

CISCO



Runtrack Réseau

Qu'est ce qu'un réseau ?

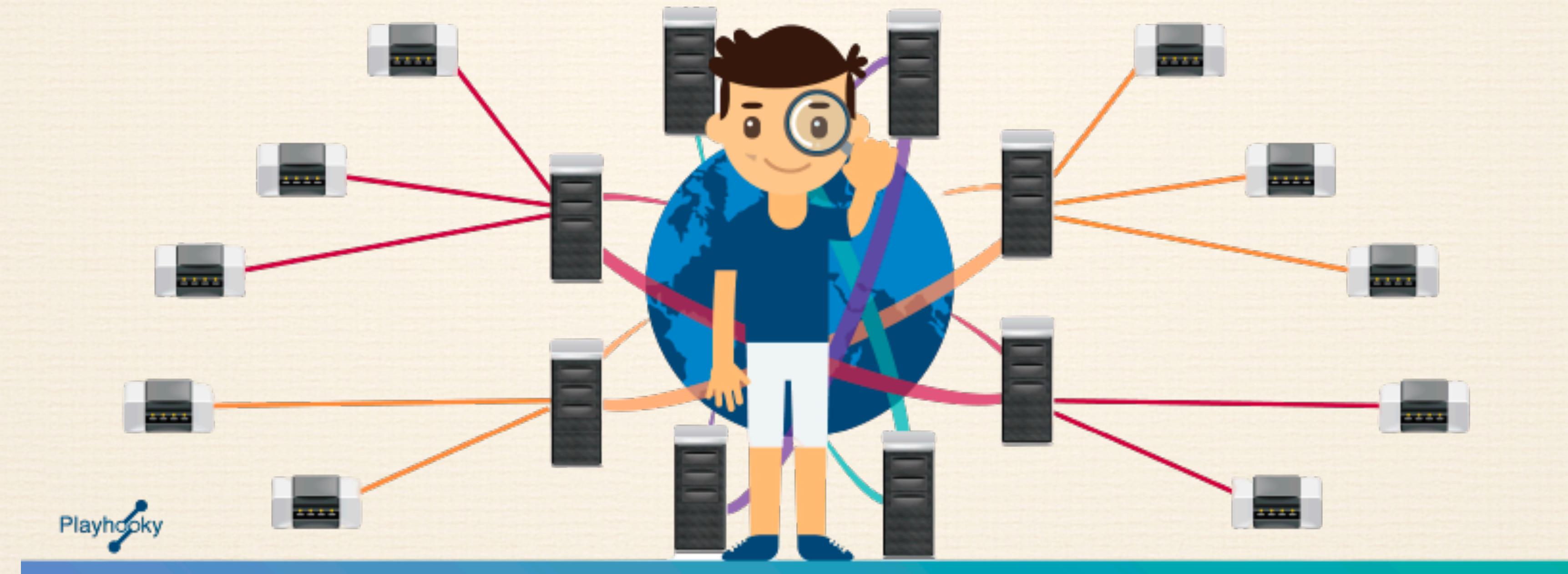
Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs, serveurs, périphériques, routeurs, commutateurs, etc.) interconnectés par des moyens de transmission (câbles, ondes radio, fibres optiques, etc.) permettant l'échange et le partage de données et de ressources.



Ces équipements peuvent communiquer entre eux en suivant des protocoles de communication spécifiques, définissant les règles et formats d'échange d'informations. Les réseaux informatiques peuvent varier en taille et en portée, allant des réseaux locaux (LAN) de petite échelle, comme un réseau domestique ou d'entreprise, aux réseaux étendus (WAN) couvrant des régions géographiques plus larges, voire le globe, comme l'Internet.

A quoi sert un réseau informatique ?

Ces réseaux permettent non seulement la communication entre dispositifs, mais aussi la centralisation et la décentralisation de l'information, la collaboration en temps réel, l'accès à distance à des ressources, et bien d'autres fonctions cruciales dans le monde numérique moderne.



Quel matériel avons-nous besoin pour construire un réseau ?

La construction d'un réseau informatique nécessite divers équipements en fonction de la taille, du type et des besoins spécifiques du réseau. Voici un aperçu des composants matériels couramment utilisés pour construire un réseau :

- **Ordinateurs / Dispositifs clients** : Ce sont les appareils utilisés par les utilisateurs finaux pour accéder au réseau. Cela peut inclure des ordinateurs de bureau, des ordinateurs portables, des smartphones, des tablettes, etc.
- **Câbles** : Ils sont utilisés pour relier physiquement les dispositifs entre eux. Les types de câbles courants comprennent :
 - **Câble Ethernet (câble à paires torsadées)** : couramment utilisé pour les connexions LAN.
 - **Fibre optique** : offre des débits plus élevés et est généralement utilisée pour les réseaux étendus ou les connexions backbone.

- **Câbles coaxiaux** : anciennement utilisés pour les réseaux Ethernet et toujours utilisés pour certaines connexions TV.
- **Commutateurs (Switches)** : Ils fonctionnent principalement au niveau de la couche de liaison de données (couche 2 du modèle OSI) pour connecter plusieurs dispositifs dans un réseau local, permettant la transmission de données entre eux.
- **Routeurs** : Ce sont des dispositifs qui opèrent principalement au niveau de la couche réseau (couche 3 du modèle OSI) et sont responsables de la transmission de paquets de données entre différents réseaux ou sous-réseaux. Ils déterminent le chemin optimal pour les données à travers un réseau complexe.
- **Points d'accès sans fil (Wireless Access Points - WAP)** : Ils permettent à des dispositifs équipés de WiFi de se connecter à un réseau sans avoir besoin de câbles.
- **Modems** : Ils convertissent les signaux numériques de votre réseau en signaux analogiques pour la transmission sur des lignes téléphoniques ou câblées, et vice versa.
- **Cartes réseau ou adaptateurs réseau** : Ce sont des composants matériels ou des périphériques externes qui permettent à un ordinateur ou à un autre dispositif de se connecter à un réseau.

- **Pare-feu matériel** : Un dispositif conçu pour bloquer ou permettre le trafic réseau selon des règles de sécurité définies.
- **Répéteurs, ponts et concentrateurs** : Ce sont des dispositifs qui peuvent étendre, relayer ou centraliser les signaux dans un réseau.
- **Armoires et racks de réseau** : Utilisés pour loger, organiser et protéger le matériel de réseau dans un environnement d'entreprise.
- **Alimentations sans interruption (ASI)** : Fournissent une alimentation de secours en cas de coupure de courant, garantissant ainsi la continuité des opérations réseau.
- **Systèmes de gestion et de surveillance** : Bien qu'ils ne soient pas strictement nécessaires pour construire un réseau, ils sont essentiels pour surveiller, gérer et optimiser les performances d'un réseau à grande échelle.

La nature exacte du matériel nécessaire dépendra de la taille du réseau, de son objectif, de son emplacement et d'autres facteurs spécifiques.

Quels câbles avez-vous choisis pour relier les 2 ordinateurs ?

Un câble "copper cross-over" (souvent simplement appelé câble croisé ou "cross-over") est utilisé pour relier directement deux dispositifs similaires sans avoir besoin d'un équipement intermédiaire comme un commutateur ou un routeur.

Dans un câble croisé, les fils utilisés pour la transmission de données sur un bout sont connectés aux fils utilisés pour la réception de données sur l'autre bout, et vice-versa. Cela permet aux PC de communiquer directement entre eux.

Les ordinateurs, lorsqu'ils utilisent des câbles Ethernet standard (non croisés), s'attendent à envoyer des données sur certains fils et à recevoir des données sur d'autres fils. Si vous essayez de connecter deux PC avec un câble standard, ils essaieront tous les deux d'émettre sur les mêmes fils et de recevoir sur les mêmes fils, ce qui entraîne des collisions et l'absence de communication. Le câble croisé résout ce problème en "croisant" les fils d'émission et de réception.

Cependant, il convient de noter que de nombreux équipements modernes, y compris les cartes réseau sur les ordinateurs récents, sont équipés de la fonctionnalité "Auto MDI/MDI-X". Cela leur permet de détecter automatiquement le type de câble et de configurer leurs ports en conséquence, rendant parfois le câble croisé obsolète pour de telles connexions. Mais dans les situations où l'équipement ne dispose pas de cette fonctionnalité, un câble croisé reste essentiel pour connecter directement deux PC.

Qu'est ce qu'une adresse IP et à quoi ça sert ?

Une adresse IP (Internet Protocole) est un identifiant numérique unique qui est attribué à chaque dispositif connecté à un réseau informatique utilisant le protocole IP. Cette adresse sert à identifier de manière univoque un dispositif (comme un ordinateur, un serveur, un smartphone ou une imprimante) afin de permettre la transmission de données entre les dispositifs sur un réseau ou sur Internet.

Chaque adresse IP est composée de séries de chiffres séparées par des points (dans le cas d'IPv4) ou de séries de chiffres et de lettres séparées par des deux-points (dans le cas d'IPv6). Elle est essentielle au bon fonctionnement du protocole TCP/IP, qui est la fondation des communications modernes sur Internet.

De plus, l'adresse IP peut être utilisée pour déterminer la localisation géographique approximative d'un dispositif et, dans certains cas, pour appliquer des politiques de réseau ou des restrictions basées sur l'emplacement.

Qu'est ce qu'une adresse MAC ?

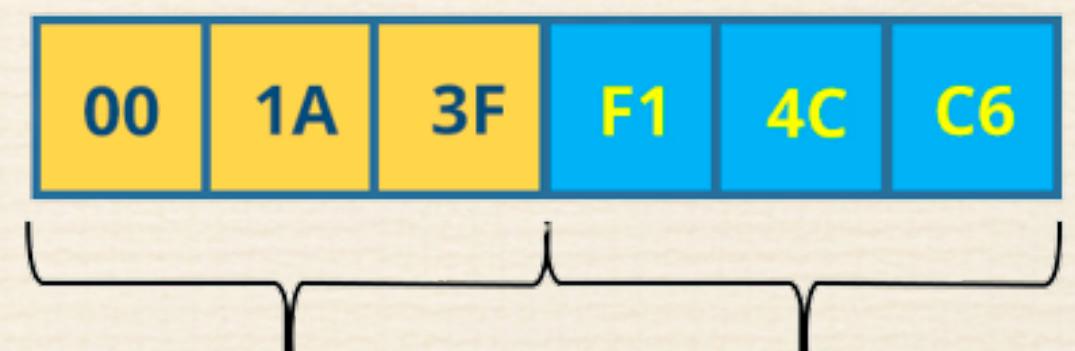
Une adresse MAC (Media Access Control) est un identifiant physique unique composé de 12 caractères hexadécimaux, attribué à la carte réseau d'un dispositif pour garantir son unicité au sein d'un réseau local.

Contrairement à l'adresse IP, qui peut changer selon le réseau sur lequel un dispositif est connecté, l'adresse MAC demeure constante et est généralement gravée dans le matériel par le fabricant.

Elle est utilisée pour la transmission de données au sein de sous-réseaux et fonctionne à la couche 2 (liaison de données) du modèle OSI. Cette adresse est souvent formatée en six groupes de deux caractères hexadécimaux séparés par des deux-points ou des tirets.

MAC

Media Access Control Address



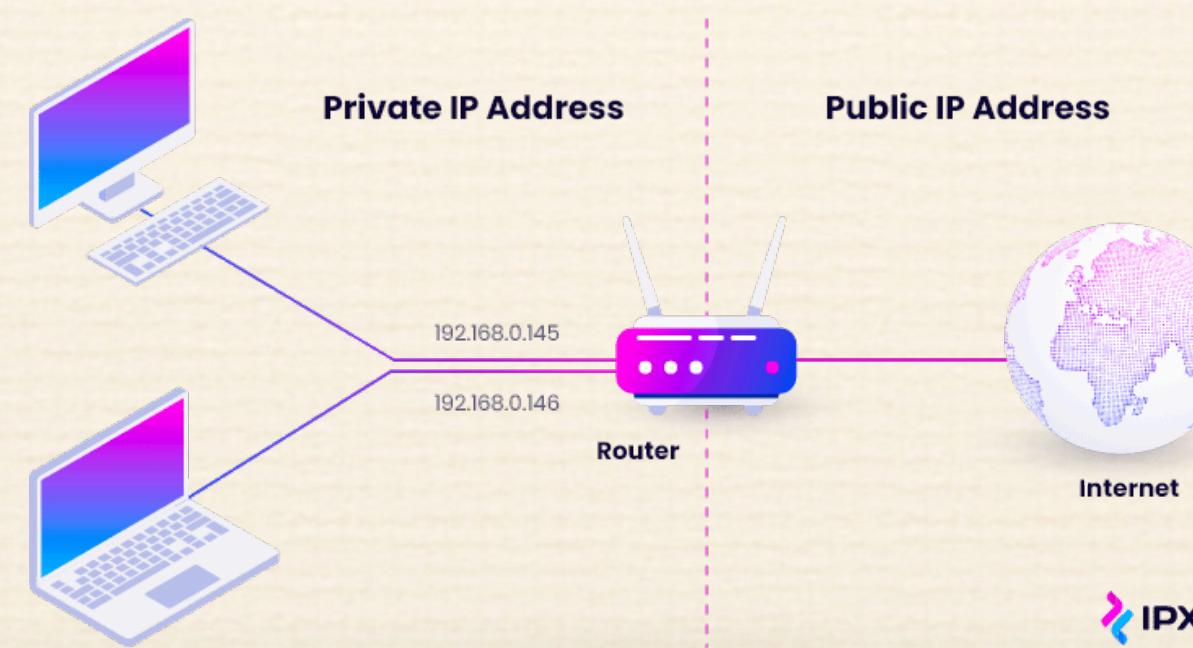
Organizationally Unique Identifier Network Interface Controller Specific

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

Une adresse IP publique est une adresse unique assignée à un dispositif, permettant sa communication et son identification sur Internet. Elle est visible sur le réseau mondial, ce qui signifie que les sites web et les serveurs distants utilisent cette adresse pour communiquer avec le dispositif. Les fournisseurs de services Internet (ISP) attribuent généralement ces adresses.

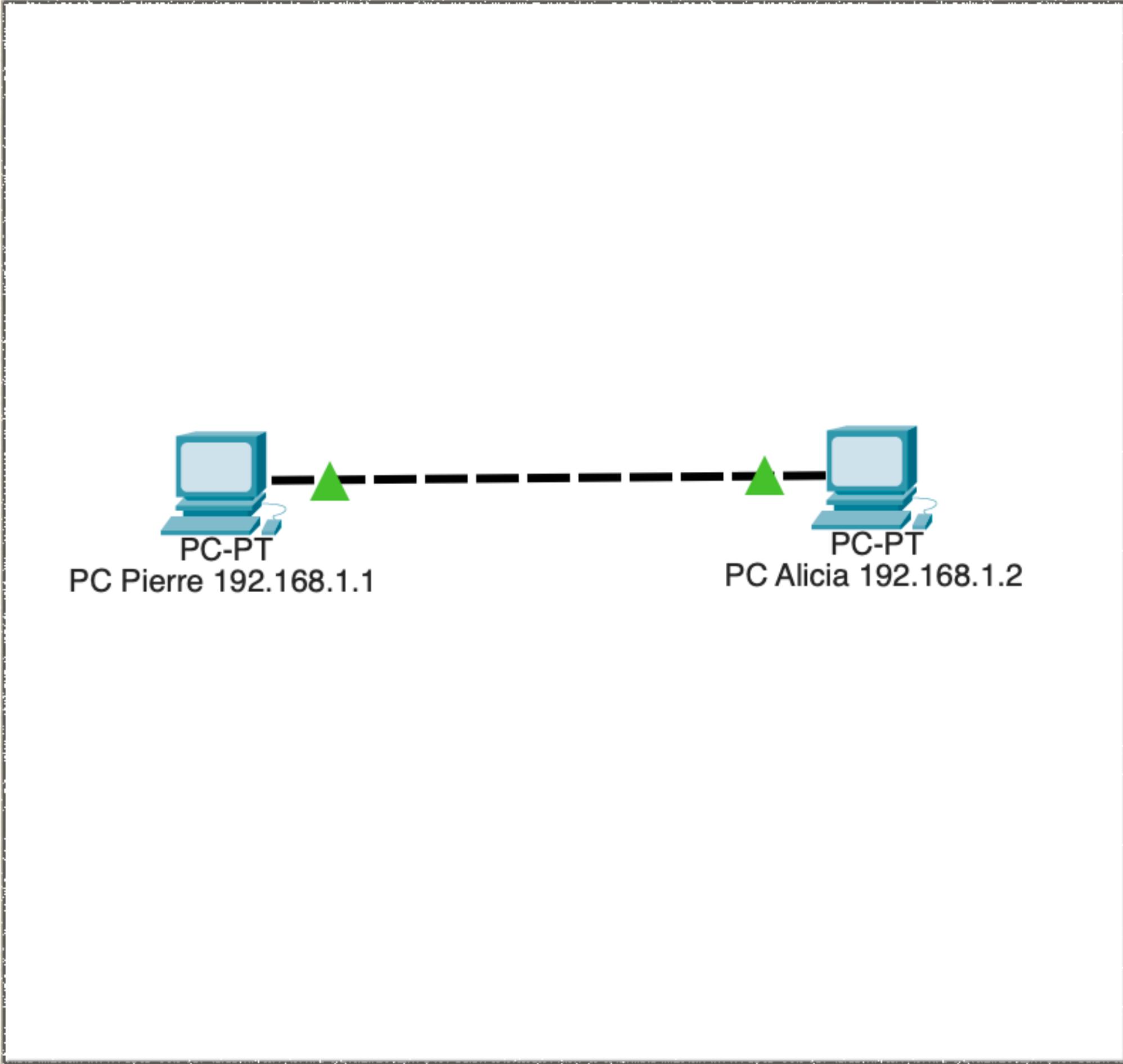
Une adresse IP privée, en revanche, est utilisée à l'intérieur d'un réseau local et n'est pas directement accessible depuis Internet. Elle permet la communication entre les dispositifs au sein d'un même réseau local, comme votre domicile ou une entreprise. Ces adresses sont attribuées par le routeur du réseau et suivent des plages spécifiques définies par les normes IP (par exemple, 192.168.x.x pour IPv4).

En résumé, tandis que l'IP publique sert d'identifiant pour un dispositif sur Internet, l'IP privée permet l'identification et la communication de ce dispositif au sein d'un réseau local spécifique.



Quelle est l'adresse de ce réseau ?

- ❖ Comme indiqué sur le screen-shot, l'adresse IP de Pierre est 192.168.1.1 et l'adresse IP de Alicia est 192.168.1.2



Vérification de l'adresse IP de Pierre

- ❖ Pour accéder au terminal et à l'adresse IP de l'ordinateur de Pierre :
- ❖ J'ai double cliqué sur l'icône représentant un ordinateur.
- ❖ Je suis aller dans l'onglet « Desktop » puis dans « Command prompt ».
- ❖ Puis pour finir j'ai rentré la commande « ipconfig ».

```
Command Prompt

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

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::250:FFF:FED2:AA05
IPv6 Address.....: :::
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
0.0.0.0

Bluetooth Connection:

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

C:\>
```

Vérification de l'adresse IP de Alicia

- ❖ Pour accéder au terminal et à l'adresse IP de l'ordinateur de Alicia :
- ❖ J'ai double cliqué sur l'icône représentant un ordinateur.
- ❖ Je suis aller dans l'onglet « Desktop » puis dans « Command prompt ».
- ❖ Puis pour finir j'ai rentré la commande « ipconfig ».

```
Command Prompt

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

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::290:2BFF:FEAA:5264
IPv6 Address.....: :::
IPv4 Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
0.0.0.0

Bluetooth Connection:

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

C:\>
```

Test de connectivité entre le PC de Pierre et Alicia

- ❖ Pour tester la connectivité entre les 2 PC, je me suis rendu dans le terminal du PC de Pierre et j'ai rentré la commande « ping 192.168.1.2 ».
- ❖ Cette dernière suite de chiffre correspond à l'adresse IP du pc 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<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

c:\>

Test de connectivité entre le PC de Pierre éteint et celui d'Alicia allumé

La commande ping envoie des paquets ICMP (Internet Control Message Protocol) à l'adresse IP cible en espérant recevoir une réponse. Si l'ordinateur est éteint, il ne répondra pas à ces requêtes, ce qui est le cas pour l'ordinateur de Pierre.

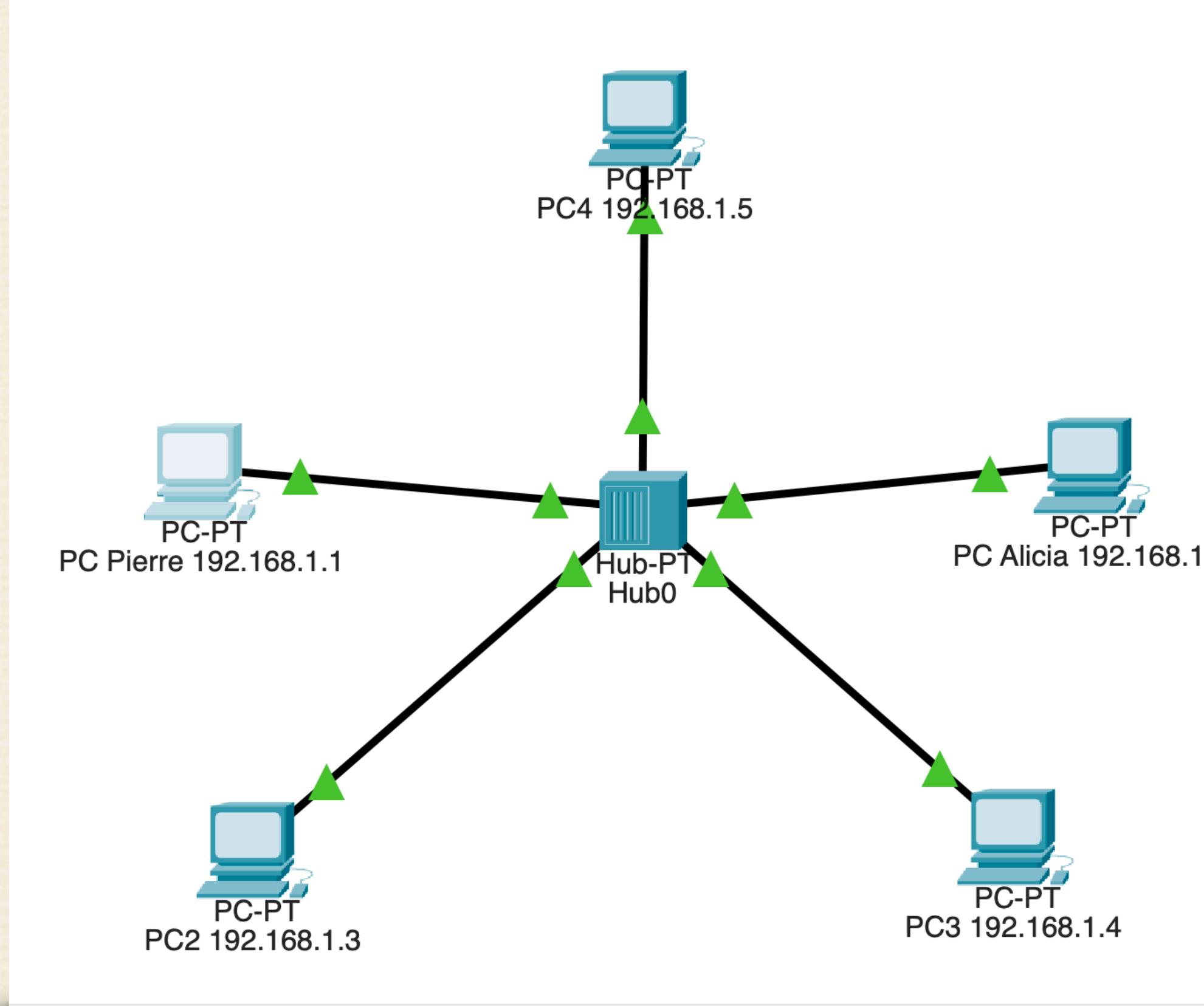
« Request timed out » : Cela signifie que la requête ICMP n'a reçu aucune réponse pendant le délai imparti. C'est le message d'erreur le plus courant dans cette situation.

Par défaut, la commande ping essaiera plusieurs fois (généralement 4 fois sur Windows) d'atteindre l'ordinateur cible. Si l'ordinateur est éteint pendant toute la durée de cette tentative, chaque requête renverra le même type de message d'erreur.

Il est à noter que des résultats similaires peuvent également se produire si l'ordinateur cible est allumé mais configuré pour ignorer les requêtes ICMP, s'il est derrière un pare-feu qui bloque ces requêtes, ou s'il y a des problèmes de réseau empêchant les paquets d'atteindre l'ordinateur cible.

```
C:\>ping  
Cisco Packet Tracer PC Ping  
  
Usage: ping [-n count | -v TOS | -t ] target  
  
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),
```

Agrandissement avec 5 PC + Test de ping entre les PC



```
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.1.3
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time=1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms 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 = 0ms, Maximum = 1ms, Average = 0ms

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=2ms 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 = 2ms, 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<1ms 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 = 1ms, Average = 0ms
```

Quelle est la différence entre un HUB et un switch ?

Un **hub** et un **switch** sont tous deux des dispositifs utilisés dans les réseaux pour connecter plusieurs appareils, mais ils opèrent de manière différente et à des niveaux distincts du modèle OSI. Voici les principales différences :

Mode de fonctionnement :

- **Hub** : Lorsqu'un paquet arrive sur l'un des ports du hub, il est dupliqué et transmis à tous les autres ports. Il fonctionne en mode "broadcast".
- **Switch** : Il est plus intelligent. Lorsqu'un paquet arrive, le switch examine l'adresse MAC de destination et ne le transmet qu'au port spécifique associé à cette adresse. Il fonctionne en mode "unicast" pour les transmissions normales.

Niveau de communication :

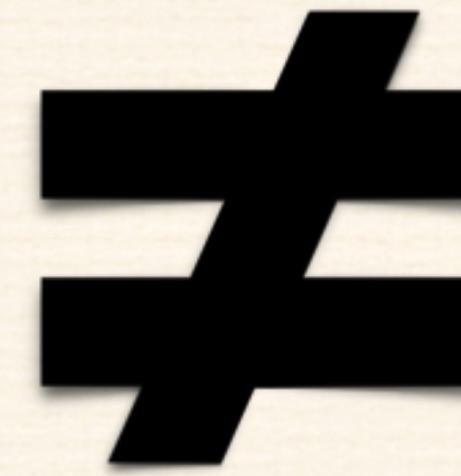
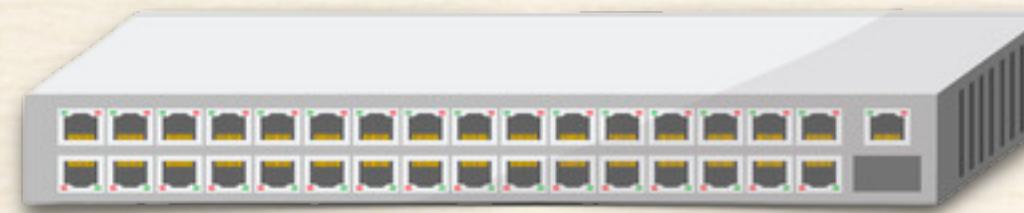
- **Hub** : Fonctionne à la couche 1 (couche physique) du modèle OSI. Il ne fait que transmettre des bits.
- **Switch** : Fonctionne à la couche 2 (couche de liaison de données) du modèle OSI. Il est capable de reconnaître les adresses MAC.

Performance :

- **Hub** : Peut causer des collisions et réduire les performances du réseau car tous les dispositifs reçoivent tous les paquets.
- **Switch** : Réduit les collisions et optimise le trafic réseau en s'assurant que seuls les dispositifs appropriés reçoivent les paquets destinés.

Sécurité :

- **Hub** : Moins sécurisé car les données sont envoyées à tous les appareils.
- **Switch** : Plus sécurisé car les données sont envoyées uniquement à l'appareil cible.



En résumé, alors qu'un hub transmet simplement des données à tous les appareils connectés, un switch est plus sélectif et efficace, envoyant des données uniquement à l'appareil destinataire, offrant ainsi une meilleure performance et sécurité.

Comment fonctionne un HUB, quels sont ses avantages et ses inconvénients ?

Un **HUB** est un dispositif de réseau simple utilisé pour connecter plusieurs appareils dans un réseau local (LAN). Il fonctionne en retransmettant tous les paquets de données qu'il reçoit à tous les appareils connectés à ses ports.

Fonctionnement :

Lorsqu'un dispositif envoie un paquet de données au hub, le hub prend ce paquet et le distribue à tous les autres dispositifs connectés à lui. Il ne distingue pas la destination spécifique du paquet, il envoie donc le paquet à tous, à l'exception du dispositif d'origine.

Avantages :

- **Simplicité** : Les hubs sont faciles à installer et à configurer, ne nécessitant aucune gestion ni configuration.
- **Coût** : Ils sont généralement moins chers que d'autres dispositifs de commutation, tels que les switches ou les routeurs.

Inconvénients :

- **Collisions** : Étant donné que le hub envoie des données à tous les dispositifs, il peut y avoir des collisions si deux dispositifs ou plus tentent de communiquer en même temps. Cela peut ralentir le réseau.
- **Pas d'isolation du trafic** : Tous les dispositifs reçoivent toutes les données, qu'elles leur soient destinées ou non. Cela pose des problèmes de sécurité et de confidentialité.
- **Performance** : Dans les grands réseaux, les hubs peuvent être une source de goulot d'étranglement en raison de leur mode de fonctionnement non sélectif et des collisions qu'ils peuvent causer.
- **Pas d'intelligence** : Contrairement aux switches, les hubs n'apprennent pas et ne stockent pas les adresses MAC des dispositifs connectés. Ils ne peuvent donc pas diriger le trafic de manière efficace.

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

Un **switch** est un dispositif de réseau utilisé pour interconnecter des dispositifs au sein d'un réseau local (LAN). Contrairement à un hub, un switch est capable de diriger le trafic de manière intelligente en fonction des adresses MAC.

Avantage d'un switch

- **Efficacité du trafic** : Les switches transmettent les paquets uniquement au port de destination approprié, réduisant ainsi le trafic inutile sur le réseau.
- **Réduction des collisions** : En isolant chaque transmission de paquets à un seul destinataire, les switches réduisent les risques de collisions.
- **Tables d'adresses MAC** : Les switches maintiennent une table d'adresses MAC, leur permettant de "se souvenir" des dispositifs connectés et d'améliorer l'efficacité du routage des paquets.
- **Sécurité** : Les données sont envoyées uniquement au dispositif destinataire, offrant une meilleure confidentialité par rapport à un hub.
- **Segmentation du réseau** : Les switches peuvent créer des VLAN (réseaux locaux virtuels) pour segmenter le trafic du réseau.

Inconvénients d'un switch

- **Coût:** Les switches de haute qualité, en particulier ceux dotés de nombreuses fonctionnalités ou de nombreux ports, peuvent être coûteux.
- **Complexité de gestion:** Les switches administrables (ou manageable) peuvent nécessiter une configuration avancée, ce qui demande des compétences techniques. Une mauvaise configuration peut entraîner des problèmes de réseau.
- **Vulnérabilités de sécurité:** Les switches peuvent être la cible d'attaques si leurs configurations ne sont pas sécurisées correctement. De plus, des vulnérabilités non corrigées peuvent permettre à des attaquants d'accéder au réseau.
- **Boucles de réseau:** Sans le protocole approprié (comme le Spanning Tree Protocol - STP), les switches peuvent causer des boucles, conduisant à des broadcast storms, ce qui peut saturer le réseau.
- **Scalabilité:** Même si un switch peut avoir de nombreux ports, il arrive un point où il est nécessaire d'ajouter d'autres switches ou de structurer différemment le réseau, ce qui peut compliquer la topologie.
- **Dépendance à l'électricité:** Comme tous les équipements électroniques, les switches sont vulnérables aux coupures de courant.
- **Obsolescence technologique:** Avec l'évolution rapide de la technologie, un switch peut rapidement devenir dépassé par de nouvelles normes ou technologies.
- **Limitation de la distance:** Dans un contexte de réseau local, les switches sont limités en termes de distance pour la transmission de données, notamment avec certaines technologies comme l'Ethernet.

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

Apprentissage : Lorsqu'un appareil envoie un paquet, le switch enregistre l'adresse MAC de l'appareil et le port associé dans une table de commutation.

Décision de transmission :

Si la destination est une adresse MAC connue dans sa table, le switch dirige le paquet uniquement vers le port associé à cette adresse.

Si la destination est inconnue, le switch envoie le paquet à tous les ports sauf le port d'origine (broadcast).

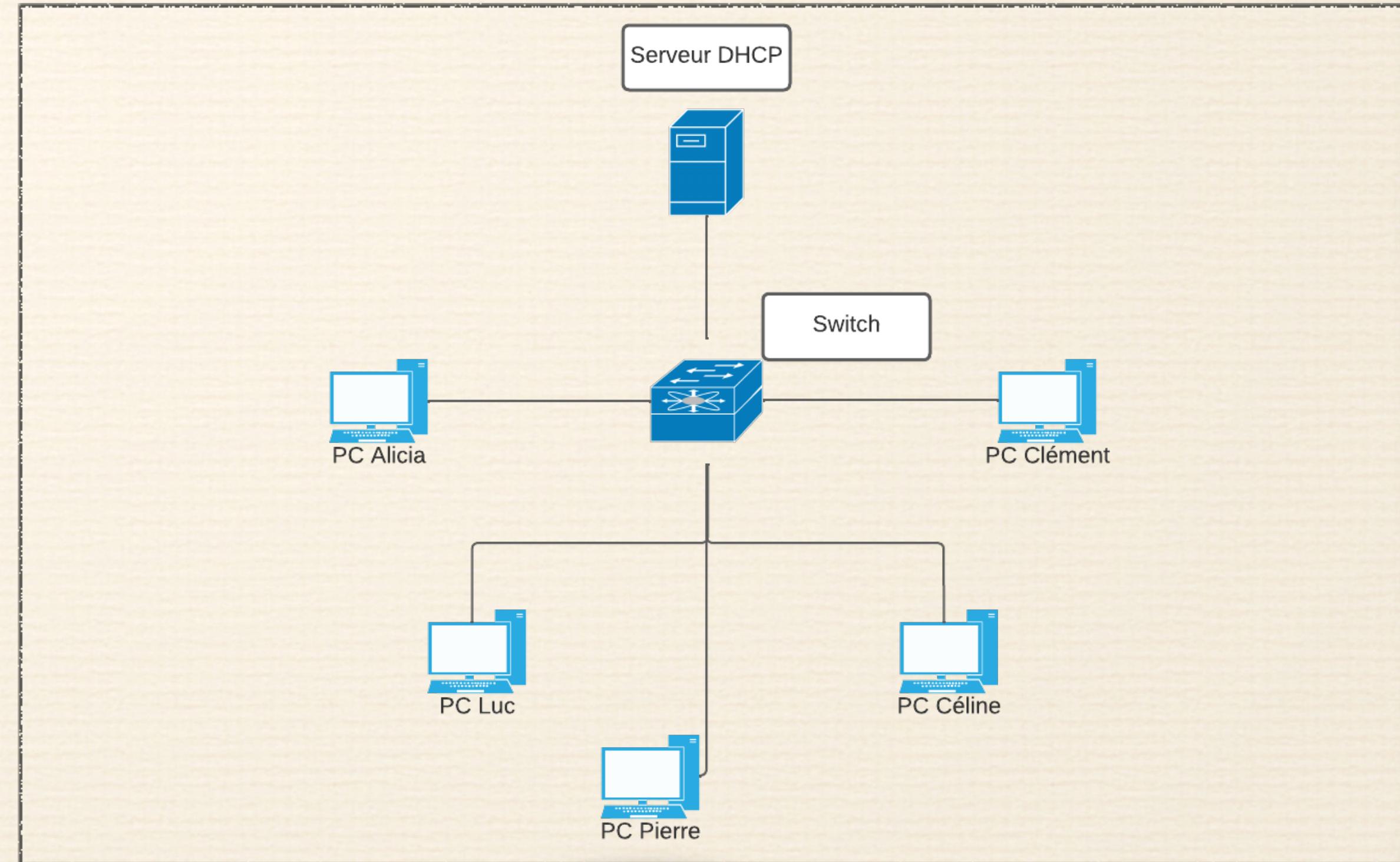
Élimination des boucles : Le switch utilise le protocole Spanning Tree Protocol (STP) pour éviter les boucles dans le réseau, qui peuvent causer des broadcast storms.

En bref, un switch utilise la table de commutation pour diriger efficacement les paquets vers leurs destinations appropriées dans un réseau local.

Les avantages d'un schéma type CISCO

1) Apprentissage et formation :

- **Expérimentation sans risque** : Les utilisateurs peuvent créer, configurer et dépanner des réseaux virtuels sans craindre d'endommager l'équipement ou de causer des perturbations dans un environnement réel. Cela permet un apprentissage pratique et approfondi.
- **Compréhension visuelle** : Avec Cisco Packet Tracer, les utilisateurs peuvent visualiser le fonctionnement interne d'un réseau, y compris la manière dont les paquets de données se déplacent à travers le réseau.
- Cela aide à comprendre des concepts complexes tels que le routage, la commutation, etc.



2) Flexibilité et test :

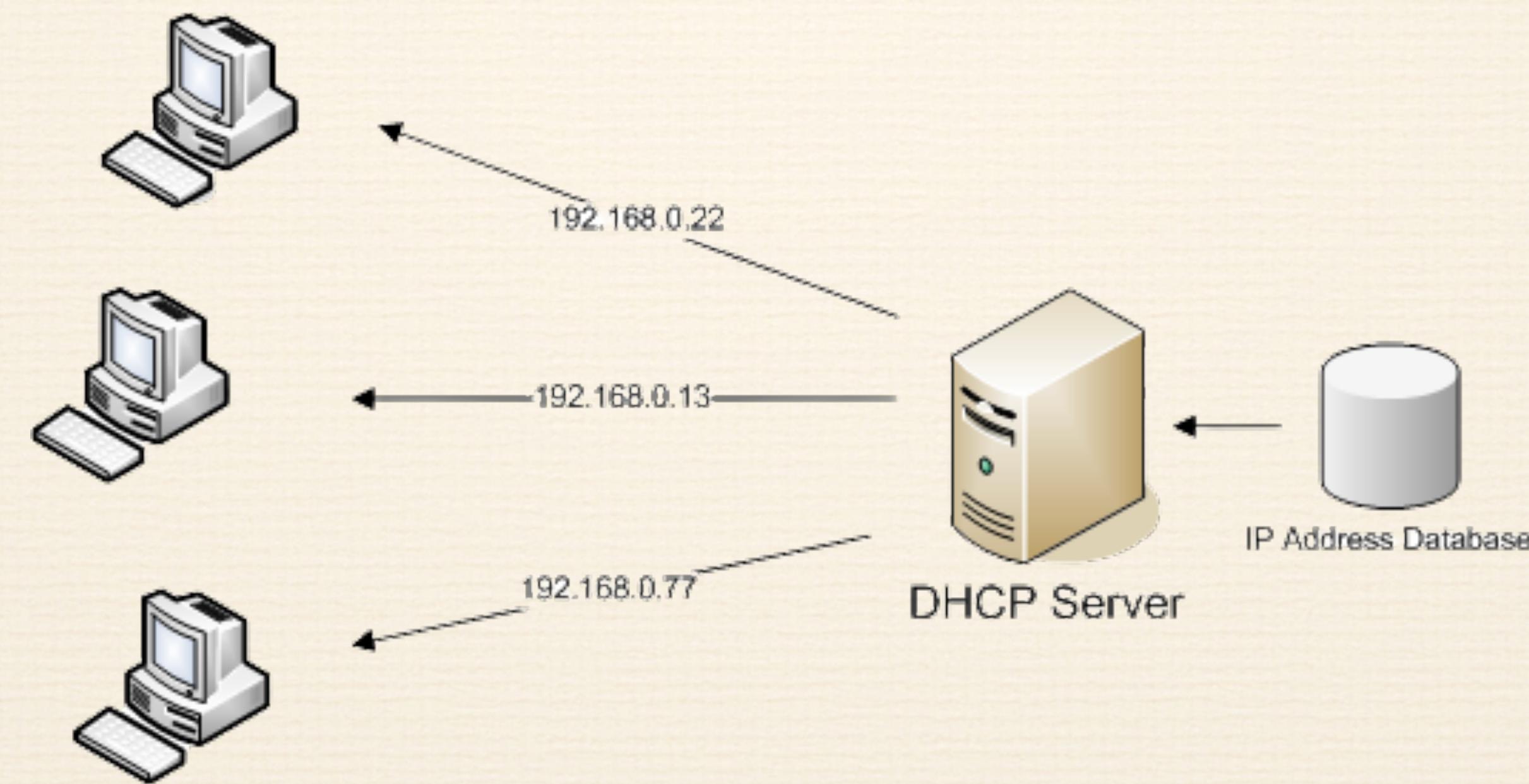
- **Test avant déploiement** : Avant de mettre en œuvre de nouvelles configurations ou technologies dans un environnement réel, les ingénieurs et les administrateurs réseau peuvent les tester dans Cisco Packet Tracer pour s'assurer qu'ils fonctionnent comme prévu.
- **Reproduction des scénarios réels** : Si un problème survient dans un réseau réel, il peut être reproduit dans Packet Tracer pour aider au dépannage sans affecter l'environnement de production.

3) Coût-Efficacité :

- **Moins de matériel nécessaire** : Au lieu d'acheter un équipement coûteux pour chaque scénario d'apprentissage ou de test, les utilisateurs peuvent simuler un grand nombre de dispositifs et de topologies réseau avec un seul logiciel.
- **Économies d'énergie** : Puisque l'équipement physique n'est pas nécessaire, il n'y a pas de coûts énergétiques associés au fonctionnement et au refroidissement de cet équipement.

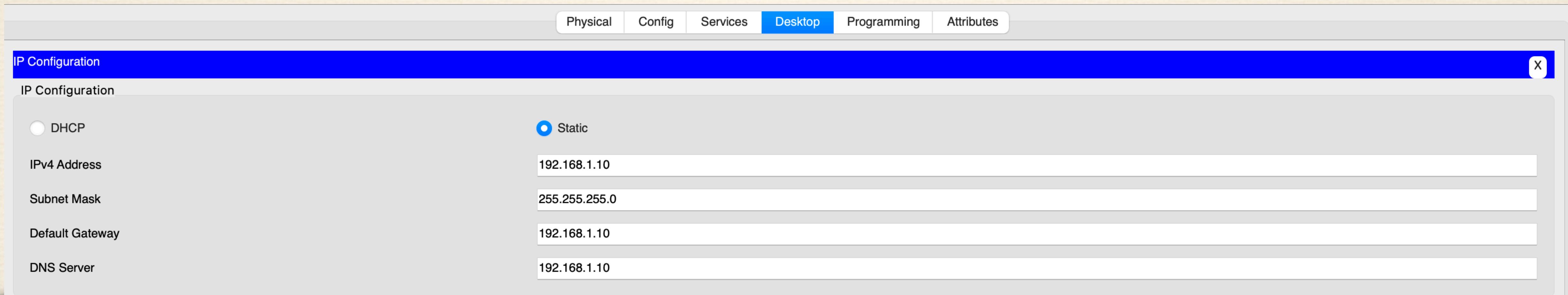
Quelle est la différence entre une adresse IP statique et une attribué par DHCP ?

Une adresse IP statique est une adresse IP fixe manuellement configurée sur un périphérique et qui ne change pas. Une adresse IP attribuée par DHCP est automatiquement assignée à un périphérique par un serveur DHCP pour une durée déterminée et peut varier au fil du temps.



Mise en place d'un serveur DHCP

Pour mettre en place un serveur DHCP nous allons tout d'abord créer notre serveur en le déposant dans le schéma de CISCO. La prochaine étape est de cliquer sur le serveur, se rendre dans desktop et cliquer sur « IP Configuration » pour assigner une adresse IP statique.



Nous entrons donc l'adresse IP dans « IPv4 Adresse, Default Gateway et dans le DNS Serveur ». Nous entrons également l'adresse Subnet Mask.

Dans le même serveur, on se rend cette fois-ci dans l'onglet « service » et on clique sur « DHCP » dans le menu vertical.

The screenshot shows a software interface for managing services. On the left, a vertical sidebar lists various services: HTTP, DHCP (which is selected and highlighted in blue), DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, and Radius EAP. At the top, a horizontal navigation bar includes tabs for Physical, Config, Services (which is active), Desktop, Programming, and Attributes. The main area is titled "DHCP" and contains the following configuration fields:

- Interface: FastEthernet0
- Service status: On (radio button selected)
- Pool Name: server DHCP
- Default Gateway: 192.168.1.10
- DNS Server: 192.168.1.10
- Start IP Address: 192
- Subnet Mask: 255
- Maximum Number of Users: 236
- TFTP Server: 0.0.0.0
- WLC Address: 0.0.0.0

Below these fields are three buttons: Add, Save, and Remove. A table summary row is shown at the bottom:

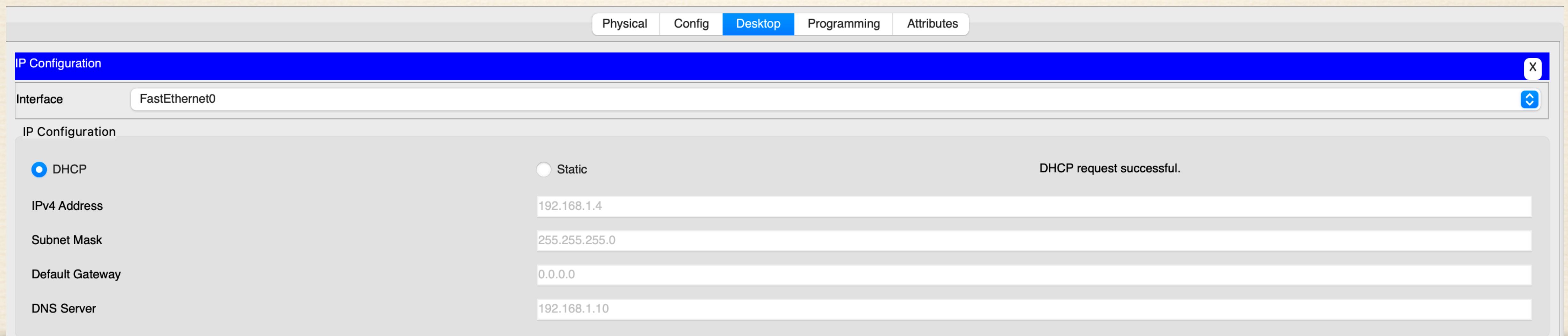
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
server DHCP	192.168.1.10	192.168.1.10	192.168.1.20	255.255.255.0	236	0.0.0.0	0.0.0.0

Avant toute choses, on active le service DHCP en cliquant sur « On ». On rempli alors le « default gateway » et « DNS » comme précédemment. Ensuite dans « Start IP Adresse » on entre la première adresse que la machine aura dans la plage.

Dans la partie « Maximum Numbers » on entre la quantité de machines que l'on veut connecter.

Il ne nous reste plus qu'à activer DHCP pour chaque ordinateurs que l'on souhaite connecter au serveur.

Pour cela, on clique sur l'ordinateur que l'on veut activer en DHCP, puis on se rend dans l'onglet « Desktop » puis « IP Config »



Si tout s'est bien déroulé, on devrait avoir le message « DHCP request successful » qui s'affiche après avoir cliqué sur DHCP.

Le plan d'adressage du réseau

Un plan d'adressage en informatique est une stratégie organisée pour attribuer et gérer des adresses IP au sein d'un réseau, assurant une communication efficace et évitant les conflits d'adresses.

Pour créer des sous-réseaux, nous devons d'abord déterminer le nombre de bits nécessaires pour chaque taille de sous-réseau en fonction du nombre d'hôtes requis.

Pour calculer combien de bits nous avons besoin on doit trouver une puissance de 2 qui est égale ou supérieure au nombre d'hôtes requis PLUS deux adresses pour l'adresse réseau et l'adresse de diffusion.

Par exemple, pour 12 hôtes, nous avons besoin d'au moins 14 adresses (12 pour les hôtes, 1 pour l'adresse réseau et 1 pour l'adresse de diffusion). La plus petite puissance de 2 qui est supérieure ou égale à 14 est 16, ce qui est 2^4 . Donc, nous avons besoin de 4 bits pour les hôtes.

On répète le processus pour chaque taille de sous-réseau.

- Pour 12 hôtes, nous avons besoin de 14 adresses (2^4). Donc, 4 bits sont nécessaires. On notera le masque « /28 »
- Pour 30 hôtes, nous avons besoin de 32 adresses (2^5). Donc, 5 bits sont nécessaires. On notera le masque « /27 »
- Pour 120 hôtes, nous avons besoin d'au moins 122 adresses. La plus petite puissance de 2 qui est supérieure ou égale à 122 est 128, qui est 2^7 . Donc, 7 bits sont nécessaires. On notera le masque « /25 »
- Pour 160 hôtes, nous avons besoin d'au moins 162 adresses. La plus petite puissance de 2 qui est supérieure ou égale à 162 est 256, qui est 2^8 . Donc, 8 bits sont nécessaires. On notera le masque « /24 »

La clé est de se rappeler que l'on ajoute toujours deux adresses supplémentaires pour chaque sous-réseau: une pour l'adresse réseau et une pour l'adresse de diffusion. Ces deux adresses ne peuvent pas être assignées à des hôtes.

Adressage du plan :

L'idée est d'allouer des blocs d'adresses IP en fonction du nombre de bits d'hôte nécessaires pour chaque sous-réseau. En commençant par l'adresse réseau initiale 10.0.0.0, nous allons définir des plages d'adresses pour chaque type de sous-réseau en nous basant sur les notations de masques (/28, /27, /25 et /24) que nous avons déterminées précédemment.

- Sous-réseau de 12 hôtes (/28) :
- Adresse réseau : 10.0.0.0
- **Plage d'adresses** : 10.0.0.1 à 10.0.0.14 (pour les hôtes)
- Adresse de diffusion : 10.0.0.15
- Prochaine adresse réseau disponible : 10.0.0.16

	192	45	2	9
Adresse IP	11000000	00101101	00000010	00001001
Masque	255	255	255	0
Sous réseau	11000000	00101101	00000010	00000000
Hôte	0	0	0	9

- 5 sous-réseaux de 30 hôtes (/27) :
- Pour ces sous-réseaux, chaque bloc aura 32 adresses (2^5). Nous créons 5 de ces blocs.
- **1er sous-réseau :** 10.0.0.16 à 10.0.0.47
- **2e sous-réseau :** 10.0.0.48 à 10.0.0.79
- (On continue d'incrémenter 32 adresses pour chaque sous-réseau suivant.)
- **Prochaine adresse réseau disponible :** 10.0.0.128 (après avoir alloué 5 blocs de 32 adresses)
- 5 sous-réseaux de 120 hôtes (/25) :
- Chaque bloc aura 128 adresses (2^7). Nous créons 5 de ces blocs.
- **1er sous-réseau :** 10.0.0.128 à 10.0.1.127
- **2e sous-réseau :** 10.0.1.128 à 10.0.2.127
- (On continue 128 adresses pour chaque sous-réseau suivant.)
- **Prochaine adresse réseau disponible :** 10.0.3.0 (après avoir alloué 5 blocs de 128 adresses)

5 sous-réseaux de 160 hôtes (/24) :

- Chaque bloc aura 256 adresses (2^8). Nous créons 5 de ces blocs.
- **1er sous-réseau** : 10.0.3.0 à 10.0.3.255
- **2e sous-réseau** : 10.0.4.0 à 10.0.4.255
- (Continuez d'incrémenter de 256 adresses pour chaque sous-réseau suivant.)



A savoir : Un routeur est un dispositif matériel ou logiciel dans un réseau informatique qui transmet des données sous forme de paquets entre différents segments de réseau.

Il joue un rôle essentiel dans la gestion des communications entre différents sous-réseaux, en veillant à ce que le trafic soit acheminé efficacement tout en appliquant les politiques de sécurité et d'optimisation nécessaires.

Cependant il n'est pas obligatoire dans cette configuration.

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

L'adresse 10.0.0.0 fait partie des adresses IP privées définies par le RFC 1918. Ces adresses sont réservées pour une utilisation interne dans des réseaux privés et ne sont pas routables sur Internet public.

- **Espace d'adressage massif** : Les adresses de classe A offrent un vaste espace d'adressage. Avec 10.0.0.0, on peut avoir potentiellement 16 millions d'adresses (10.0.0.0 à 10.255.255.255).
- **Flexibilité pour le sous-réseau** : Grâce à la grande quantité d'adresses disponibles, nous avons une grande flexibilité pour diviser le réseau en nombreux sous-réseaux selon nos besoins.
- **Standardisation** : De nombreuses organisations utilisent l'adresse 10.0.0.0 par convention, car elle est facilement reconnaissable comme une adresse privée de classe A.

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

La différence entre ces classes réside principalement dans la répartition des bits pour le réseau et l'hôte. Cela affecte le nombre d'adresses disponibles et la taille des réseaux. Avec l'introduction du CIDR, cette division stricte en classes est devenue obsolète, mais elle est toujours utilisée dans certains contextes éducatifs ou historiques.

- Classe A :
 - Plage d'adresses : 1.0.0.0 à 126.0.0.0
 - Masque par défaut : /8
 - Utilisée pour les très grands réseaux, elle offre plus de 16 millions d'adresses sur le même réseau.

- Classe B :

- Plage d'adresses : 128.0.0.0 à 191.255.0.0
- Masque par défaut : /16
- Conçue pour des réseaux de taille moyenne à grande, elle offre 65,536 adresses.

- Classe C :

- Plage d'adresses : 192.0.0.0 à 223.255.255.0
- Masque par défaut : /24
- Destinée aux petits réseaux, elle offre 256 adresses



Il existe également des classes D (pour le multicast) et E (réservée pour des utilisations futures ou expérimentales), mais elles sont moins courantes dans les discussions sur l'adressage IP traditionnel.

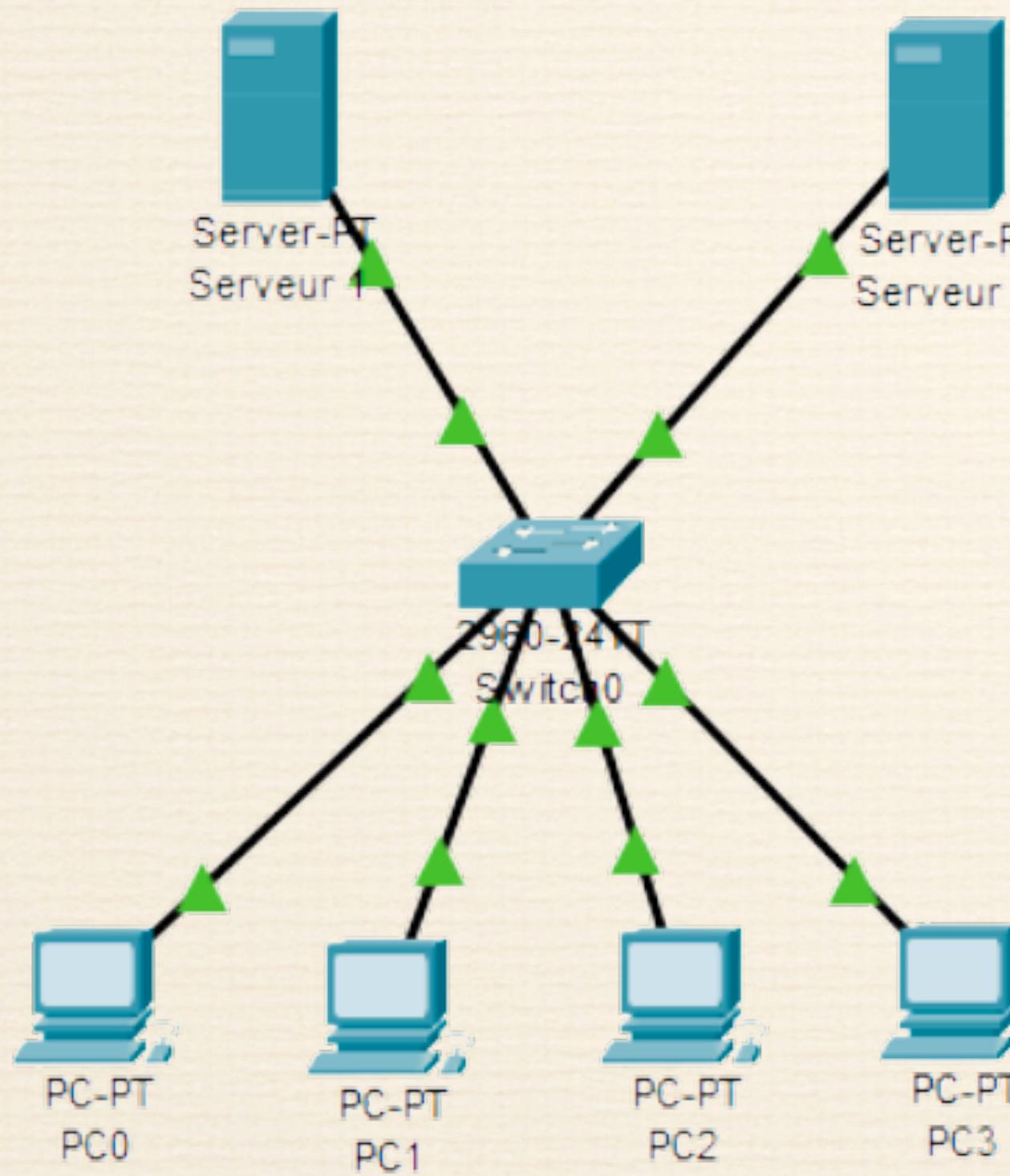
Le modèle OSI

Le modèle OSI (Open Systems Interconnection) est un modèle de référence pour comprendre et concevoir des réseaux et des systèmes de communication. Il divise les fonctions de communication en sept couches distinctes, chacune ayant une responsabilité spécifique dans le processus de communication entre deux systèmes informatiques.

Couche OSI	Rôle
1. Physique	Décrit le média de transmission, les débits, les modulations, et les caractéristiques électriques. S'occupe de la transmission et de la réception de bits bruts sur un média physique. Grâce à la fibre optique , câble RJ45
2. Liaison de données	Fournit une transmission fiable des données sur le même réseau. Déetecte et corrige les erreurs au niveau du bit. Inclut des protocoles comme Ethernet, MAC, WI-FI .
3. Réseau	Se charge du routage (routeur) des paquets entre les dispositifs sur des réseaux différents. Attribue des adresses logiques et détermine le chemin via des protocoles comme IP. IPv4, IPv6
4. Transport	Assure la transmission fiable des données entre les systèmes et peut établir une connexion. Règle la taille et le taux d'échange des paquets. Inclut des protocoles comme TCP et UDP
5. Session	Gère l'établissement, la maintenance et la terminaison des sessions entre les applications. PPTP
6. Présentation	S'occupe de la traduction, du chiffrement et de la compression des données. Garantit que les données sont présentées à la couche Application dans un format compréhensible. SSL/TLS
7. Application	Fournit une interface pour les applications afin d'accéder aux services réseau. Inclut des protocoles comme HTML, FTP, HTTP, SMTP , etc...

Quelle est l'architecture de ce réseau ?

L'architecture semble être un réseau local (LAN) simple, où les PCs et les serveurs sont probablement connectés via un commutateur (switch) ou un concentrateur (hub). Les adresses IP sont toutes du même sous-réseau, ce qui indique qu'ils sont tous sur le même réseau local.



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

Avec un masque de sous-réseau :
255.255.255.0

Quelle est l'adresse IP du réseau ?

Pour déterminer l'adresse IP du réseau, nous combinons l'adresse IP de n'importe quelle machine du réseau avec le masque de sous-réseau. Avec le masque 255.255.255.0 (ou /24 en notation CIDR), les trois premiers octets de l'adresse IP définissent le réseau, et le dernier octet est réservé pour les hôtes sur ce réseau.

En utilisant l'adresse IP du PC0 (192.168.10.6) comme exemple :

Adresse IP : 192.168.10.6

Masque: 255.255.255.0

Adresse réseau: 192.168.10.0

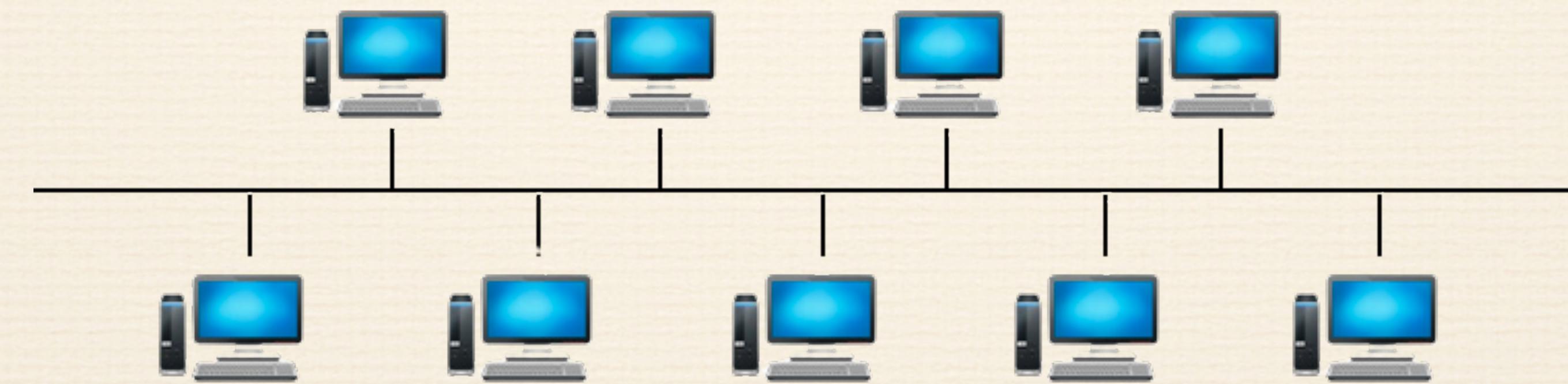
L'adresse IP du réseau est donc 192.168.10.0.

Combien de machines peut-on brancher sur le réseau ?

Avec un masque de sous-réseau de 255.255.255.0 (ou /24), il y a 256 adresses possibles ($2^8 = 256$). Cependant, nous devons soustraire 2 de ce total :

- 1 pour l'adresse réseau (192.168.10.0 dans ce cas).
- 1 pour l'adresse de diffusion.

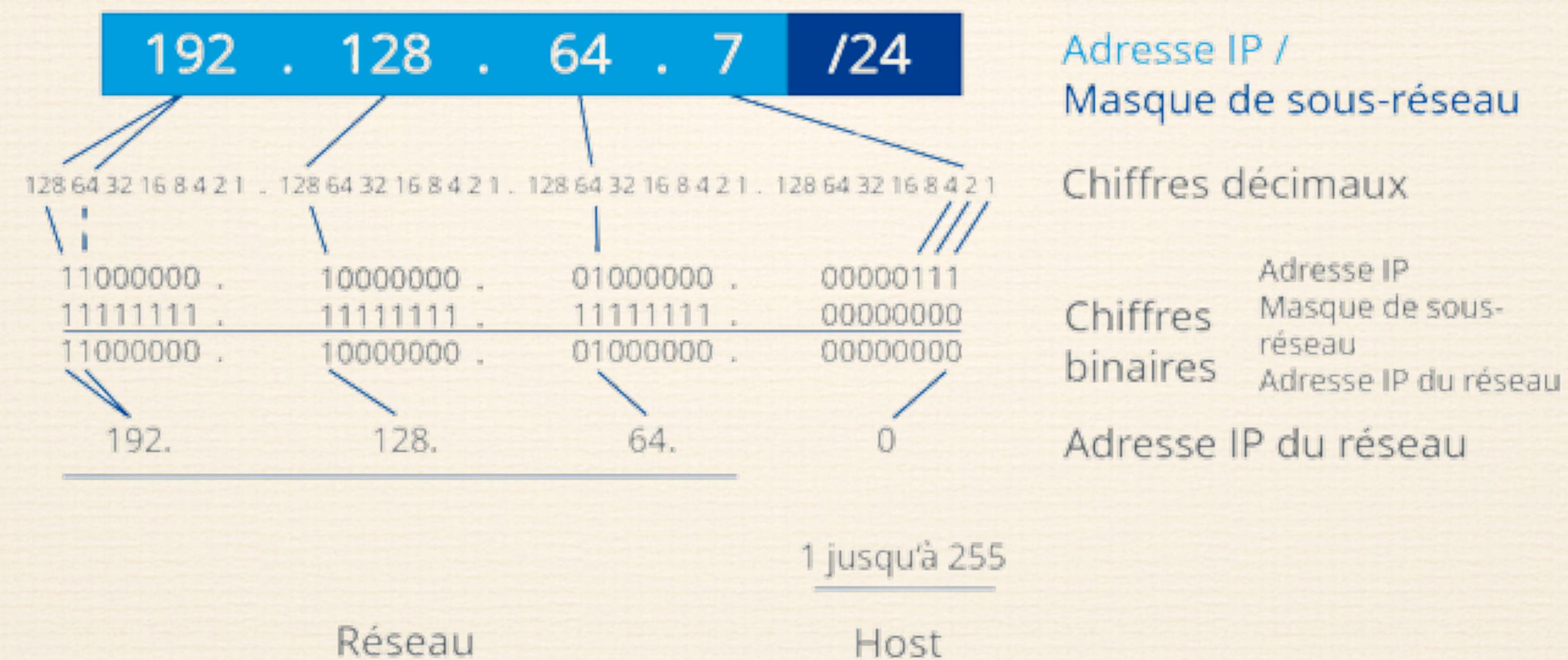
Ce qui nous donne 254 adresses utilisables pour les hôtes. Ainsi, 254 machines peuvent être connectées à ce réseau.



Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion est l'adresse où tous les bits d'hôte sont définis sur 1. Pour un masque de 255.255.255.0, cela signifie que l'adresse de diffusion est 192.168.10.255.

Composition d'une adresse IPv4



IONOS

Comment convertir une adresse IP en binaire ?

Dans un premier temps, on divise l'adresse IP en octets :

Par exemple, pour l'adresse 145.32.59.24, nous avons les octets suivants : 145, 32, 59 et 6.

On convertit maintenant chaque octet en binaire :

1. Pour un octet donné, on le divise par 2.
2. On note le reste (0 ou 1). Si le résultat est un nombre entier alors = 0. Si le résultat est un nombre décimal alors = 1
3. On continue à diviser le quotient par 2 et on note le reste.
4. On répète cette opération jusqu'à ce que le quotient soit 0.
5. On écrit les restes de bas en haut et on lis la représentation binaire de la droite vers la gauche.
6. Si la représentation binaire a moins de 8 chiffres, on ajoute des zéros à gauche jusqu'à obtenir une représentation sur 8 bits.

Pour l'adresse IP 145.32.59.24

145 en binaire :

$$145 \div 2 = 72 \text{ reste } 1$$

$$72 \div 2 = 36 \text{ reste } 0$$

$$36 \div 2 = 18 \text{ reste } 0$$

$$18 \div 2 = 9 \text{ reste } 0$$

$$9 \div 2 = 4 \text{ reste } 1$$

$$4 \div 2 = 2 \text{ reste } 0$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$



En écrivant les restes de bas en haut, nous obtenons **10010001**.

Pour l'adresse IP 145.32.59.24

32 en binaire :

$$32 \div 2 = 16 \text{ reste } 0$$

$$16 \div 2 = 8 \text{ reste } 0$$

$$8 \div 2 = 4 \text{ reste } 0$$



$$4 \div 2 = 2 \text{ reste } 0$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$

Avec les zéros de remplissage à gauche pour obtenir 8 bits, nous avons **00100000**.

Pour l'adresse IP 145.32.59.24

59 en binaire :

$$59 \div 2 = 29 \text{ reste } 1$$

$$29 \div 2 = 14 \text{ reste } 1$$

$$14 \div 2 = 7 \text{ reste } 0$$

$$7 \div 2 = 3 \text{ reste } 1$$

$$3 \div 2 = 1 \text{ reste } 1$$

$$1 \div 2 = 0 \text{ reste } 1$$



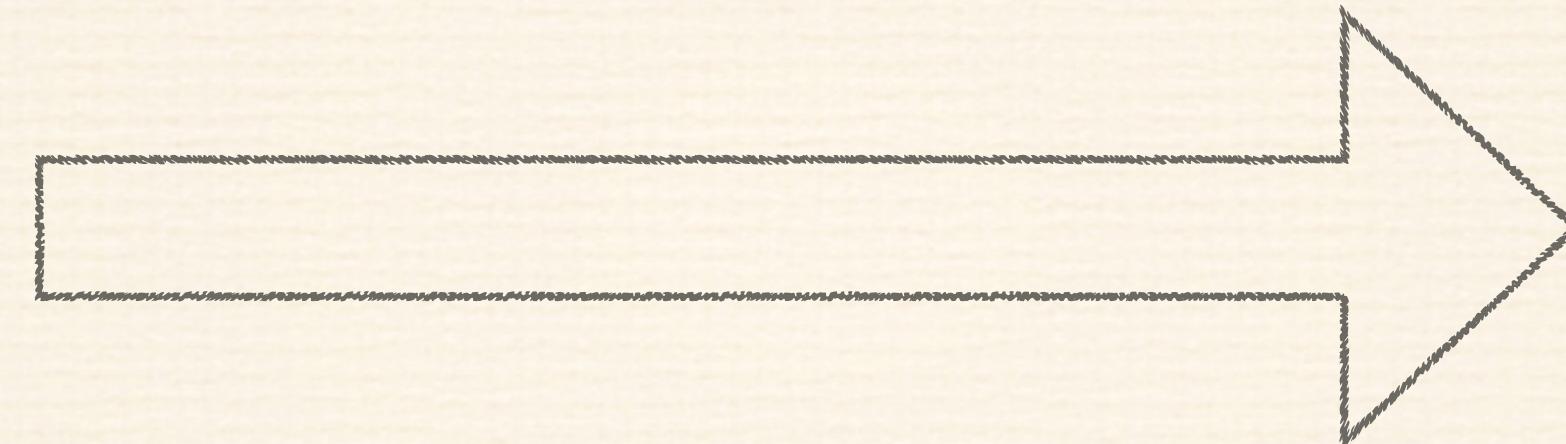
En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons
00111011.

Pour l'adresse IP 145.32.59.24

24 en binaire :

$$24 \div 2 = 12 \text{ reste } 0$$

$$12 \div 2 = 6 \text{ reste } 0$$



$$6 \div 2 = 3 \text{ reste } 0$$

$$3 \div 2 = 1 \text{ reste } 1$$

$$1 \div 2 = 0 \text{ reste } 1$$

En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons **00011000**.

En combinant tout cela, l'adresse IP 145.32.59.24 en binaire est :

10010001.00100000.00111011.00011000.

Pour l'adresse IP **200.42.129.16**

200 en binaire :

$$200 \div 2 = 100 \text{ reste } 0$$

$$100 \div 2 = 50 \text{ reste } 0$$

$$50 \div 2 = 25 \text{ reste } 0$$

$$25 \div 2 = 12 \text{ reste } 1$$

$$12 \div 2 = 6 \text{ reste } 0$$

$$6 \div 2 = 3 \text{ reste } 0$$

$$3 \div 2 = 1 \text{ reste } 1$$

$$1 \div 2 = 0 \text{ reste } 1$$



En écrivant les restes de bas en haut, nous obtenons **11001000**.

Pour l'adresse IP 200.42.129.16

42 en binaire :

$$42 \div 2 = 21 \text{ reste } 0$$

$$21 \div 2 = 10 \text{ reste } 1$$

$$10 \div 2 = 5 \text{ reste } 0$$



$$5 \div 2 = 2 \text{ reste } 1$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$

En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons **00101010**.

Pour l'adresse IP 200.42.129.16

129 en binaire :

$$129 \div 2 = 64 \text{ reste } 1$$

$$64 \div 2 = 32 \text{ reste } 0$$

$$32 \div 2 = 16 \text{ reste } 0$$

$$16 \div 2 = 8 \text{ reste } 0$$

$$8 \div 2 = 4 \text{ reste } 0$$

$$4 \div 2 = 2 \text{ reste } 0$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$



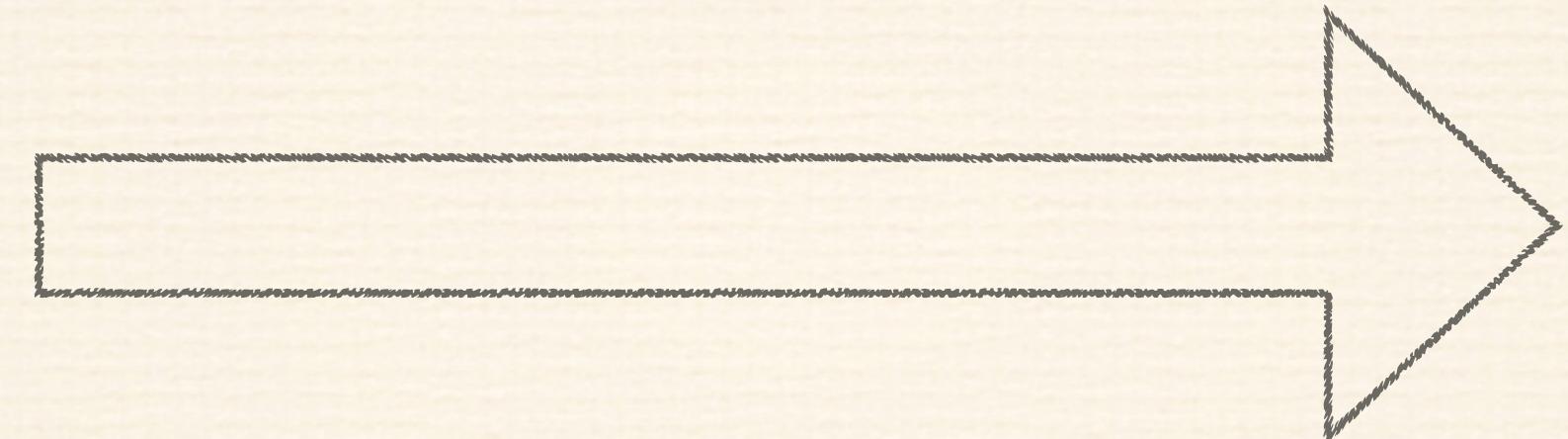
En écrivant les restes de bas en haut, nous obtenons **10000001**.

Pour l'adresse IP 200.42.129.16

16 en binaire :

$$16 \div 2 = 8 \text{ reste } 0$$

$$8 \div 2 = 4 \text{ reste } 0$$



$$4 \div 2 = 2 \text{ reste } 0$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$

En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons **00010000**. En combinant tout cela, l'adresse IP 200.42.129.16 en binaire est :

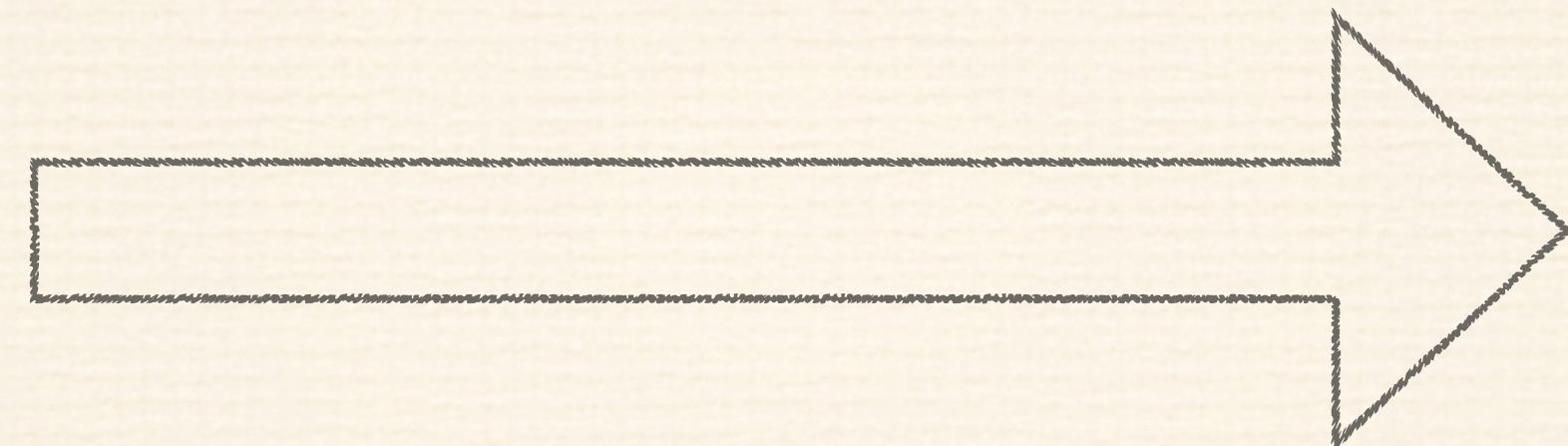
11001000.00101010.1000001.00010000.

Pour l'adresse IP 14.82.19.54

14 en binaire :

$$14 \div 2 = 7 \text{ reste } 0$$

$$7 \div 2 = 3 \text{ reste } 1$$



$$3 \div 2 = 1 \text{ reste } 1$$

$$1 \div 2 = 0 \text{ reste } 1$$

En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons **00001110**.

Pour l'adresse IP 14.**82**.19.54

82 en binaire :

$$82 \div 2 = 41 \text{ reste } 0$$

$$41 \div 2 = 20 \text{ reste } 1$$

$$20 \div 2 = 10 \text{ reste } 0$$

$$10 \div 2 = 5 \text{ reste } 0$$

$$5 \div 2 = 2 \text{ reste } 1$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$



En écrivant les restes de bas en haut, nous obtenons **01010010**.

Pour l'adresse IP 14.82.19.54

19 en binaire :

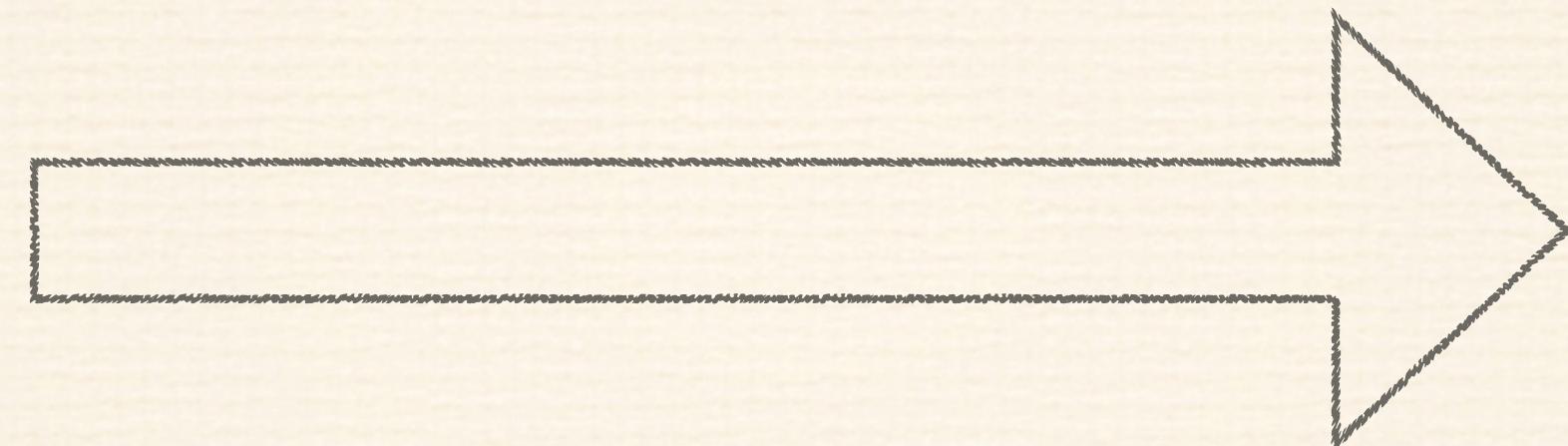
$$19 \div 2 = 9 \text{ reste } 1$$

$$9 \div 2 = 4 \text{ reste } 1$$

$$4 \div 2 = 2 \text{ reste } 0$$

$$2 \div 2 = 1 \text{ reste } 0$$

$$1 \div 2 = 0 \text{ reste } 1$$



En écrivant les restes de bas en haut et en ajoutant les zéros nécessaires pour obtenir 8 bits, nous avons **00010011**.

Pour l'adresse IP 14.82.19.54

54 en binaire :

$$54 \div 2 = 27 \text{ reste } 0$$

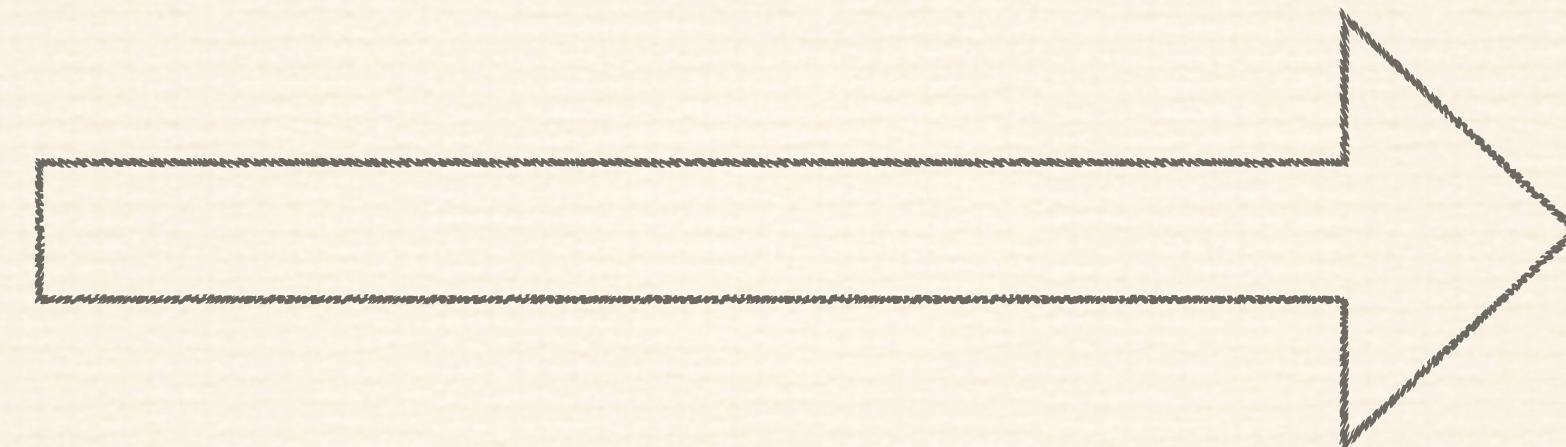
$$27 \div 2 = 13 \text{ reste } 1$$

$$13 \div 2 = 6 \text{ reste } 1$$

$$6 \div 2 = 3 \text{ reste } 0$$

$$3 \div 2 = 1 \text{ reste } 1$$

$$1 \div 2 = 0 \text{ reste } 1$$



En écrivant les restes de bas en haut, nous obtenons **00110110**. En combinant tout cela, l'adresse IP 14.82.19.54 en binaire est : **00001110.01010010.00010011.00110110**.

Qu'est ce que le rootage ?

Dans le contexte des réseaux informatiques, le "rootage" fait référence à l'obtention de droits d'accès de niveau "root" ou administrateur sur un dispositif réseau (comme un routeur, un commutateur ou un serveur). Ce processus permet à l'utilisateur de :

- **Contrôler entièrement** le dispositif, outrepassant les configurations par défaut ou les restrictions de sécurité.
- **Modifier les configurations** pour rediriger le trafic, ouvrir ou fermer des ports, et ajuster d'autres paramètres du réseau.
- **Installer des logiciels** ou des firmwares personnalisés.

Le rootage dans le contexte réseau peut être utilisé à des fins légitimes, comme la personnalisation ou l'optimisation, mais il peut aussi être exploité à des fins malveillantes si effectué sans autorisation.

Qu'est ce qu'un Gateway ?

En informatique réseau, une "gateway" (ou passerelle en français) est un dispositif qui fait le lien entre deux réseaux ayant des protocoles ou des architectures différents. Elle permet à ces réseaux de communiquer entre eux. De manière concise :

- **Liaison entre réseaux** : Une gateway connecte généralement un réseau local (LAN) à Internet ou à un autre LAN.
- **Traduction de protocoles** : Elle peut convertir des données d'un protocole à un autre, facilitant la communication entre des réseaux incompatibles.
- **Routage** : Elle dirige les paquets de données vers leur destination appropriée, soit à l'intérieur du LAN, soit vers un autre réseau.

Dans de nombreux contextes domestiques, le terme "gateway" est souvent utilisé pour désigner le routeur ou le modem qui connecte un réseau local à Internet

Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network, ou Réseau Privé Virtuel en français) en informatique réseau est une technologie qui permet à un utilisateur de créer une connexion sécurisée et cryptée sur un réseau public, généralement Internet, pour accéder à des ressources distantes comme s'il était sur un réseau local. De manière concise :

- **Sécurité** : Le VPN crypte les données pour garantir leur confidentialité pendant la transmission.
- **Anonymat** : Il masque l'adresse IP de l'utilisateur, le rendant difficile à tracer en ligne.
- **Accès aux ressources distantes** : Permet aux utilisateurs d'accéder à des réseaux et services bloqués géographiquement ou de se connecter à un réseau d'entreprise de n'importe où.

Un VPN est souvent utilisé pour la protection de la vie privée, la sécurité en ligne et pour contourner les restrictions géographiques.

Qu'est-ce qu'un DNS ?

Le DNS (Domain Name System, ou Système de Noms de Domaine en français) en informatique réseau est un système servant à traduire des noms de domaine faciles à mémoriser (comme « www. valuxsurlinux.com ») en adresses IP numériques (comme "192.0.2.1") utilisées pour identifier et localiser des dispositifs sur un réseau. De manière concise :

- **Traduction** : Convertit des noms de domaine en adresses IP et vice-versa.
- **Hiérarchique** : Organisé en plusieurs niveaux, avec des serveurs DNS racine, de top niveau (TLD) et d'autorité.
- **Fondamental pour la navigation web** : Permet aux utilisateurs d'accéder à des sites web en utilisant des noms de domaine plutôt que des adresses IP difficilement mémorisables.

Le DNS facilite la navigation sur Internet en permettant aux gens d'utiliser des noms de domaine faciles à retenir au lieu de se souvenir des adresses IP numériques.

Fin



CISCO Runtrack Réseau