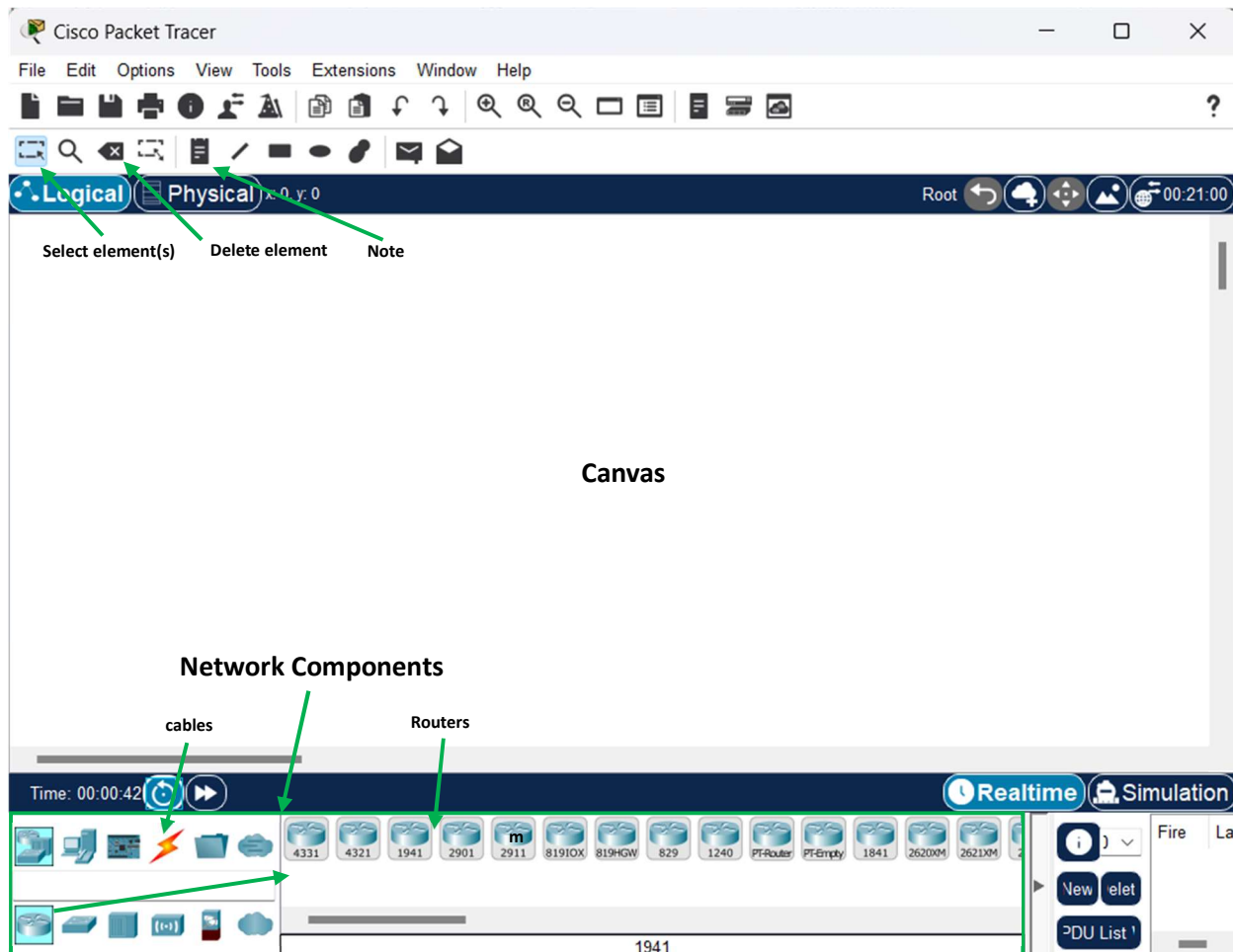


# Runtrack Réseau

## 1 – Logiciel Cisco Packet Tracer pour la planification du réseaux

Avec Cisco Packet Tracer, nous pouvons planifier et simuler des réseaux, qu'ils soient simples ou sophistiqués. Pour installer le [logiciel](#), nous devons nous inscrire et créer un compte d'étudiant.

Voici à quoi ressemble l'application lorsqu'une nouvelle fenêtre est ouverte :



## 2 – Construction du réseau informatique

### → Qu'est-ce qu'un réseau ?

Un réseau est un groupe ou un système d'éléments interconnectés qui peuvent communiquer entre eux et partager des données les uns avec les autres.

### → À quoi sert un réseau informatique ?

Un réseau informatique permet à ses utilisateurs de partager instantanément des ressources, qu'il s'agisse de données ou de périphériques, avec un ou plusieurs utilisateurs (collaboration sur des documents, partage d'imprimantes, de serveurs dédiés, de connexions Internet).

### → Quel matériel avons-nous besoin pour construire un réseau ?

Pour créer un réseau local (LAN - Local Area Network) simple sans connexion Internet, nous avons besoin de quelques éléments essentiels. Tout d'abord, **deux ordinateurs** équipés de ports Ethernet RJ45 et des **câbles Ethernet RJ45 cross-over** sont nécessaires.

**Câbles Ethernet RJ45** sont indispensables pour établir une communication stable et rapide entre les appareils du réseau. Ils permettent aux données de circuler efficacement. RJ45 signifie Registered Jack 45, et c'est un connecteur standard utilisé pour les câbles Ethernet, notamment dans les réseaux Ethernet. Pour connecter le routeur au modem, nous avons besoin d'un câble Ethernet croisé (crossover), mais pour connecter les appareils (ordinateurs, concentrateurs, commutateurs) au routeur ou switch ou hub, nous avons besoin d'un **câble Ethernet droit (straight-through) avec le même connecteur RJ45**.

En cas de besoin de connexion à Internet, une **connexion Internet active** fournie par un fournisseur de services Internet est requise.

**Modem** est responsable de la traduction du signal Internet dans un format lisible par l'ordinateur. Généralement fourni par le fournisseur de services Internet, le modem détient une adresse IP publique qui lui est fournie par le fournisseur de services Internet. Cette adresse IP publique ne peut être utilisée que par un seul ordinateur, même s'il est connecté à un commutateur (switch) ou à un concentrateur (hub) auquel de nombreux ordinateurs sont connectés. Un modem peut également être utilisé seul lorsque vous travaillez avec un seul ordinateur. Il peut être connecté via Ethernet ou même via Wi-Fi pour certains modèles qui combinent les fonctionnalités de modem et de routeur, simplifiant ainsi la configuration et ajoutant des fonctionnalités réseau.

**Routeur** joue un rôle essentiel lorsque plusieurs appareils sont configurés dans le réseau. Il peut fournir une connexion Internet via Wi-Fi à plusieurs appareils et permettre le partage de la seule adresse IP publique entre eux. Le routeur dispose d'un service appelé NAT (Network Address Translation - Traduction d'Adresse Réseau). Ce module est responsable de la création de plusieurs adresses IP privées individuelles que chaque ordinateur du LAN peut utiliser pour établir une connexion Internet via la seule adresse IP publique. En résumé, le routeur prend cette unique adresse IP publique et en crée de nombreuses autres adresses IP privées. De plus, les routeurs modernes offrent souvent des fonctionnalités de sécurité avancées, telles que des pare-feux, pour protéger le réseau contre les menaces en ligne.

En résumé, le modem relie le réseau à Internet, le routeur dirige le trafic, les câbles Ethernet RJ45 permettent aux données de circuler, et les ordinateurs se connectent entre eux et au réseau.

### 3 – Câbles Ethernet – Droit ou Croisé

Les câbles Ethernet peuvent être câblés en tant que câbles droits ou croisés (straight-through or cross-over).



Deux ordinateurs sont connectés entre eux à l'aide du câble Ethernet RJ45 croisé en cuivre - il s'agit d'un câble RJ45 croisé standard utilisé pour connecter deux dispositifs du même type entre eux.

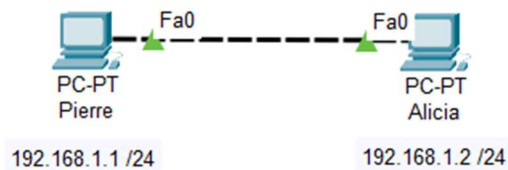
Un câble droit est un type de câble utilisé dans les réseaux locaux pour connecter un ordinateur à un concentrateur de réseau tel qu'un routeur. Sur un câble droit, les broches câblées sont identiques. Les câbles droits utilisent une norme de câblage : les deux extrémités utilisent la norme de câblage T568A ou les deux extrémités utilisent la norme de câblage T568B. Ils peuvent être utilisés avec les types de ports Ethernet, Fast Ethernet et Gigabit Ethernet.

Un câble Ethernet croisé est un type de câble Ethernet utilisé pour connecter directement des dispositifs informatiques entre eux. Contrairement au câble droit, le câble Ethernet croisé RJ45 utilise deux normes de câblage différentes : une extrémité utilise la norme de câblage T568A, et l'autre extrémité utilise la norme de câblage T568B. Le câble Ethernet croisé inverse les signaux de transmission et de réception au niveau du câblage interne. Il est le plus souvent utilisé pour connecter deux dispositifs du même type, par exemple deux ordinateurs ou deux commutateurs entre eux.

Généralement, les câbles droits sont principalement utilisés pour connecter des dispositifs différents, tandis que les câbles croisés sont utilisés pour connecter des dispositifs similaires. Ainsi, pour connecter deux ordinateurs, nous avons choisi un câble Ethernet croisé.

## 4 – Configuration des adresses IP

Afin que ces ordinateurs puissent communiquer entre eux, il est nécessaire de configurer manuellement les adresses IP de chaque ordinateur. Configurons l'ordinateur de Pierre avec l'adresse IP 192.168.1.1 et le masque de sous-réseau 255.255.255.0, et l'ordinateur d'Alicia avec l'adresse IP 192.168.1.2 et le masque de sous-réseau 255.255.255.0.



### → Qu'est-ce qu'une adresse IP ?

Une adresse IP est une adresse unique, un identifiant, qui permet l'envoi d'informations entre des appareils sur un réseau. Les adresses IP contiennent des informations de localisation et rendent les appareils accessibles pour la communication. IP signifie "Internet Protocol", qui est l'ensemble de règles régissant le format des données envoyées via Internet ou un réseau local. Une adresse IP est une série de chiffres séparés par des points. Les adresses IP sont exprimées sous la forme de quatre chiffres - par exemple, une adresse type pourrait être 192.168.1.38. Chaque chiffre de l'ensemble peut aller de 0 à 255. Ainsi, la plage complète des adresses IP va de 0.0.0.0 à 255.255.255.255.

Le développement de l'IP a commencé en 1974, sous la direction des informaticiens Bob Kahn et Vint Cerf. Elle est fréquemment utilisée avec le protocole de contrôle de transmission, ou TCP (transmission control protocol). Ensemble, ils sont désignés sous le nom de TCP/IP.

La première version majeure du Protocole Internet était la version 4, ou IPv4. En 1981, elle a été formellement définie dans le [RFC 791](#) par le groupe de travail d'ingénierie de l'Internet, ou IETF ([Internet Engineering Task Force](#)).

Le successeur d'IPv4 est IPv6, qui a été formalisé par l'IETF en 1998. Il a été conçu pour finalement remplacer IPv4. Cependant, IPv6 est adopté lentement. On s'attendait à ce que le trafic IPv6 atteigne 50 % en 2018, et en septembre 2023, l'utilisation d'IPv6 par Google a atteint un nouveau record de 45,28 %. On prévoit qu'il atteindra une adoption de 50 % quelque part en 2024 (soit 6 ans plus tard que prévu). Le pays le plus adapté à IPv6 est l'Inde - [selon APNIC Labs](#), plus de 77 % du trafic en Inde transite via IPv6.

Les adresses IP ne sont pas aléatoires. Elles sont mathématiquement produites et allouées par l'Autorité des numéros attribués sur Internet (IANA – [Internet Assigned Numbers Authority](#)), une division de la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN – [Internet Corporation for Assigned Names and Numbers](#)). L'ICANN est une organisation à but non lucratif créée aux États-Unis en 1998 pour contribuer à maintenir la sécurité d'Internet et permettre son utilisation par tous. Chaque fois que quelqu'un enregistre un domaine sur Internet, il passe par un registraire de noms de domaine, qui paie des frais minimes à l'ICANN pour enregistrer le domaine.

### → À quoi sert un IP ?

Internet a besoin d'un moyen de différencier entre différents ordinateurs, routeurs et sites web. Les adresses IP fournissent un moyen de le faire et constituent une partie essentielle du fonctionnement d'Internet.

Une adresse IP remplit deux fonctions principales : elle identifie l'hôte, plus précisément son interface réseau, et elle fournit l'emplacement de l'hôte dans le réseau, permettant ainsi d'établir un chemin vers cet hôte. Le protocole Internet offre la possibilité de "[livrer un paquet de bits d'une source à une destination via un système interconnecté de réseaux](#)". L'en-tête de chaque paquet IP contient l'adresse IP de l'hôte émetteur et celle de l'hôte de destination.

IP addresses are therefore used to identify devices and are unique to a device within a subnet. A subnet cannot have a duplicate IP address. This means that no devices on the network can have the identical IP address as it causes an IP conflict. If two devices have the same IP address, the network will confuse the devices, and to resolve the conflict, one will be kicked off the network.

Les adresses IP sont donc utilisées pour identifier les appareils et sont uniques pour un appareil au sein d'un sous-réseau. Un sous-réseau ne peut pas avoir une adresse IP en double. Cela signifie que aucun appareil sur le réseau ne peut avoir la même adresse IP, car cela provoquerait un conflit IP. Si deux appareils ont la même adresse IP, le réseau confondra les appareils, et pour résoudre le conflit, l'un d'eux sera exclu du réseau.

### → Qu'est-ce qu'une adresse MAC ?

Adresse MAC (Media Access Control) – c'est une adresse matérielle ou physique d'un appareil. C'est un attribut unique composé de 12 caractères alphanumériques qui est assigné par le fabricant. Un exemple d'adresse MAC est : 00-B0-D0-63-C2-26.



Les adresses MAC sont statiques, contrairement aux adresses IP dynamiques, qui peuvent fluctuer. L'adresse MAC identifie les appareils auprès d'autres appareils sur le même réseau local. Tandis que l'adresse IP identifie la connexion de l'appareil sur le réseau de manière globale (sur Internet). Les adresses MAC ne peuvent pas être facilement trouvées par un tiers. Les adresses IP peuvent être trouvées par un tiers.

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

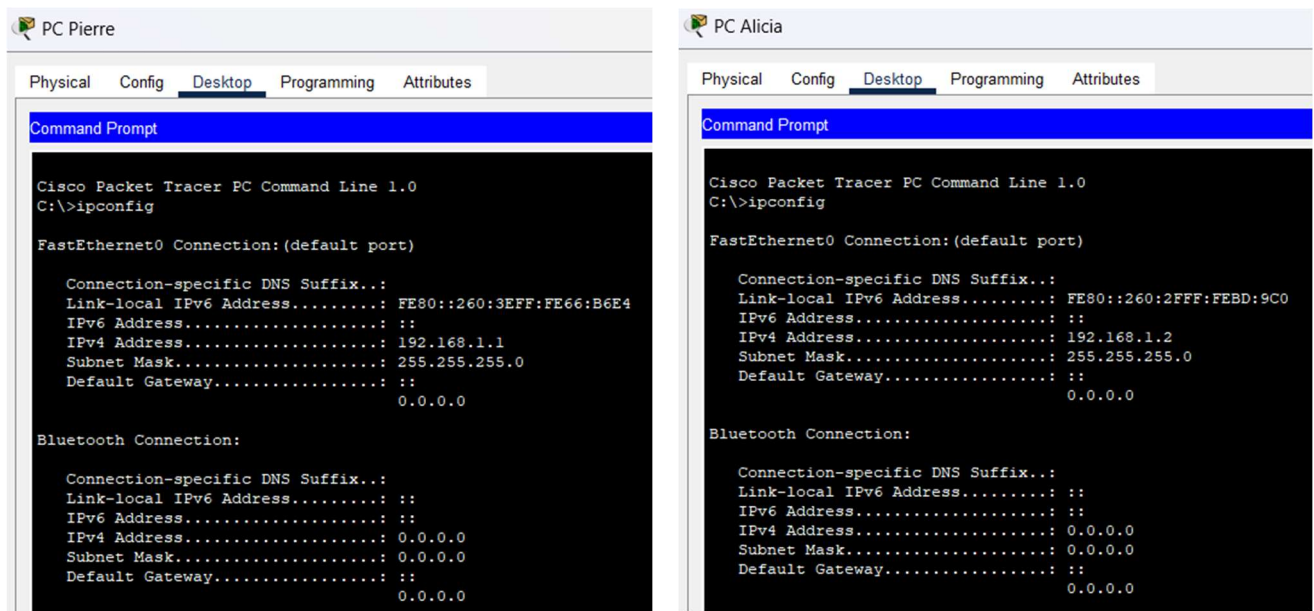
Les adresses IP publiques sont attribuées par les fournisseurs de services Internet (FSI) et sont utilisées pour communiquer avec d'autres appareils sur Internet. Les sites Web, les serveurs et les appareils qui doivent être accessibles depuis Internet ont des adresses IP publiques. Elles sont globalement uniques, ce qui signifie que deux appareils sur Internet ne peuvent pas avoir la même adresse IP publique en même temps. Les adresses IP publiques sont utilisées pour router le trafic à travers Internet, permettant la transmission de données entre différents réseaux et appareils dans le monde entier.

Une adresse IP privée est utilisée au sein d'un réseau privé, tel qu'un réseau local domestique ou professionnel (LAN). Ces adresses ne sont pas accessibles depuis Internet public. Les adresses IP privées sont généralement utilisées pour que les appareils au sein d'un réseau local communiquent entre eux. Elles ne sont pas globalement uniques et peuvent être réutilisées dans différents réseaux privés. Les plages d'adresses IP privées couramment utilisées incluent : IPv4 : 192.168.x.x, 172.16.x.x - 172.31.x.x et 10.x.x.x ; IPv6 : Adresses avec le préfixe fd ou fc. Les adresses IP privées sont souvent attribuées automatiquement par les routeurs ou configurées manuellement par les administrateurs réseau.

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

L'adresse réseau est toujours la première adresse du sous-réseau. Dans notre cas, avec un masque de sous-réseau de 255.255.255.0, cela signifie que les 8 premiers bits sont la partie hôte et les 24 bits restants sont la partie réseau. Avec 8 bits, on peut avoir 256 adresses au total. Cependant, 0 est également considéré comme une adresse, et c'est la première adresse dans le sous-réseau allant de 192.168.1.0 à 192.168.1.255. Par conséquent, l'adresse réseau de ce réseau est 192.168.1.0.

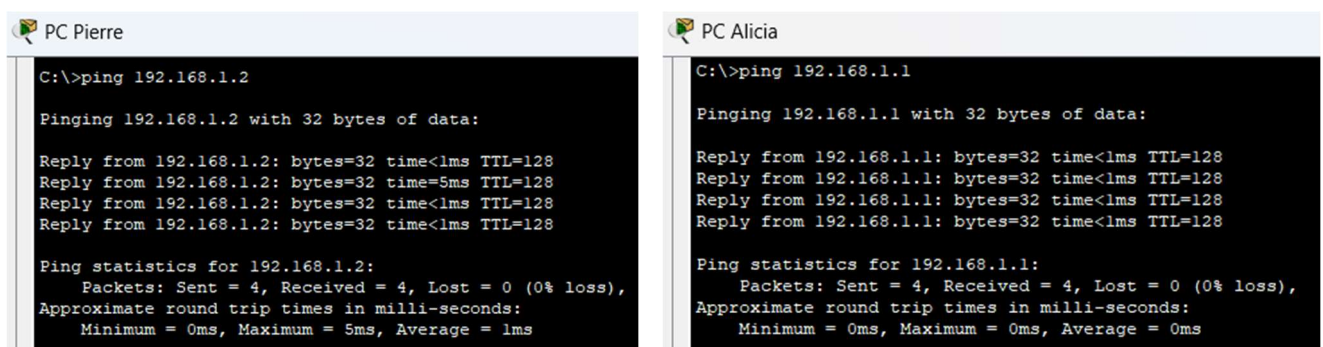
## 5 – ipconfig – Vérification des informations réseau sur PC



La commande "ipconfig" affiche les informations de base sur le réseau provenant des adaptateurs réseau de l'ordinateur. Dans notre cas, nous avons les connexions Fast Ethernet et Bluetooth. Dans les connexions Fast Ethernet, nous pouvons voir que l'adresse IP de l'ordinateur de Pierre est 192.168.1.1 avec un masque de sous-réseau de 255.255.255.0, et l'adresse IP de l'ordinateur d'Alicia est 192.168.1.2 avec le même masque de sous-réseau que celui de Pierre. IPv6 nécessite une adresse de lien local sur chaque interface réseau sur laquelle le protocole IPv6 est activé, mais nous pouvons constater que les adresses IPv6 ne sont pas définies (non activées) sur les deux ordinateurs. De plus, la passerelle par défaut 0.0.0.0 n'est pas spécifiée, ce qui signifie qu'il n'y a pas de routeur ou de périphérique permettant à ces ordinateurs de communiquer avec des dispositifs sur d'autres réseaux, tels qu'Internet. Aucune connexion Bluetooth n'est établie.

## 6 – ping – Vérification de la connexion entre les ordinateurs

Pour vérifier si les ordinateurs sont connectés localement, dans la même fenêtre de terminal, nous pouvons vérifier la connexion à l'aide de la commande 'ping' :



La commande 'ping <adresse IP de l'ordinateur cible>', par exemple 'ping 192.168.1.2', permet de vérifier la connectivité entre deux destinations.

La commande ping envoie des paquets de demande Echo du protocole de messages de contrôle Internet (ICMP) à l'ordinateur cible spécifié par son adresse IP.

Réponse. Si l'ordinateur cible est accessible et opérationnel, il devrait répondre à la source en renvoyant des paquets de réponse Echo ICMP.



Temps aller-retour (RTT). Ping mesure le temps nécessaire à chaque paquet pour aller vers l'ordinateur cible et revenir. Il calcule des statistiques telles que les temps aller-retour minimum, maximum et moyen. Ces informations peuvent être utilisées pour diagnostiquer des problèmes de latence réseau ou de perte de paquets.

Perte de paquets. En cas de congestion réseau ou de problème de connectivité, certains paquets peuvent être perdus. Ping signale le pourcentage de paquets perdus lors du test. Nous pouvons voir qu'aucun paquet n'a été perdu lors de la vérification de la connectivité entre les ordinateurs de Pierre et d'Alicia.

Résolution DNS. Lors de l'envoi de la commande ping, nous pouvons soit utiliser une adresse IP, soit un nom de domaine. Si nous fournissons le nom de domaine, ping trouvera d'abord l'adresse IP correspondante.

## 7 – ping – Test de la connexion avec un ordinateur éteint

Si nous éteignons l'ordinateur de Pierre et envoyons un ping depuis le terminal de l'ordinateur d'Alicia vers celui de Pierre, l'ordinateur de Pierre ne reçoit pas les paquets envoyés par Alicia. Veuillez consulter la capture d'écran du terminal de l'ordinateur d'Alicia :

```
PC Alicia
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

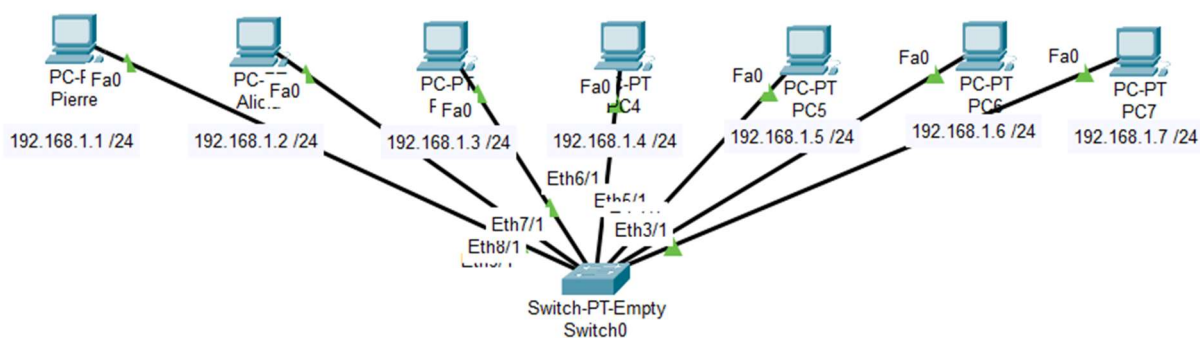
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Cela s'est produit parce que l'ordinateur de Pierre était éteint et déconnecté du réseau, ce qui signifie qu'il ne pouvait pas recevoir de paquets, tout comme l'ordinateur d'Alicia.


## 8 – expansion du réseau

Nous allons maintenant étendre le réseau avec 5 autres ordinateurs et configurer leurs adresses IP sur ce réseau. Comme il n'y a qu'un seul port Ethernet dans un PC, nous devons utiliser un concentrateur (hub) ou un commutateur (switch) qui dispose de plusieurs ports Ethernet et nous permet de connecter plusieurs appareils.



Dans cette configuration ci-dessus, le commutateur (switch) est utilisé.

Pour vérifier si tous les ordinateurs sont connectés, nous utiliserons la commande ping à l'aide de l'invite de commandes :




PC6

Physical
Config
Desktop
Programming
Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0  
C:\>ping 192.168.1.7  
  
Pinging 192.168.1.7 with 32 bytes of data:  
  
Reply from 192.168.1.7: bytes=32 time=2ms TTL=128  
Reply from 192.168.1.7: bytes=32 time=7ms TTL=128  
Reply from 192.168.1.7: bytes=32 time=6ms TTL=128  
Reply from 192.168.1.7: bytes=32 time=6ms TTL=128  
  
Ping statistics for 192.168.1.7:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 2ms, Maximum = 7ms, Average = 5ms  
  
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=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 = 0ms, Maximum = 4ms, Average = 1ms  
  
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=8ms 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 = 8ms, Average = 2ms



PC2

Physical
Config
Desktop
Programming
Attributes

Command Prompt

Reply from 192.168.1.3: bytes=32 time=6ms TTL=128  
Reply from 192.168.1.3: bytes=32 time=3ms TTL=128  
Reply from 192.168.1.3: bytes=32 time=5ms TTL=128  
Reply from 192.168.1.3: bytes=32 time=6ms TTL=128  
  
Ping statistics for 192.168.1.3:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 3ms, Maximum = 6ms, 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<1ms TTL=128  
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.4: bytes=32 time<1ms 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 = 0ms, Maximum = 0ms, Average = 0ms  
  
C:\>ping 192.168.1.5  
  
Pinging 192.168.1.5 with 32 bytes of data:  
  
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.5: bytes=32 time=5ms TTL=128  
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.1.5:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 5ms, Average = 1ms  
  
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<1ms TTL=128  
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128  
Reply from 192.168.1.6: bytes=32 time<1ms 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 = 0ms, Maximum = 0ms, Average = 0ms

## Hub vs Switch

Hub	Switch
<p>Un hub est un dispositif de réseau de couche physique qui est utilisé pour connecter plusieurs appareils dans un réseau. Un hub comporte de nombreux ports. Un ordinateur qui souhaite être connecté au réseau est branché sur l'un de ces ports. Lorsqu'une trame de données arrive au hub, il diffuse un message simple et rapide que tous les appareils du réseau peuvent entendre, mais ils n'ont pas nécessairement à faire quelque chose à moins que le message ne leur soit spécifiquement destiné. Un commutateur est un dispositif de réseau de couche liaison de données qui connecte des appareils dans un réseau. Comme un hub, un commutateur comporte également de nombreux ports. Cependant, lorsqu'une trame de données arrive à n'importe quel port d'un commutateur réseau, il examine l'adresse de destination et envoie la trame au(x) dispositif(s) correspondant(s). Ainsi, il prend en charge à la fois les communications unicast et multicast.</p>	<p>A switch is a <b>data link layer</b> networking device which connects devices in a network. Like a hub, a switch also has many ports. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both <b>unicast and multicast</b> communications.</p>



### Avantages et inconvénients des Hubs :

- + **Simplicité** - Les hubs peuvent **connecter** différents types de supports en même temps avec un hub central dans un espace physique, comme une seule pièce ou un petit bureau (LAN).
- + **Connectivité** - Les hubs utilisent un **analyseur de protocole réseau**, ce qui aide les appareils à comprendre les différents protocoles les uns des autres afin qu'ils puissent converser et partager des informations.
- + Le modèle de **diffusion** sur lequel les hubs fonctionnent affecte rarement le réseau, car il fonctionne de manière à ne pas surcharger le réseau et à ne pas créer beaucoup de travail supplémentaire pour les appareils.
- + **Coût** - Comparés aux commutateurs, les hubs sont vraiment **peu coûteux**, grâce à leur **simplicité**.
- Les hubs **peuvent créer un domaine de collision**. Cela se produit lorsque deux appareils essaient d'envoyer des données en même temps, et leurs signaux entrent en collision et se mélangent. Les hubs n'empêchent pas ces collisions ; ils les rendent en réalité plus susceptibles de se produire.
- Les hubs ne peuvent pas communiquer en mode full-duplex, ils ne **peuvent fonctionner qu'en mode half-duplex**. En mode half-duplex, un appareil peut soit envoyer des données, soit en recevoir à un moment donné, mais pas les deux simultanément. C'est similaire à une radio bidirectionnelle ; quand une personne parle, l'autre doit attendre qu'elle ait fini avant de répondre.
- Les hubs ne peuvent pas prendre en charge les grands réseaux et **contribuent à un niveau élevé de trafic** car ils diffusent les données à tous les appareils connectés sans les filtrer ou les réduire. Lorsque de nombreux appareils sont connectés à un hub, le réseau peut devenir congestionné en raison du volume élevé de données diffusées. Cela peut entraîner une inefficacité du réseau, une transmission de données plus lente et une probabilité accrue de collisions de données.
- Les hubs ne peuvent pas allouer de bande passante dédiée ou prioritaire à des appareils spécifiques. Lorsque des tâches gourmandes en données sont effectuées par certains appareils connectés au hub, ils consomment une grande partie de la bande passante partagée, ce qui peut ralentir le réseau pour les autres appareils. Cette inefficacité dans l'utilisation de la bande passante est ce que l'on appelle le gaspillage de bande passante (**Bandwidth Wastage**).

### Avantages et inconvénients des Commutateurs:

- + **Simplicité** - les commutateurs sont des dispositifs plug-and-play, permettant des connexions directes aux postes de travail sans configurations complexes.
- + Les commutateurs fonctionnent en **mode full-duplex** et augmentent la bande passante disponible du réseau en permettant une transmission de données plus rapide en permettant une transmission de données simultanée entre les appareils.
- + **Réduit la charge de travail** sur les ordinateurs hôtes individuels car ils envoient des données uniquement au dispositif spécifique qui en a besoin.
- + **Améliore les performances** du réseau en acheminant les données directement vers le destinataire prévu - les commutateurs réduisent la congestion et la latence du réseau.
- + **Réduit les collisions** - les commutateurs créent des canaux de communication isolés, appelés domaines de collision, pour chaque appareil connecté. Cela réduit les chances de collisions de données, ce qui permet une transmission de données plus fluide.
- + **Améliore la sécurité** - les commutateurs isolent le trafic de données, garantissant qu'il atteigne uniquement la destination prévue. Cette isolation renforce la sécurité du réseau en empêchant l'accès non autorisé aux données du réseau.
- **Coût** - les commutateurs ont tendance à être **plus chers** par rapport aux concentrateurs réseau ou à d'autres dispositifs plus simples en raison de leurs fonctionnalités et capacités avancées.
- **Dépannage difficile** des problèmes de connectivité réseau et nécessité de compétences et d'outils avancés.
- **Problèmes de diffusion** : Le trafic de diffusion peut poser problème dans les réseaux basés sur des commutateurs, car les paquets de diffusion inutiles peuvent consommer de la bande passante et entraîner une congestion du réseau.
- Lorsque les commutateurs ne sont pas configurés de manière sécurisée, ils **peuvent être vulnérables aux attaques de sécurité** telles que la falsification d'adresse IP ou la capture de trames Ethernet.

## Gestion du trafic réseau par les commutateurs - processus de commutation de paquets

Les commutateurs sont une technologie plus récente que les concentrateurs et sont plus intelligents dans la gestion du trafic réseau. Alors que les concentrateurs gèrent le trafic par diffusion et sont limités à la création d'un seul domaine de collision. Lorsqu'un concentrateur reçoit des données d'un appareil, il diffuse ces données à tous les autres appareils connectés au concentrateur. Par conséquent, tous les appareils connectés au concentrateur se trouvent dans le même domaine de collision. Contrairement aux concentrateurs, les commutateurs créent des domaines de collision séparés pour chacun de leurs ports. Cela signifie que chaque appareil connecté à un port de commutation se trouve dans son propre domaine de collision.

Les commutateurs gèrent le trafic réseau grâce à un processus différent appelé "commutation de paquets". La commutation de paquets, une technologie fondamentale en informatique et à la base de l'Internet moderne, a été développée en collaboration par divers chercheurs et organisations. Paul Baran et Leonard Kleinrock ont apporté des contributions précoces au concept, et la mise en œuvre réelle a impliqué les efforts d'organisations telles qu'ARPA dans la création de l'ARPANET, un précurseur de l'Internet d'aujourd'hui.

Lorsqu'un commutateur reçoit des données (sous forme de paquets) d'un appareil connecté à l'un de ses ports, il examine l'adresse MAC de destination des données.

Le commutateur maintient une table d'adresses MAC qui associe les adresses MAC au port spécifique sur lequel chaque appareil est connecté. Cette table aide le commutateur à identifier où acheminer les paquets.

Initialement, le commutateur peut ne pas connaître l'emplacement exact d'un appareil sur le réseau. Cependant, à mesure qu'il reçoit des paquets, il apprend les adresses MAC des appareils connectés à ses ports. Il enregistre ces associations dans sa table d'adresses MAC.

Lorsqu'un paquet arrive au commutateur avec une adresse MAC de destination, le commutateur consulte sa table d'adresses MAC pour déterminer le port associé à cette adresse. Il transmet ensuite le paquet uniquement au port où se trouve l'appareil de destination.

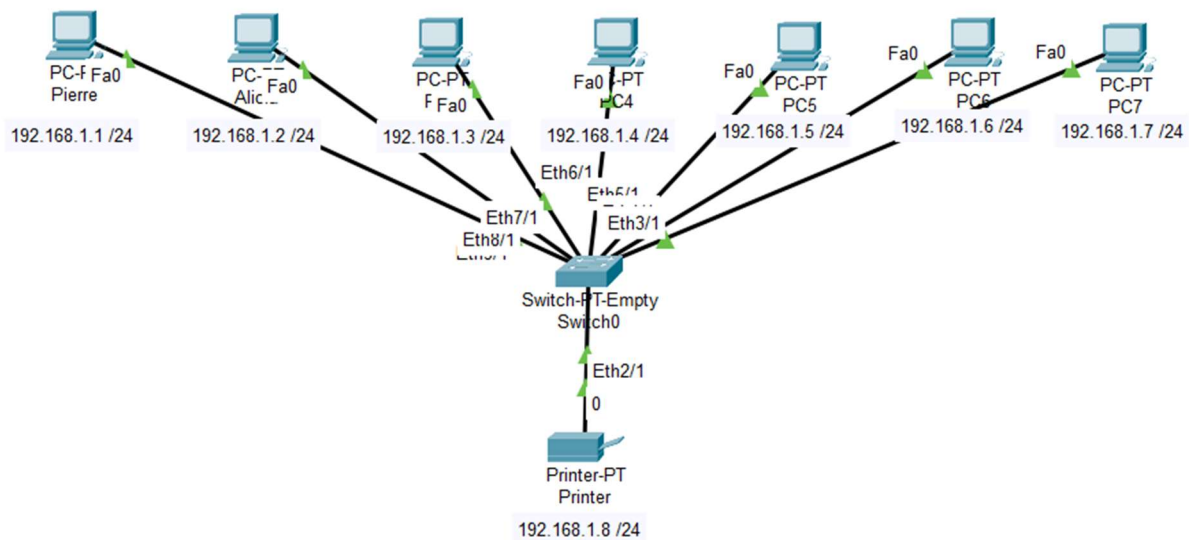
Les paquets de diffusion, destinés à tous les appareils du réseau, sont envoyés à tous les ports, sauf celui à partir duquel ils ont été émis.

En transmettant le trafic uniquement vers le port nécessaire, les commutateurs minimisent la transmission inutile de données, ce qui entraîne un transfert de données plus rapide et plus efficace au sein du réseau.

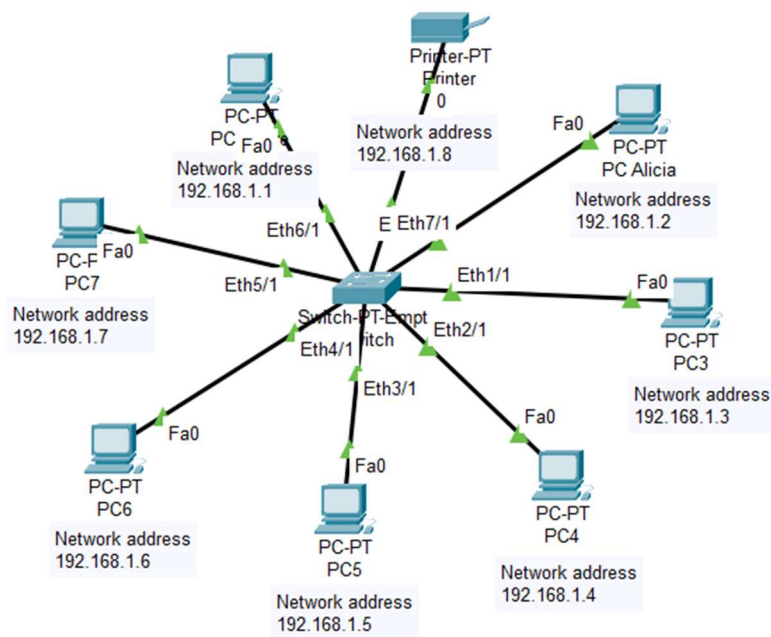
En résumé, les commutateurs utilisent les adresses MAC et une table d'adresses MAC pour acheminer intelligemment le trafic réseau, réduisant les collisions et optimisant le transfert de données pour les appareils connectés au réseau. Cette approche améliore les performances et l'efficacité du réseau par rapport aux technologies plus anciennes comme les concentrateurs.

## 9 – ajout d'une imprimante au réseau informatique

Maintenant, ajoutons une imprimante au réseau.



Nous pouvons choisir une topologie différente pour créer le réseau. Par exemple, voici le même réseau avec une topologie de type « Étoile » :

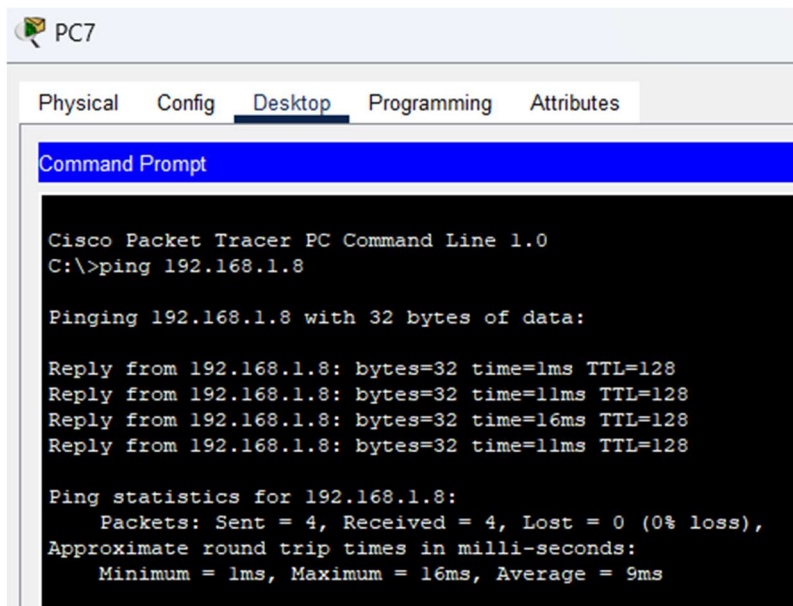


Les topologies réseau existent pour définir comment les appareils sont connectés physiquement ou logiquement au sein d'un réseau informatique. En choisissant la topologie la plus appropriée pour les besoins spécifiques d'un réseau, les organisations peuvent optimiser la communication, la scalabilité, la tolérance aux pannes, le partage des ressources, les performances et l'efficacité économique. Chaque topologie présente ses avantages et ses inconvénients, et le choix doit être en adéquation avec les objectifs et les exigences du réseau.

### Différents types de topologies réseau



Test la connexion avec l'imprimante depuis l'invite de commande de PC7 à l'aide de la commande ping :



```
PC7
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.8

Pinging 192.168.1.8 with 32 bytes of data:

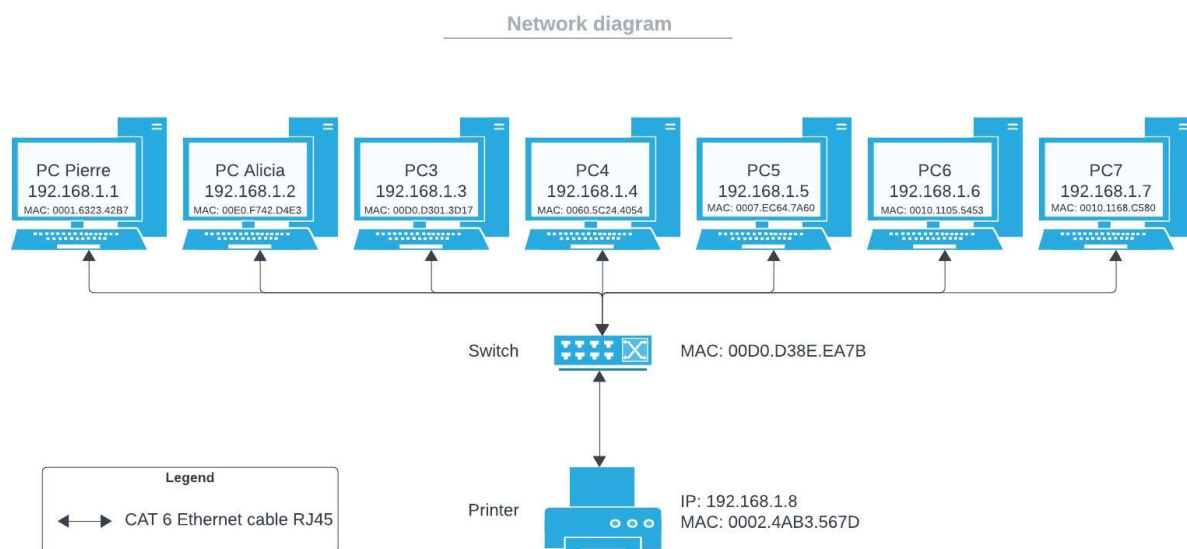
Reply from 192.168.1.8: bytes=32 time=1ms TTL=128
Reply from 192.168.1.8: bytes=32 time=11ms TTL=128
Reply from 192.168.1.8: bytes=32 time=16ms TTL=128
Reply from 192.168.1.8: bytes=32 time=11ms TTL=128

Ping statistics for 192.168.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 9ms
```

Pour une gestion efficace du réseau, la création et la maintenance d'un diagramme de réseau informatique sont cruciales :

- Il fournit de la clarté, ce qui facilite la compréhension de la manière dont les appareils sont connectés, tant pour les professionnels de l'informatique que pour les parties prenantes non techniques.
- Il simplifie et accélère le dépannage en identifiant où un problème peut se produire, qu'il s'agisse d'un câble défectueux, d'un appareil mal configuré ou d'un commutateur surchargé.
- Il améliore la sécurité en permettant aux administrateurs d'identifier les vulnérabilités potentielles en matière de sécurité et de mettre en place des contrôles d'accès et des pare-feux de manière stratégique.
- Il optimise l'allocation des ressources en montrant quels appareils sont connectés à chaque commutateur ou concentrateur, ce qui facilite l'allocation de la bande passante et garantit qu'aucun point unique ne devienne un goulot d'étranglement du réseau.
- Il facilite les efforts de reprise après sinistre en cas de panne ou de catastrophe, en aidant à une récupération rapide.

J'ai choisi une topologie en arbre pour un réseau simple et de petite échelle, avec une hiérarchie claire et un contrôle centralisé, et j'ai utilisé le logiciel "Lucid chart" (<https://lucid.app>) pour le réaliser.

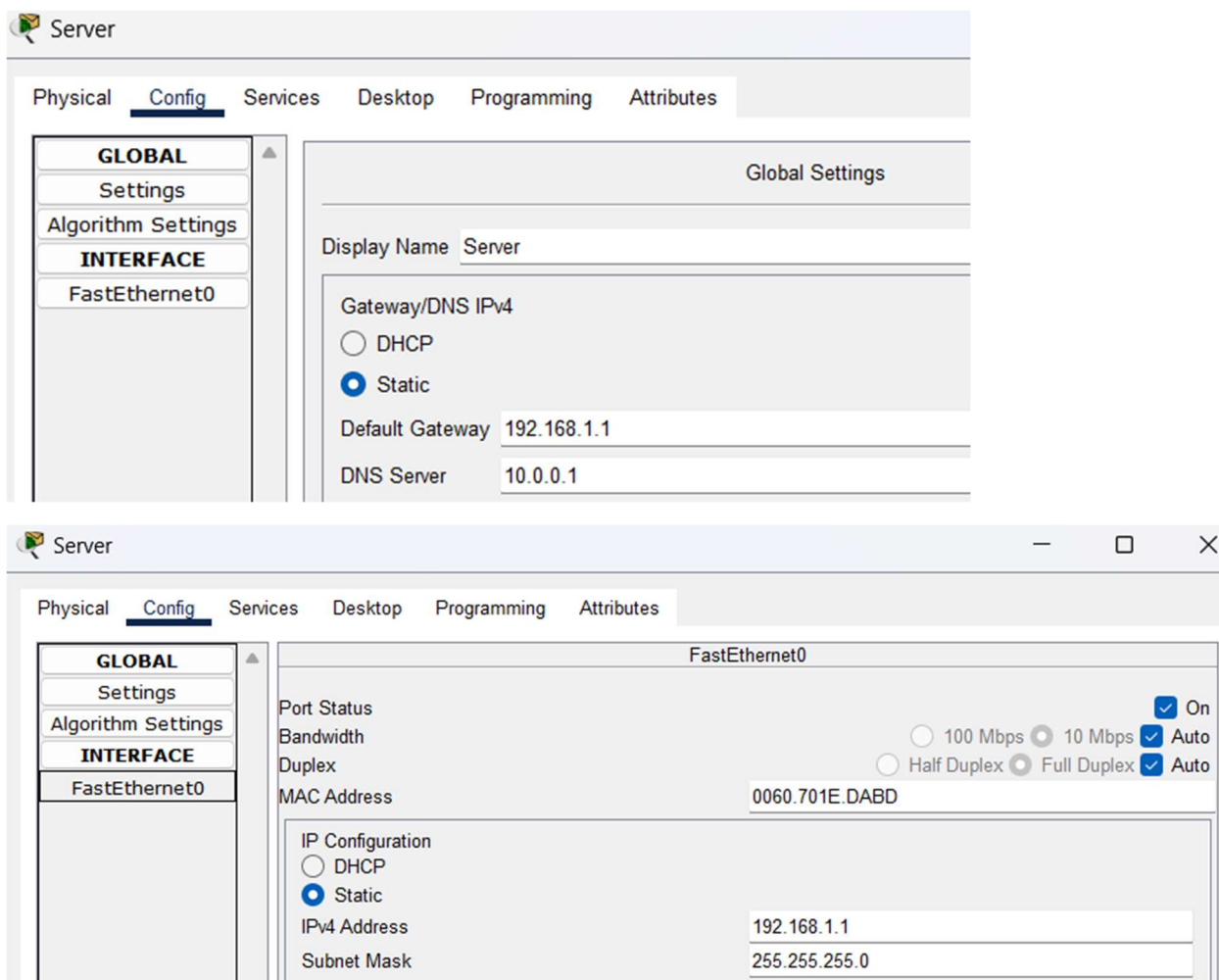


## 10 – configuration du serveur DHCP

La configuration du serveur DHCP offre l'avantage de l'attribution automatisée et centralisée des adresses IP au sein d'un réseau. Contrairement aux adresses IP statiques, qui sont configurées manuellement sur chaque appareil, le protocole **DHCP attribue dynamiquement des adresses IP aux appareils lors de leur connexion au réseau**.

L'attribution automatique des adresses IP à l'aide du protocole DHCP simplifie l'administration du réseau, réduit le risque d'erreurs de configuration et permet de gérer efficacement les ressources en adresses IP. Le DHCP est flexible, évolutif et idéal pour les réseaux de grande envergure ou dynamiques où les appareils se connectent fréquemment ou quittent le réseau. Il permet la prise en charge de la mobilité, la création de réseaux invités et la surveillance facile de l'utilisation des adresses IP. En revanche, les adresses IP statiques sont définies manuellement et restent fixes, ce qui peut entraîner une inefficacité, une complexité accrue de l'administration et une adaptabilité limitée dans les environnements dynamiques.

Pour configurer le serveur DHCP, nous devons d'abord ajouter le serveur à notre réseau informatique (à partir de la section [End Devices]) et le configurer avec une adresse IP statique. Nous attribuons la première adresse IP du sous-réseau (192.168.0.1) comme passerelle et adresse IPv4 du serveur. Nous laissons le masque de sous-réseau à 255.255.255.0.



Maintenant, nous devons activer le service DHCP et définir la passerelle par défaut (adresse IP statique du serveur DHCP) ainsi que le serveur DNS sur 10.0.0.1 (c'est souvent utilisé comme adresse IP de passerelle par défaut ou de routeur au sein de réseaux privés. Il n'est généralement pas utilisé comme adresse de serveur DNS (Domain Name System) sur l'internet public). L'adresse IP de départ est 192.168.1.0, ce qui correspond au début du sous-réseau, car le serveur sautera automatiquement les adresses IP occupées. Le masque de sous-réseau est de 255.255.255.0, ce qui donne un maximum de 254



utilisateurs. Cependant, nous laisserons l'adresse des imprimantes en statique, ce qui nous donnera un maximum de 253 utilisateurs. Nous devons enregistrer ces paramètres et activer le service DHCP.

The screenshot shows the 'Server' configuration window with the 'Services' tab selected. The 'DHCP' service is configured for the 'FastEthernet0' interface. The 'Service' is set to 'On'. The configuration includes a pool named 'serverPool' with a default gateway of 192.168.1.1, DNS server of 10.0.0.1, 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 253. The TFTP server and WLC address are both set to 0.0.0.0. A table at the bottom lists the configuration for the 'serverPool'.

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.1	10.0.0.1	192.168.1.0	255.255.255.0	253	0.0.0.0	0.0.0.0

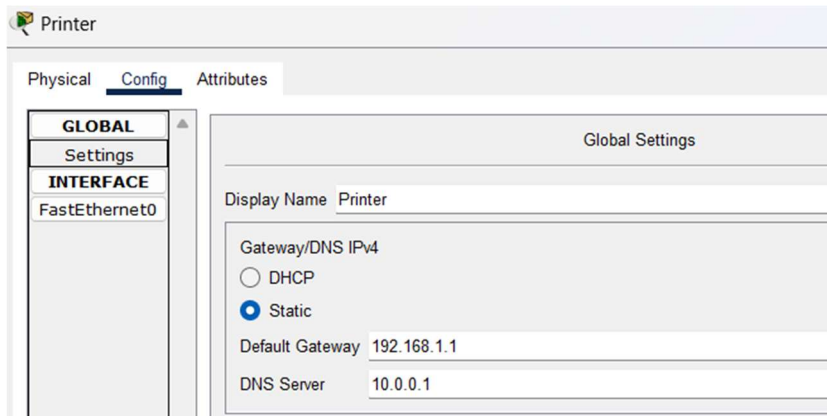
Dans la configuration IP du serveur, nous laissons l'adresse IP en statique.

The screenshot shows the 'Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is visible, showing the 'Static' radio button selected. The configuration includes an IPv4 address of 192.168.1.1, a subnet mask of 255.255.255.0, a default gateway of 192.168.1.1, and a DNS server of 10.0.0.1.

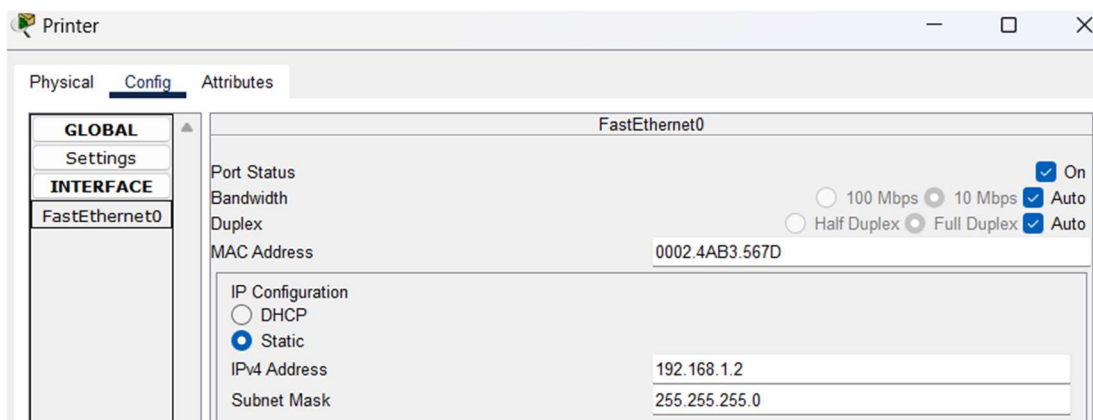
Maintenant, nous devons configurer l'adresse IP de tous les appareils actuels en DHCP. Lorsque l'adresse IP passe de statique à DHCP, le message « Demande DHCP réussie » apparaît dans l'application de configuration IP sur le bureau de chaque appareil.

The screenshot shows the 'PC7' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is visible, showing the 'DHCP' radio button selected. The configuration includes an interface of 'FastEthernet0', an IPv4 address of 192.168.0.3, a subnet mask of 255.255.255.0, a default gateway of 192.168.0.1, and a DNS server of 10.0.0.1. A message 'DHCP request successful.' is displayed.

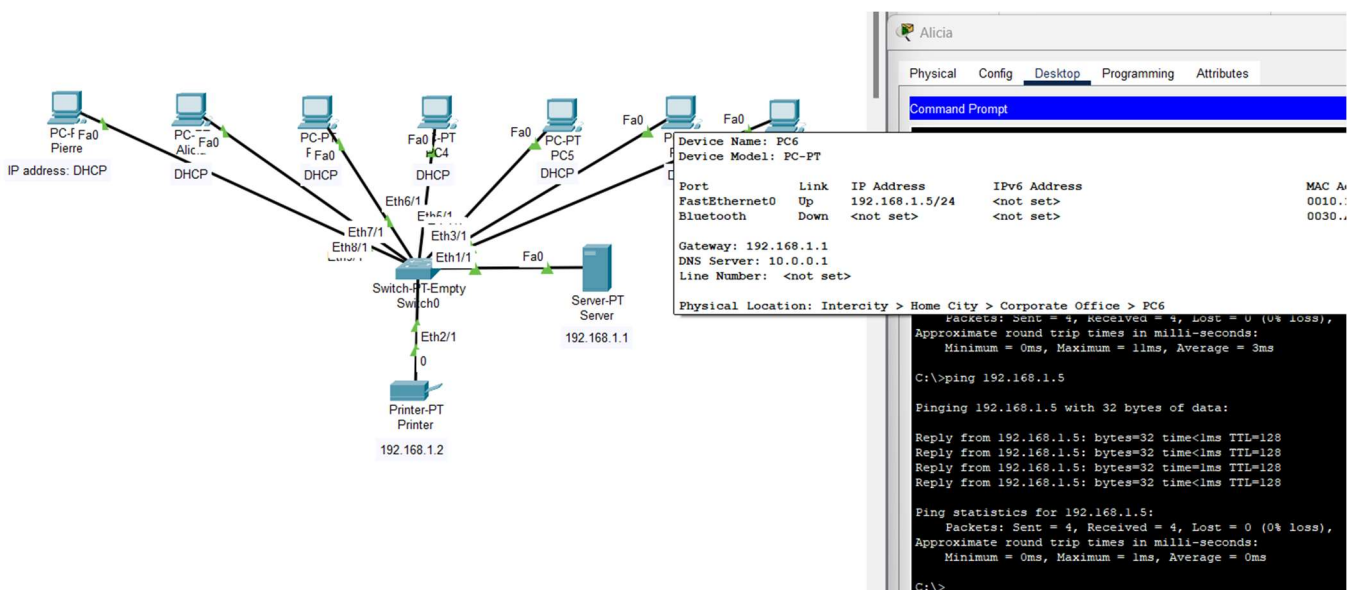
Pour définir l'adresse IP de l'imprimante en statique, nous devons définir la passerelle par défaut et le serveur DNS sur les mêmes valeurs que dans le routeur :



Ensuite, nous définissons l'adresse IPv4 sur 192.168.1.2 et la même masque de sous-réseau que celle définie dans le serveur DHCP.



Nous pouvons survoler la souris sur n'importe quel ordinateur pour voir son adresse IP et essayer de le pinguer depuis d'autres appareils. Le test montre un échange de paquets réussi :



## 11 – l'adressage réseau

On était attribué une adresse réseau de classe A 10.0.0.0. On doit créer 21 sous-réseaux. Il doit prendre en charge :

- 1 sous-réseau de 12 hôtes
- 5 sous-réseaux de 30 hôtes
- 5 sous-réseaux de 120 hôtes
- 5 sous-réseaux de 160 hôtes

Voilà le plan d'adressage défini :

Subnet	Gateway	Usable addresses	Broadcast	Subnet mask
12 hosts subnet	10.0.0.1	10.0.0.2-10.0.0.14	10.0.0.15	255.255.255.240
30 hosts subnet 1	10.0.0.16	10.0.0.17-10.0.0.46	10.0.0.47	255.255.255.224
30 hosts subnet 2	10.0.0.48	10.0.0.49-10.0.0.78	10.0.0.79	255.255.255.224
30 hosts subnet 3	10.0.0.80	10.0.0.81-10.0.0.110	10.0.0.111	255.255.255.224
30 hosts subnet 4	10.0.0.112	10.0.0.113-10.0.0.142	10.0.0.143	255.255.255.224
30 hosts subnet 5	10.0.0.144	10.0.0.145-10.0.0.174	10.0.0.175	255.255.255.224
120 hosts subnet 1	10.0.0.176	10.0.0.177-10.0.1.46	10.0.1.47	255.255.255.128
120 hosts subnet 2	10.0.1.48	10.0.1.49-10.0.1.174	10.0.1.175	255.255.255.128
120 hosts subnet 3	10.0.1.176	10.0.1.177-10.0.2.46	10.0.2.47	255.255.255.128
120 hosts subnet 4	10.0.2.48	10.0.2.49-10.0.2.174	10.0.2.175	255.255.255.128
120 hosts subnet 5	10.0.2.176	10.0.2.177-10.0.3.46	10.0.3.47	255.255.255.128
160 hosts subnet 1	10.0.3.48	10.0.3.47-10.0.4.46	10.0.4.47	255.255.255.0
160 hosts subnet 2	10.0.4.48	10.0.4.47-10.0.5.46	10.0.5.47	255.255.255.0
160 hosts subnet 3	10.0.5.48	10.0.5.47-10.0.6.46	10.0.6.47	255.255.255.0
160 hosts subnet 4	10.0.6.48	10.0.6.47-10.0.7.46	10.0.7.47	255.255.255.0
160 hosts subnet 5	10.0.7.48	10.0.7.47-10.0.8.46	10.0.8.47	255.255.255.0

Voici les calculs :

For 12 hosts:									
256	128	64	32	16	8	4		2 bits = addresses	
255	127	63	31	15	7	3		1 for calculation (or use formula: $256 - 2^{\text{bits of host portion}}$ )	
1	1	1	1	0	0	0	0	32 bits	$8 * 4$ 4 octets
network portion				host portion					
12 hosts + 2 reserved = 16 addresses									
$2^4 = 16$									
$256 - 16 = 240$									

For 30 hosts:									
256	128	64	32	16	8	4		2 bits = addresses	
255	127	63	31	15	7	3		1 for calculation	
1	1	1	0	0	0	0	0	0	
$2^5 - 1 = 31$									
$255 - 31 = 224$									

For 120 hosts:									
254	<b>128</b>	64	32	16	8	4	2 bits = addresses		
255	127	63	31	15	7	3	1 for calculation		
1	0	0	0	0	0	0	0		
net		host portion							
$255 - 127 = 128$									

For 160 hosts:								
256	128	64	32	16	8	4	2 bits = addresses	
255	127	63	31	15	7	3	1 for calculation	
0	0	0	0	0	0	0	0	
address		addresses					mask:	
10.0.3.	48	start					255	- 255 = 0
	255	end	208					
	0	start	209					
10.0.4.	47	end	256					

### Différentes classes de réseau

Classe	Description	Adresse réseau	Masque sous- réseau	Nombre maximal d'adresses
A	Ces réseaux ont un très grand nombre d'hôtes mais un petit nombre d'adresses réseau. Le premier octet représente la partie réseau, et les trois octets restants sont réservés aux adresses des hôtes.	10.0.0.0	255.0.0.0	16'777'214
B	Les réseaux de classe B ont un nombre modéré de réseaux et d'hôtes. Les deux premiers octets sont réservés aux adresses réseau, et les deux octets suivants sont réservés aux adresses des hôtes	172.16.0.0	255.255.0.0	65'534
C	Les réseaux de classe C ont un grand nombre de réseaux mais un petit nombre d'hôtes par réseau. Les trois premiers octets sont réservés aux adresses réseau, et seul le dernier octet est réservé aux adresses des hôtes.	192.168.0.0	255.255.255.0	254

Il existe également des adresses de réseaux de classe D et de classe E réservées aux groupes de multidiffusion et qui ne sont pas utilisées pour la communication classique de machine à machine. Les adresses de réseaux de classe D sont réservées à des fins expérimentales et ne sont pas utilisées pour les réseaux standard.

## 12 – Modèle OSI (Open Systems Interconnection)

Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel utilisé pour comprendre et normaliser la manière dont différents protocoles et technologies de réseau interagissent au sein d'un système en réseau. Il définit une série de sept couches, chacune ayant des fonctions et des responsabilités spécifiques. Ces couches fournissent collectivement des lignes directrices pour la conception et la mise en œuvre de la communication en réseau :

Couche	Description des rôles	Exemples de dispositifs ou protocoles
1 – couche physique	La couche physique traite de la transmission physique réelle de bits de données sur un support de réseau, tel que des câbles, des fils ou des signaux sans fil. Elle spécifie des caractéristiques telles que les niveaux de tension, les types de câbles et les méthodes de codage des signaux.	cable RJ45, fibre optique, Wi-Fi
2 – couche liaison de données	La couche liaison de données est responsable de la création d'une liaison fiable entre deux nœuds directement connectés sur un réseau. Elle comprend des tâches telles que le cadrage, l'adressage, et la détection et correction d'erreurs.	Cable RJ45, fibre optique, Wi-Fi, MAC, Ethernet
3 – couche réseau	La couche réseau se concentre sur l'acheminement des paquets de données entre différents réseaux et sous-réseaux. Elle attribue des adresses logiques (par exemple, des adresses IP) aux dispositifs et détermine le meilleur chemin pour que les données atteignent leur destination.	IPv4, IPv6, Router
4 – couche transport	La couche transport gère la communication de bout en bout entre les dispositifs à travers un réseau. Elle garantit la fiabilité des données, le contrôle du flux et la correction des erreurs.	TCP (Transmission Control Protocol), UDP (User Datagram Protocol)
5 – couche session	La couche session est responsable de l'établissement, de la maintenance et de la terminaison des sessions de communication entre deux dispositifs. Elle gère le contrôle du dialogue et la synchronisation entre les applications.	PPTP (Point-to-Point Tunneling Protocol)
6 – couche présentation	La couche présentation traite de la traduction des données, de la cryptage et de la compression pour garantir que les données envoyées par une application peuvent être comprises par une autre, même si elles utilisent des formats de données différents. Elle gère également le cryptage et le décryptage des données.	SSL/TLS (Secure Sockets Layer/Transport Layer Security)
7 – couche application	La couche application représente l'interface entre les applications de l'utilisateur et les couches inférieures du modèle OSI. Elle comprend divers protocoles d'application pour des services tels que les e-mails (SMTP, POP3), la navigation web (HTTP) et le transfert de fichiers (FTP).	FTP (File Transfer Protocol), HTML (Hypertext Markup Language)

Le modèle OSI est un cadre de référence qui aide les ingénieurs réseau et les développeurs à comprendre les protocoles réseau et à résoudre les problèmes de réseau. Bien qu'il s'agisse d'un outil conceptuel utile, les protocoles et technologies réseau du monde réel brouillent souvent les limites entre ces couches, et de nombreux modèles et protocoles de mise en réseau ne correspondent pas parfaitement au modèle OSI. Cependant, il reste un outil éducatif et de référence précieux pour comprendre la communication en réseau.



## 13 – comprendre l'architecture du réseau

Nous avons un réseau informatique composé de quatre ordinateurs et de deux serveurs avec les adresses IP suivantes et un masque de sous-réseau de 255.255.255.0 :

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

L'architecture réseau fait référence à la disposition structurelle et logique d'un réseau. Elle décrit comment les dispositifs réseau sont connectés et les règles qui régissent le transfert de données entre eux.

Il existe de nombreuses façons d'aborder la conception de l'architecture réseau, qui dépendent de l'objectif et de la taille du réseau. Par exemple, les réseaux étendus (WAN) désignent un groupe de réseaux interconnectés, souvent sur de longues distances. L'architecture de son réseau sera très différente de celle d'un réseau local (LAN) dans une succursale de bureau plus petite.

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

Sous-réseau : Tous les appareils, y compris les PC et les serveurs, ont des adresses IP dans la plage 192.168.10.x. Cela suggère qu'ils font probablement partie du même sous-réseau ou VLAN.

Adressage : L'utilisation d'adresses IP privées (192.168.x.x) indique que ce réseau est probablement un intranet ou un réseau local plutôt que directement connecté à Internet.

Topologie : À partir des informations fournies uniquement, il est difficile de déterminer la topologie réseau physique ou logique (par exemple, étoile, bus, anneau) ou comment les dispositifs sont interconnectés.

Rôles : Les PC sont généralement utilisés par les utilisateurs finaux, tandis que les serveurs peuvent avoir diverses fonctions, telles que le stockage de fichiers, l'hébergement d'applications ou la gestion de bases de données. Cependant, les rôles spécifiques des serveurs ne sont pas mentionnés.

Taille : Le réseau semble relativement petit, composé de quatre PC et de deux serveurs. Cela suggère un réseau local de petite taille (LAN) plutôt qu'un réseau d'entreprise plus important.

### → Quelle est l'adresse IP du réseau ?

192.168.10.0, parce que la masque nous montre que le réseaux peut avoir jusqu'à 256 adresses IP, alors le début de l'adresse IP du réseau est ce qui nous voyons comme constant '192.168.10' et le dernier octet est 0 du part de réseau, parce que le partie de host est 8 bits que peut nous donner 256 adresses (de 0 jusqu'à 255).

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

On peut brancher 254 machines en total sur ce réseau, parce que le premier et le dernier adresses sont réservés pour Gateway et Broadcast.

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

192.168.10.255 – L'adresse de diffusion est toujours la dernière adresse du sous-réseau.

### Different network types

Type de réseau	Nom	Zone de couverture	Usage et utilité	Nombre d'appareils pris en charge	Exemples
PAN	Personal Area Network – réseau personnel	Très courte portée (jusqu'à 10 mètres) Typiquement quelques appareils	Connecter des appareils à usage personnel, par exemple, Bluetooth	Typically a few devices	Appareils connectés en Bluetooth, écouteurs sans fil
LAN	Local Area Network – réseau local	Petite zone géographique (par exemple, un bâtiment ou un campus)	Partage de données locales, partage de fichiers et accès aux ressources	Des centaines à des milliers	Réseaux de bureau, réseaux domestiques
MAN	Metropolitan Area Network – réseau métropolitain	Ville ou zone métropolitaine	Connecter plusieurs LAN dans une ville	De milliers à dizaines de milliers	Réseaux Wi-Fi municipaux, campus universitaires
WAN	Wide Area Network – réseau étendu	Zone géographique étendue (à travers des villes, des pays)	Long-distance Communication de données à longue distance, accès à Internet communication, Internet access	De milliers à des millions	Internet, réseaux d'entreprise mondiaux

Il existe de nombreux types de réseaux différents comme :

- PAN (Personal Area Network) : Réseau personnel.
- LAN (Local Area Network) : Réseau local.
- MAN (Metropolitan Area Network) : Réseau métropolitain.
- WAN (Wide Area Network) : Réseau étendu.
- SAN (Storage Area Network) : Réseau de stockage.
- CAN (Campus Area Network) : Réseau de campus.
- VLAN (Virtual Local Area Network) : Réseau local virtuel.
- VPN (Virtual Private Network) : Réseau privé virtuel.
- VoIP (Voice over Internet Protocol) : Voix sur IP.
- Internet : Le réseau mondial d'ordinateurs interconnectés.
- Intranet : Réseau privé interne à une organisation.
- Extranet : Extension sécurisée d'un réseau intranet pour inclure des partenaires commerciaux.
- Cloud Network (Réseau Cloud) : Réseau de serveurs et de services basés sur le cloud.
- Wireless Network : Réseau qui utilise des technologies sans fil telles que le Wi-Fi.

Ces types de réseaux varient en taille, en portée et en fonctionnalités, et sont utilisés pour différentes applications et besoins de communication.

## 14 – conversion des adresses IP en valeurs binaires

Adresse IP	Binaire
145.32.59.24	10010001.00100000.00111011.00011000
200.42.129.16	11001000.00101010.10000001.00010000
14.82.19.54	00001110.01010010.00010011.00110110

Les adresses IP IPv4 utilisent 4 octets divisés par des points. Un octet est composé de 8 bits. Une valeur de bit peut être 0 ou 1. 8 bits peuvent atteindre la valeur de 255 en ajoutant les puissances de deux en commençant par la puissance 0 :

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64, 2^7 = 128;$$

$$1 + 2 + 4 + 8 + 16 + 32 + 64 + 128 = 255.$$

Donc, une valeur décimale peut être convertie en binaire en trouvant la combinaison de bits qui utilise huit puissances de deux, nous devrions écrire ces nombres de droite à gauche : 128 64 32 16 8 4 2 1.

Pour trouver la valeur binaire d'un nombre jusqu'à 255 en une séquence de 8 bits, nous devons trouver les nombres correspondants qui s'additionnent pour obtenir le résultat souhaité.

Par exemple, 145 peut être obtenu en additionnant 128, 16 et 1. Cela donne la valeur binaire de 145 comme 10010001 :

128	64	32	16	8	4	2	1
1	0	0	1	0	0	0	1

$$128 + 16 + 1 = 145$$

La valeur binaire 10010001 signifie que 128 est oui, 64 et 32 sont non ; 16 est oui, 8, 4, 2 sont non, et 1 est oui.

## 15 – routing, gateway, VPN, DNS

### → Qu'est ce que le routage ?

Le routage est un concept fondamental dans les réseaux informatiques. Il fait référence au processus de détermination du meilleur chemin pour que les paquets de données voyagent de la source vers la destination à travers un réseau. Le routage est une fonction cruciale dans le fonctionnement d'Internet et de la plupart des autres réseaux informatiques. Voici comment fonctionne le routage :

1. Transfert de paquets : Dans un réseau, les données sont divisées en unités plus petites appelées paquets. Lorsqu'un appareil souhaite envoyer des données à un autre appareil sur le réseau, il divise les données en paquets et attache une adresse de destination à chaque paquet.
2. Table de routage : Les routeurs sont des dispositifs réseau spécialement conçus pour le routage. Chaque routeur maintient une table de routage, qui est une liste des routes connues vers diverses destinations sur le réseau. Cette table contient des informations sur la façon d'atteindre différents réseaux ou sous-réseaux.
3. Adresse de destination : Lorsqu'un routeur reçoit un paquet, il examine l'adresse de destination sur le paquet. Le routeur consulte sa table de routage pour déterminer le meilleur chemin pour faire avancer le paquet vers sa destination.
4. Prochain saut : La table de routage fournit des informations sur le prochain routeur ou saut vers lequel le paquet devrait être envoyé afin de se rapprocher de la destination. Le routeur fait ensuite avancer le paquet vers le prochain saut en fonction de ces informations.
5. De saut en saut : Ce processus est répété à chaque routeur le long du chemin jusqu'à ce que le paquet atteigne sa destination finale. Chaque routeur prend une décision indépendante sur l'endroit où envoyer le paquet ensuite en se basant sur sa table de routage.
6. Routage dynamique : Dans le routage dynamique, les routeurs échangent des informations de routage avec les routeurs voisins, ce qui leur permet de mettre automatiquement à jour leurs tables de routage en fonction des modifications du réseau. Des protocoles de routage populaires comme OSPF (Open Shortest Path First) et BGP (Border Gateway Protocol) permettent le routage dynamique.
7. Routage statique : Alternativement, les administrateurs réseau peuvent configurer manuellement des routes statiques dans les routeurs, en spécifiant le chemin exact qu'un paquet devrait emprunter pour atteindre une destination. Les routes statiques ne changent pas sauf si elles sont reconfigurées par un administrateur.

### → Qu'est ce qu'un gateway ?

Une passerelle est un composant essentiel en informatique réseau, servant de pont ou de point d'entrée entre deux réseaux différents, souvent avec des protocoles ou des méthodes de communication distincts. On peut la considérer comme un interprète numérique ou un médiateur qui permet la communication entre des réseaux qui pourraient autrement avoir du mal à se comprendre mutuellement. Voici une explication détaillée :

- Traducteur de Réseau : Fondamentalement, une passerelle est un traducteur de réseau. Elle comprend les règles, les langages et les protocoles d'un réseau et traduit les données de ce réseau dans un format compréhensible pour un autre réseau. Cela est particulièrement essentiel lorsque les réseaux utilisent des normes de communication différentes.
- Liaison entre les Réseaux Différents : Les passerelles sont couramment utilisées pour connecter des réseaux locaux (comme les LAN ou les PAN) à des réseaux externes, y compris Internet ou des réseaux étendus privés (WAN). Elles servent de porte par laquelle les données du réseau local peuvent passer de et vers le réseau externe.
- Conversion de Protocole : Les réseaux reposent souvent sur différents protocoles ou langages de communication. Par exemple, votre réseau domestique peut utiliser Ethernet, tandis qu'Internet

utilise un protocole appelé TCP/IP. Une passerelle peut traduire les paquets de données entre ces protocoles, assurant une communication transparente.

- **Sécurité et Pare-feu** : Les passerelles intègrent souvent des fonctionnalités de sécurité telles que des pare-feux et des serveurs proxy. Cela renforce la sécurité du réseau local en filtrant les données entrantes et sortantes, en bloquant le trafic malveillant et en protégeant les informations sensibles.
- **Passerelle Internet** : Dans un réseau domestique ou de petite entreprise, votre routeur agit souvent comme une passerelle Internet. Il connecte vos appareils locaux à Internet, en traduisant entre les adresses IP locales de vos appareils et les adresses IP publiques utilisées sur Internet.
- **Passerelle de Messagerie** : Dans les systèmes de messagerie électronique, une passerelle peut être responsable de la transmission des courriers électroniques entre différents services de messagerie ou domaines. Elle joue un rôle dans la garantie que les courriers électroniques sont livrés correctement, même si l'expéditeur et le destinataire utilisent différentes plateformes de messagerie.
- **Passerelle IoT** : Avec l'avènement de l'Internet des objets (IoT), les passerelles sont devenues cruciales pour connecter les dispositifs IoT à Internet et aux services cloud. Elles collectent des données à partir de divers capteurs IoT et les envoient vers le cloud pour analyse.
- **Passerelles Vocales** : Dans les télécommunications, les passerelles vocales convertissent les appels vocaux à partir de lignes téléphoniques traditionnelles (analogiques) en paquets de données (numériques) adaptés à la transmission sur des réseaux IP.

En résumé, une passerelle est comme un interprète numérique et un facilitateur, permettant à différents réseaux de communiquer efficacement, de garantir que les données sont correctement formatées et d'améliorer la sécurité en cours de route. C'est une partie vitale des réseaux modernes, rendant possible le monde interconnecté sur lequel nous comptons aujourd'hui.

### → Qu'est ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel, est une technologie qui fournit une connexion sécurisée et chiffrée sur Internet. Il permet aux utilisateurs d'accéder à un réseau privé, comme un réseau d'entreprise ou un réseau domestique, comme s'ils y étaient directement connectés. Voici comment fonctionne un VPN :

- **Chiffrement** : La fonction principale d'un VPN est le chiffrement. Lorsque vous vous connectez à un serveur VPN, toutes les données transmises entre votre appareil et le serveur sont chiffrées. Cela signifie que même si quelqu'un intercepte les données, il ne pourra pas les déchiffrer sans la clé de chiffrement.
- **Tunnelisation** : Les VPN utilisent une technologie appelée "tunnelisation" pour créer une connexion sécurisée et privée entre votre appareil et le serveur VPN. Cette connexion est souvent appelée "tunnel VPN". Toutes les données envoyées et reçues via ce tunnel sont protégées.
- **Serveur VPN** : Pour utiliser un VPN, vous avez besoin d'accéder à un serveur VPN. Ce serveur fait office d'intermédiaire entre votre appareil et Internet. Lorsque vous vous connectez au serveur VPN, le trafic Internet est acheminé via ce serveur avant d'atteindre sa destination finale.
- **Masquage de l'Adresse IP** : Lorsque vous vous connectez à un serveur VPN, votre véritable adresse IP est masquée, et vous obtenez une adresse IP de l'emplacement du serveur. Cela contribue à anonymiser vos activités en ligne et offre une couche supplémentaire de confidentialité.

Utilisations et avantages des VPN :

- **Sécurité** : Les VPN sont principalement utilisés pour renforcer la sécurité en ligne. Ils protègent vos données contre l'écoute indiscrete, les piratages et autres menaces cybernétiques lorsque vous utilisez des réseaux Wi-Fi publics ou des connexions Internet non fiables.
- **Vie privée** : Les VPN contribuent à protéger votre vie privée en masquant votre adresse IP. Cela rend plus difficile pour les sites web et les services en ligne de suivre votre emplacement et vos activités en ligne.



- Contournement des restrictions géographiques : Les VPN peuvent être utilisés pour accéder à du contenu qui est géo-restreint ou bloqué dans votre région. En vous connectant à un serveur dans un pays différent, vous pouvez accéder à des sites web et des services de streaming comme si vous étiez dans ce pays.
- Accès à distance : Les entreprises utilisent souvent des VPN pour fournir un accès distant sécurisé aux employés. Cela permet aux employés d'accéder aux ressources et aux systèmes de l'entreprise depuis l'extérieur du bureau en toute sécurité.
- Torrenting et partage P2P : Certains utilisateurs utilisent des VPN pour le torrenting et le partage de fichiers en pair-à-pair (P2P). Les VPN offrent anonymat et sécurité lors du téléchargement de fichiers via ces méthodes.
- Contournement de la censure : Dans les pays où il existe une stricte censure d'Internet, les VPN peuvent être utilisés pour contourner les restrictions imposées par le gouvernement et accéder à des sites web et des services bloqués.
- Jeux en ligne : Les joueurs peuvent utiliser des VPN pour réduire la latence, se protéger contre les attaques par déni de service distribué (DDoS) et accéder à des serveurs de jeux restreints par région.

Types de VPN :

- VPN d'accès distant : Utilisé par des individus ou des employés pour se connecter en toute sécurité à un réseau d'entreprise depuis un emplacement distant.
- VPN de site à site : Utilisé pour connecter de manière sécurisée plusieurs succursales du réseau d'une entreprise via Internet.
- VPN client-à-site : Similaire aux VPN d'accès distant, mais utilisé par des clients ou des individus pour se connecter à un réseau spécifique.
- VPN pair-à-pair : Permet à des individus de créer une connexion directe et sécurisée les uns avec les autres via Internet.

En résumé, un VPN est un outil puissant qui offre des avantages en termes de sécurité, de confidentialité et d'accessibilité pour les utilisateurs et les organisations. Il y parvient en cryptant les données, en masquant les adresses IP et en créant des tunnels sécurisés pour la transmission des données, ce qui en fait une technologie essentielle dans le monde numérique d'aujourd'hui.

## → Qu'est ce qu'un DNS ?

Le DNS, qui signifie Domain Name System, est une technologie fondamentale qui joue un rôle crucial dans le fonctionnement d'Internet. Il agit comme l'annuaire d'Internet, traduisant les noms de domaine conviviaux pour les humains en adresses IP lisibles par les machines. Voici une explication détaillée de ce qu'est le DNS et de son fonctionnement :

Le DNS est un système de nomenclature distribué utilisé pour faire correspondre les noms de domaine (comme `www.example.com`) à leurs adresses IP correspondantes (comme `192.0.2.1`).

Hiérarchie du DNS : Le DNS fonctionne selon une structure hiérarchique. En haut de la hiérarchie se trouvent les serveurs DNS racine, qui contiennent des informations sur les domaines de premier niveau (TLD) comme `.com`, `.org`, `.net`, ainsi que sur les TLD de codes pays (par exemple, `.uk`, `.de`).

Enregistrement de noms de domaine : Lorsqu'un site Web est créé, son nom de domaine doit être enregistré auprès d'un registraire de domaines. Le registraire conserve un enregistrement du nom de domaine et de son adresse IP associée.

Résolveur DNS : Votre ordinateur ou appareil est équipé d'un résolveur DNS, qui est essentiellement un petit programme qui traduit les noms de domaine en adresses IP. Lorsque vous saisissez une adresse Web dans votre navigateur, le résolveur est responsable de la gestion de la traduction.

**Cache DNS local :** Pour accélérer le processus, la plupart des appareils conservent un cache DNS local. Ce cache stocke les noms de domaine récemment résolus et leurs adresses IP correspondantes, réduisant ainsi la nécessité de interroger à plusieurs reprises les serveurs DNS pour les mêmes informations.

**Interrogation DNS :** Lorsque vous saisissez une adresse Web, le résolveur DNS de votre appareil vérifie son cache local. S'il y trouve l'adresse IP correspondante, il l'utilise pour établir une connexion. Sinon, il envoie une requête DNS à un serveur DNS.

**Serveur DNS récursif :** Généralement, le résolveur de votre appareil transmet la requête à un serveur DNS récursif fourni par votre fournisseur de services Internet (FSI). Les serveurs récursifs effectuent la tâche de résolution des noms de domaine de manière récursive, parcourant la hiérarchie du DNS pour trouver l'adresse IP.

**Serveur DNS autorisé :** Le serveur DNS récursif peut ne pas avoir la réponse dans son cache. Dans ce cas, il interroge le serveur DNS autorisé pour le domaine spécifique. Le serveur DNS autorisé contient les enregistrements autorisés pour le domaine en question.

**Réponse :** Le serveur DNS autorisé fournit l'adresse IP du domaine au serveur DNS récursif, qui enregistre ensuite l'information et la renvoie au résolveur DNS de votre appareil.

**Accès au site Web :** Armé de l'adresse IP, le résolveur DNS de votre appareil peut maintenant établir une connexion avec le serveur Web hébergeant le site Web que vous avez demandé. Votre navigateur affiche le contenu du site Web en fonction de l'adresse IP récupérée.

**Types de DNS :**

- **Serveurs DNS récursifs :** Ces serveurs sont responsables de la recherche de l'adresse IP correspondant à un nom de domaine en parcourant la hiérarchie du DNS. Ils sont généralement fournis par les fournisseurs de services Internet (FSI) ou les fournisseurs de services DNS tiers.
- **Serveurs DNS autorisés :** Ces serveurs contiennent les enregistrements officiels d'un domaine spécifique. Lorsqu'ils sont interrogés par un serveur DNS récursif, les serveurs autorisés fournissent l'adresse IP du domaine.
- **Serveurs DNS racine :** En haut de la hiérarchie du DNS, ces serveurs contiennent des informations sur les domaines de premier niveau (TLD). Il existe 13 ensembles de serveurs DNS racine répartis dans le monde entier.

**Avantages du DNS :**

- **Convivialité :** Le DNS rend Internet plus accessible en permettant aux utilisateurs d'accéder aux sites Web à l'aide de noms de domaine faciles à retenir plutôt que d'adresses IP complexes.
- **Redondance :** Le DNS est un système distribué, ce qui signifie que même si un serveur DNS échoue, d'autres peuvent prendre le relais pour fournir des services de résolution.
- **Équilibrage de charge :** Le DNS peut être configuré pour répartir le trafic sur plusieurs serveurs, garantissant une utilisation efficace des ressources.
- **Accessibilité mondiale :** Le DNS permet aux sites Web et aux services d'être accessibles dans le monde entier, quel que soit leur emplacement physique.

En résumé, le DNS est un composant essentiel d'Internet qui simplifie la manière dont nous accédons aux sites Web et aux services. Il traduit les noms de domaine lisibles par l'homme en adresses IP, facilitant la communication Internet sans heurts.