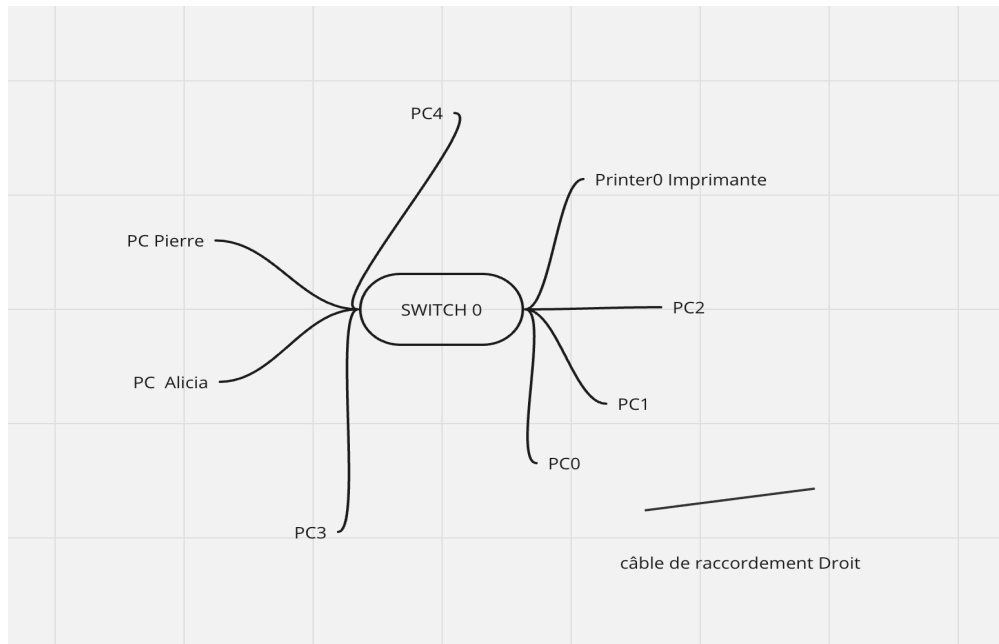
```
C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128
Reply from 192.168.1.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

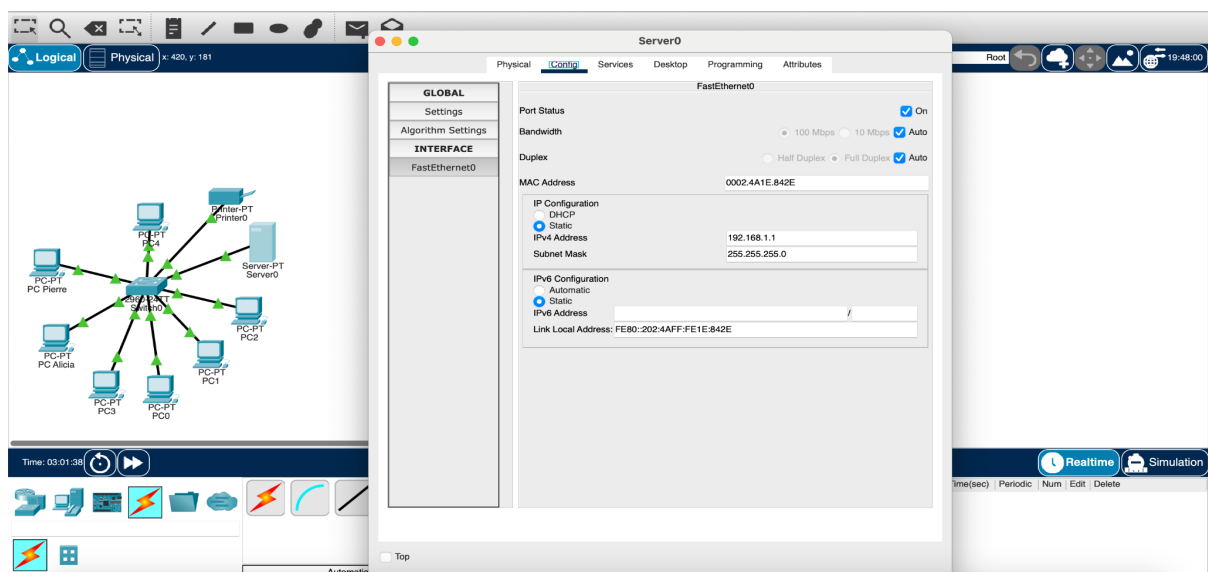
J'ai Ping l' IP de mon Imprimante pour vérifier qu'elle est bien connectée au réseau, elle l'est bien.



**identifiez au moins trois avantages importants d'avoir un schéma**

- Schéma facile et rapide à mettre en place.
- Si le travail est fait en équipe cela permet de communiquer le schéma réseau rapidement aux autres collaborateurs
- Le schéma peut être créé et communiqué à des personnes qui n'ont pas téléchargé Cisco Packet Tracer ou ne savent pas l'utiliser. Cela leur permettra de comprendre rapidement le fonctionnement du réseau.

## JOB 10



J'ai commencer par ajouter un serveur puis je l'ai relié au switch avec un raccordement droit, j'ai définis une ip statique de début dans config ainsi que le subnet mask je suis ensuite aller dans section services /dhcp définis l ip de début et le subnet mask puis sauvegarder.

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

**Adresse IP statique** Une adresse IP statique est une adresse qui est attribuée en permanence à vos appareils réseau par votre fournisseur d'accès Internet et qui ne change pas même si votre appareil est réinitialisé. Les adresses IP statiques ont généralement deux versions : IPv4 et IPv6. Une adresse IP statique est généralement attribuée à un serveur qui héberge des sites web et fournit des services de courrier électronique, de VPN et de FTP. Dans l'adressage IP statique, chaque appareil du réseau a sa propre adresse sans redondance et les adresses IP statiques devront être configurées manuellement. Lorsque de nouveaux dispositifs sont connectés à un réseau, vous devez sélectionner l'option de configuration "manuelle" et saisir l'adresse IP, le masque de sous-réseau, la passerelle de défaut et le serveur DNS. Un exemple typique d'utilisation d'une adresse IP statique est le serveur web. Depuis la fenêtre de votre ordinateur, allez à START -> RUN -> tapez "cmd" -> OK. Tapez ensuite "ping www.google.com" dans la fenêtre de commande, vous verrez l'interface comme vous pouvez le voir dans l'exemple ci-dessous. Le numéro à quatre octets 74.125.127.147 est l'adresse IP actuelle de www.google.com. S'il s'agit d'une adresse IP statique, vous pourrez vous connecter à Google à tout moment en utilisant cette adresse IP statique dans le navigateur web si vous souhaitez visiter Google.

**Adresse IP attribuée par un DHCP:** Au contraire de l'adresse IP statique, il y a l'adresse IP dynamique. Le sujet IP statique ou dynamique est très populaire auprès de nombreux techniciens en informatique. L'adresse IP dynamique est une adresse qui ne cesse de changer. Pour créer des adresses IP dynamiques, le réseau doit disposer d'un serveur DHCP configuré et opérationnel. Le serveur DHCP attribue une adresse IP vacante à tous les appareils connectés au réseau. Le DHCP est un moyen d'attribuer dynamiquement et automatiquement des adresses IP à des périphériques de réseau sur un réseau physique. Il fournit un moyen automatisé de distribuer et de mettre à jour les adresses IP et d'autres informations de configuration sur un réseau.

## **JOB 11**

### **1 sous-réseau de 12 hôtes**

On veut 2 hôtes sur le réseau étant données que deux Ip sous déjà utilisée par le réseau l'ip du réseau ainsi que l'ip broadcast nous allons devoir faire  $12+2$  ce qui fait 14 Ip à ajouter au réseau . On compte les bits en puissance de 2 donc 14 ip correspondrait à 2 puissance 4 qui fait 16.

pour connaître l'adresse de sous réseau nous allons faire partir de 255.255.255.255

et faire  $255-16+1=240$  (+1 car on comptabilise le 0 ce qui fait 256 Ip possibles)  
le masque de sous réseau est donc 255.255.255.240  
Nous avons donc un sous réseau de 16 qui pourrait compter jusqu'à 14 hôtes .

10.0.0.0 - 10.0.0.1 → 10.0.0.14 - 10.0.0.15

#### **5 sous-réseaux de 30 hôtes**

**subnet mask** : 255.255.255.224

10.1.0.0 - 10.1.0.1 → 10.1.0.30 - 10.1.0.31  
10.2.0.0 - 10.2.0.1 → 10.2.0.30 - 10.2.0.31  
10.3.0.0 - 10.3.0.1 → 10.3.0.30 - 10.3.0.31  
10.4.0.0 - 10.4.0.1 → 10.4.0.30 - 10.4.0.31  
10.5.0.0 - 10.5.0.1 → 10.5.0.30 - 10.5.0.31

#### **5 sous-réseaux de 120 hôtes**

**subnet mask** : 255.255.255.128















10.6.0.0 - 10.6.0.1 → 10.6.0.126 - 10.6.0.127  
10.7.0.0 - 10.7.0.1 → 10.7.0.126 - 10.7.0.127  
10.8.0.0 - 10.8.0.1 → 10.8.0.126 - 10.8.0.127  
10.9.0.0 - 10.9.0.1 → 10.9.0.126 - 10.9.0.127  
10.10.0.0 - 10.10.0.1 → 10.10.0.126 - 10.10.0.127

#### **5 sous-réseaux de 160 hôtes**

**subnet mask** : 255.255.255.0

10.11.0.0 - 10.11.0.1 → 10.11.0.254 - 10.11.0.255  
10.12.0.0 - 10.12.0.1 → 10.12.0.254 - 10.12.0.255  
10.13.0.0 - 10.13.0.1 → 10.13.0.254 - 10.13.0.255  
10.14.0.0 - 10.14.0.1 → 10.14.0.254 - 10.14.0.255  
10.15.0.0 - 10.15.0.1 → 10.15.0.254 - 10.15.0.255

## JOB 12

7		COUCHE APPLICATION	Point de contact avec les services réseaux	 DONNÉES	TELNET, FTP, HTTP, SMTP, ETC.
6		COUCHE PRÉSENTATION	Préparation des données pour la présentation (formatage, chiffrement, encodage etc.)	 DONNÉES	HTML, DOC, MP3, JPEG, ETC.
5		COUCHE SESSION	Organisation de la session de communication (points de contrôle, etc.)	 DONNÉES	SIP, RTP, ETC.
4		COUCHE TRANSPORT	Coordination du transfert des segments (numéro de port, contrôle réception, etc.)	 SEGMENTS	TCP, UDP, SSL, TLS, ETC.
3		COUCHE RÉSEAU	Routage des paquets entre les noeuds d'un réseau	 PAQUETS	IP, ARP, ETC.
2		COUCHE LIAISON	Assure le transfert des trames de noeud à noeud	 TRAMES	ETHERNET, PPP, ETC.
1		COUCHE PHYSIQUE	Transmission des bits	 BITS	MULTIPLEXING, MODULATION, ETC.

## JOB 13

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

L'architecture de ce réseau est un réseau local de classe C avec des adresses IP privées dans la plage 192.168.10.0/24. C'est une configuration typique pour de petits réseaux d'entreprise ou domestiques.

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

L'adresse Ip de ce réseau 192.168.10.0

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

Le nombre maximum d'ip est de 255.

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

L'adresse de diffusion de ce réseau est 192.168.10.200.



## **JOB 14**

Convertissez les adresses IP suivantes en binaires :

145.32.59.24 = 10010001.00100000.00111011.00011000  
200.42.129.16 = 11001000.00101010.10000001.00010000  
14.82.19.54 = 00001110.01010010.00010011.00110110

## **JOB 15**

### **Qu'est-ce que le routage ?**

Le routage est le processus de sélection du chemin dans un réseau. Un réseau informatique est composé de nombreuses machines, appelées nœuds, et de chemins ou de liaisons qui relient ces nœuds. La communication entre deux nœuds d'un réseau interconnecté peut s'effectuer par de nombreux chemins différents. Le routage est le processus qui consiste à sélectionner le meilleur chemin à l'aide de certaines règles prédéterminées

### **Qu'est-ce qu'un gateway ?**

Une gateway (passerelle) 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 la box Internet.

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 ?**

Le nom VPN venant de l'anglais Virtual Private Network est traduit en français Réseau Privé Virtuel. Ce réseau est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

Il y a 2 types de vpn :

**VPN SSL:** Secure Sockets Layer (SSL) est un protocole de cryptage du trafic HTTP , tel que les connexions entre les appareils des utilisateurs et les serveurs Web .

### **VPN IPSEC**

L'IPsec est un groupe de protocoles utilisés ensemble pour établir des connexions sécurisées entre des périphériques au niveau de la couche 3 du modèle OSI. Pour ce faire, IPsec brouille tous les messages afin que seules les parties autorisées puissent les comprendre.

### **Qu'est-ce qu'un DNS ?**

Les serveurs DNS traduisent des demandes de noms en adresses IP et inversement, en contrôlant à quel serveur un utilisateur final va se connecter quand il tapera un nom de domaine ou l'ip dans son navigateur. Ces demandes sont appelées requêtes.