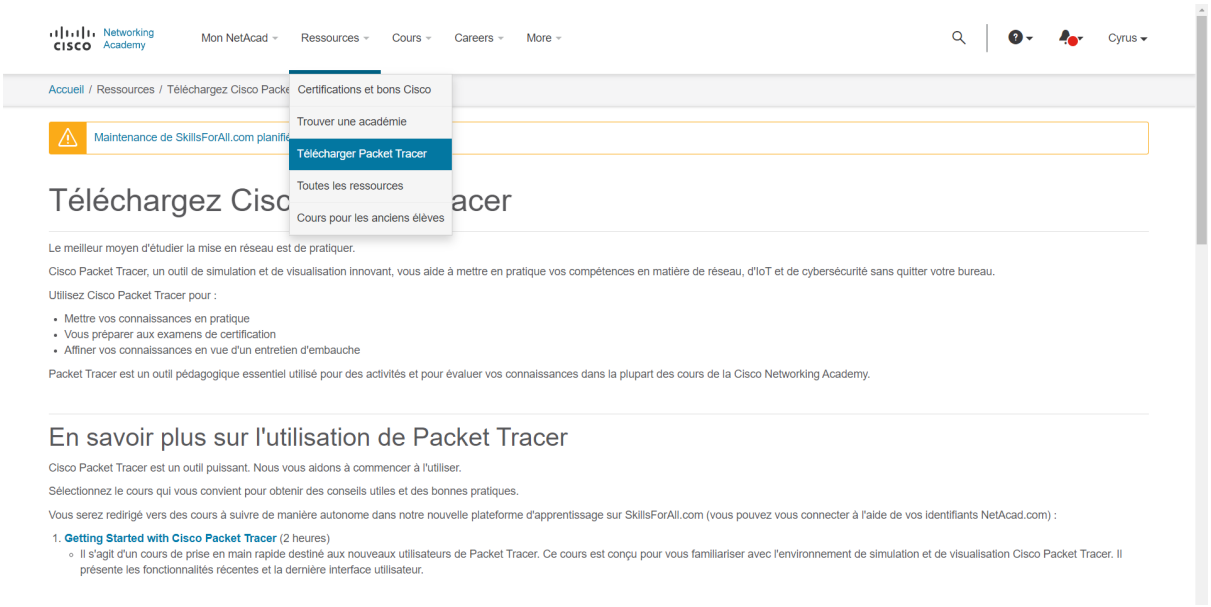
Dehghan Cyrus

Runtrack Réseau

SOMMAIRE

Job 01

Télécharger Cisco packet tracer



Job 02

→Qu'est ce qu'un réseau :

Un réseau est un ensemble de dispositifs, d'objets ou d'entités interconnectés qui communiquent entre eux. Ces connexions peuvent être physiques (câbles, fibres optiques, ondes radio, etc.) ou virtuelles (connexions logicielles via Internet ou d'autres protocoles de communication). Les réseaux sont essentiels pour permettre le transfert de données, d'informations, de ressources et de services d'un point à un autre.

→A quoi sert un réseau informatique :

Les réseaux informatiques permettent la communication dans tous les domaines ; professionnel, divertissement et recherche. Internet, la recherche en ligne, le courrier électronique, le partage d'audio et de vidéo, le commerce en ligne, le live-streaming et les réseaux sociaux existent tous grâce aux réseaux informatiques.

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

La construction d'un réseau nécessite :

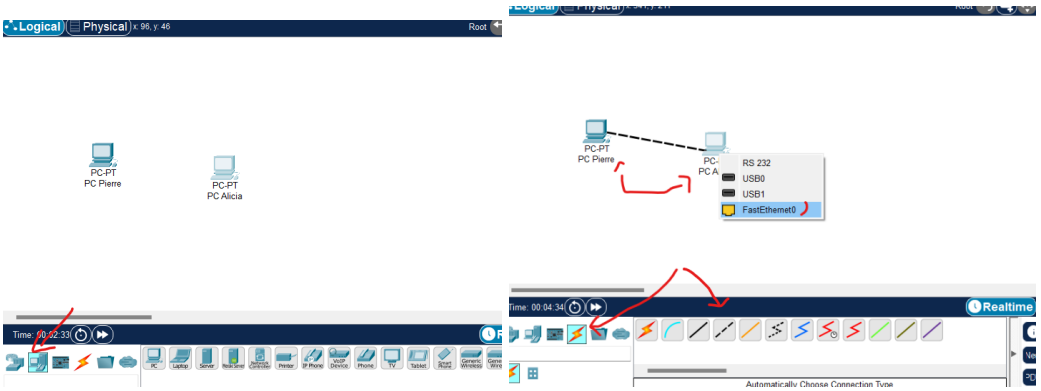
- Des ordinateurs, ce sont les points d'extrémité du réseau. Ils accèdent aux ressources partagées, envoient et reçoivent des données, et exécutent des applications réseau.
- Un Routeur ou Routeur sans fil, c'est un dispositif central du réseau qui interconnecte différentes parties du réseau. Il dirige le trafic entre les

réseaux locaux (LAN) et les réseaux étendus (WAN). Il attribue des adresses IP aux dispositifs, gère la table de routage, et fournit des services de pare-feu et de sécurité. Le routeur sans fil combine les fonctions d'un routeur standard avec un point d'accès Wi-Fi pour permettre la connectivité sans fil des dispositifs.

- Câbles réseau, ils sont utilisés pour connecter physiquement les dispositifs au sein d'un réseau. Ils transportent les données d'un point à un autre.
- Point d'accès WiFi, permet aux dispositifs compatibles Wi-Fi de se connecter sans fil au réseau.
- Serveurs, ce sont des ordinateurs spécialisés qui fournissent des services réseau. Il existe différents types de serveurs, notamment des serveurs de fichiers, de messagerie, de bases de données, de DNS (Domain Name System), etc. Ils stockent et gèrent les données et les ressources partagées.
- Firewall, le pare-feu est un dispositif de sécurité qui contrôle et filtre le trafic réseau entrant et sortant pour protéger le réseau contre les menaces potentielles.
- Composants d'interconnexion, ces composants facilitent la connexion physique des câbles réseau aux dispositifs et aux infrastructures du réseau.

Job 03

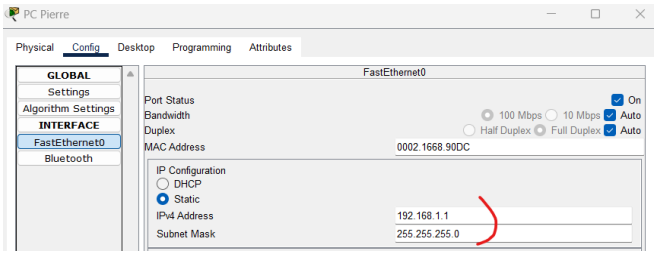
Une fois les deux PC ajoutés et renommés, les relier en connexion **Fast Ethernet** grâce au câble Copper Cross-Over

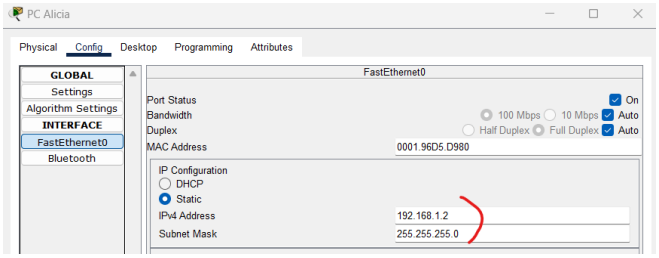


→Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

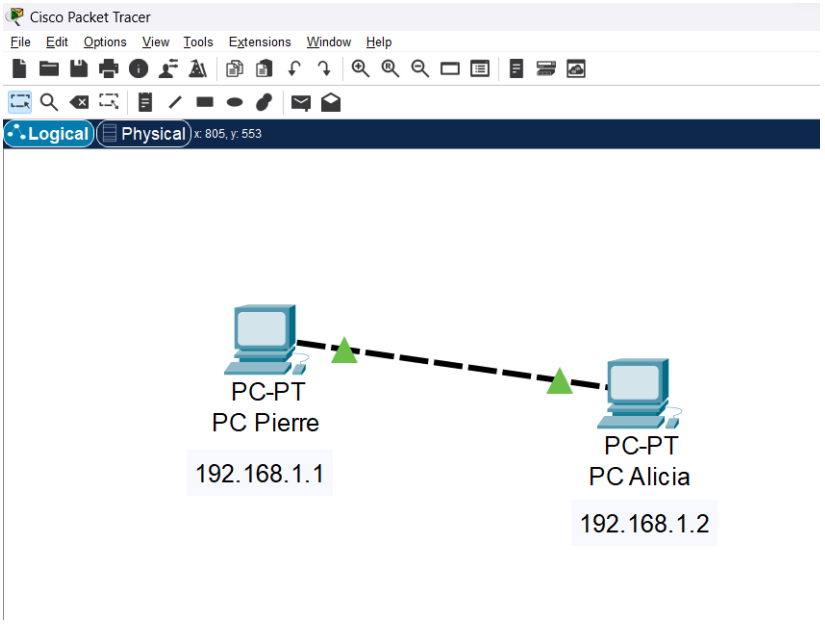
J'ai choisi le câble Copper Cross-Over car les câbles croisés sont souvent utilisés car le signal envoyé sur le câble TX depuis l'ordinateur 1 (PC Pierre) peut être reçu sur le câble RX de l'ordinateur 2 (PC Alicia).

Job 04





Pour ajouter l'adresse IP ainsi que le masque de sous-réseau il faut aller dans les paramètres du PC → Config → FastEthernet0 → rentrer les informations dans IPv4 et Subnet Mask.



Le résultat final.

→Qu'est-ce qu'une adresse IP :
Une adresse IP est un numéro d'identification unique attribué à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet.

→À quoi sert un IP :
Un IP sert à identifier les machines et à leur permettre de dialoguer entre elles, en acheminant des données et paquets sur Internet.

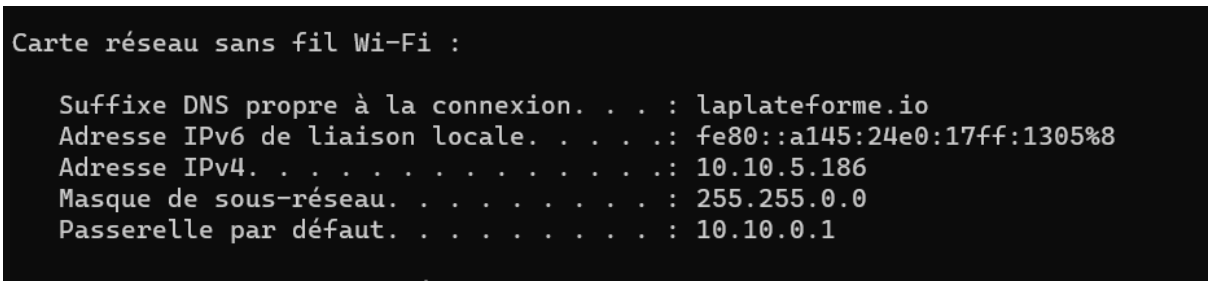
→Qu'est-ce qu'une adresse MAC :

Une adresse MAC (Media Access Control) est une adresse unique attribuée à chaque carte réseau ou adaptateur réseau, qu'il s'agisse d'une carte Ethernet filaire ou d'une carte Wi-Fi sans fil.

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

Les adresses IP publiques sont utilisées pour interagir avec Internet, alors que les IP privées fonctionnent quant à elles sur les réseaux locaux. Ces deux types d'adresses IP permettent aux appareils de communiquer entre eux.

→Quelle est l'adresse de ce réseau :



Aller dans le terminal et rentrer la commande *ipconfig*

Job 05

→Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines?
J'ai utilisé la ligne de commande ipconfig dans le terminal Prompt de PC Pierre (screen 1) puis dans celui de PC Alicia (screen 2).

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:16FF:FE68:90DC
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0
```

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::201:96FF:FED5:D980
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 0.0.0.0
```

Job 06

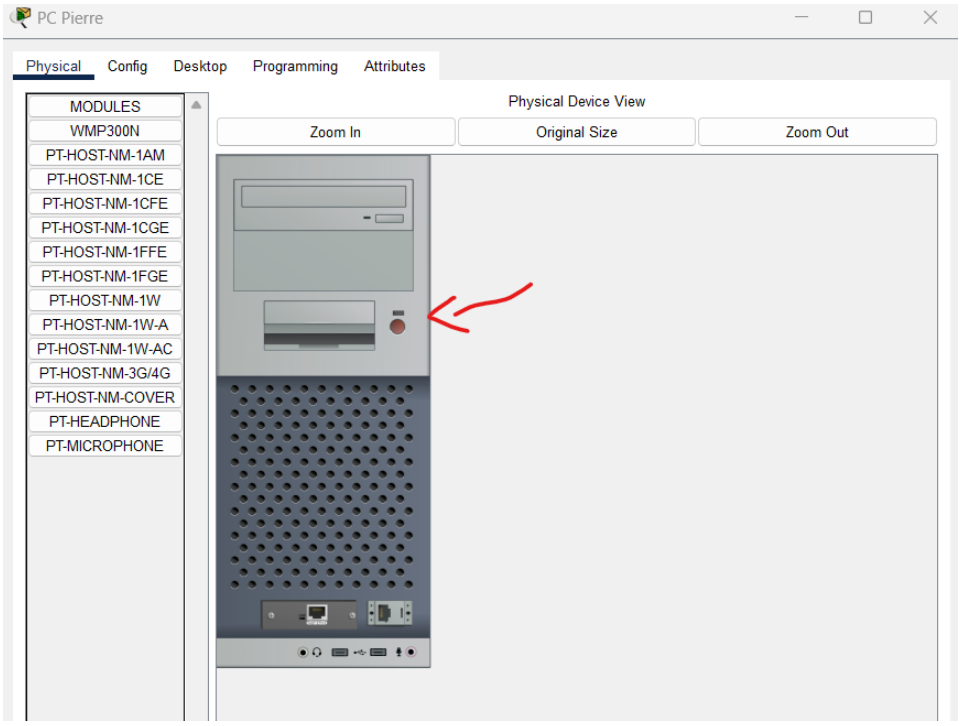
→Quelle est la commande permettant de Ping entre des PC ?
La commande pour ping est *ping+adresse ip de l'appareil a ping* dans le terminal Prompt de l'appareil qui effectue le ping.
Ci dessous sur le screen 1 PC Pierre effectue le ping vers PC Alicia, et sur le screen 2 PC Alicia effectue le ping vers PC Pierre.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

Job 07

On éteint le PC Pierre grâce au bouton indiqué sur le screen ci-dessous.



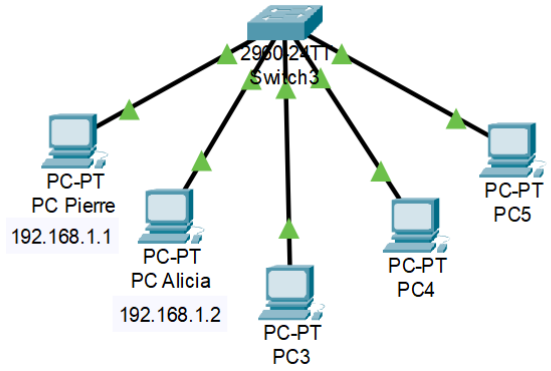
Ensuite on effectue le ping depuis PC Alicia vers PC Pierre (éteint) grâce a la commande dans *ping+adresse ip de l'appareil a ping* (screen ci-dessous).

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

→Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?
Non les Paquets envoyés (4) n'ont pas été reçus "*Lost = 4*" (screen ci-dessus).

→Expliquez pourquoi.
Le PC Pierre est éteint alors il n'est pas connecté au réseau donc le ping ne peut pas fonctionner et les paquets envoyés ne peuvent pas être reçus et sont donc perdus (screen ci-dessus).

Job 08




```
C:\> ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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

J'agrandis mon sous réseau en ajoutant un Switch et 3 autres PC à mes 2 actuels, je les relie ensuite en Fast Ethernet grâce au câble Copper Straight-Through (screen 1).
Je teste la commande ping sur le terminal Prompt pour vérifier si tous les appareils sont connectés (screen 2).

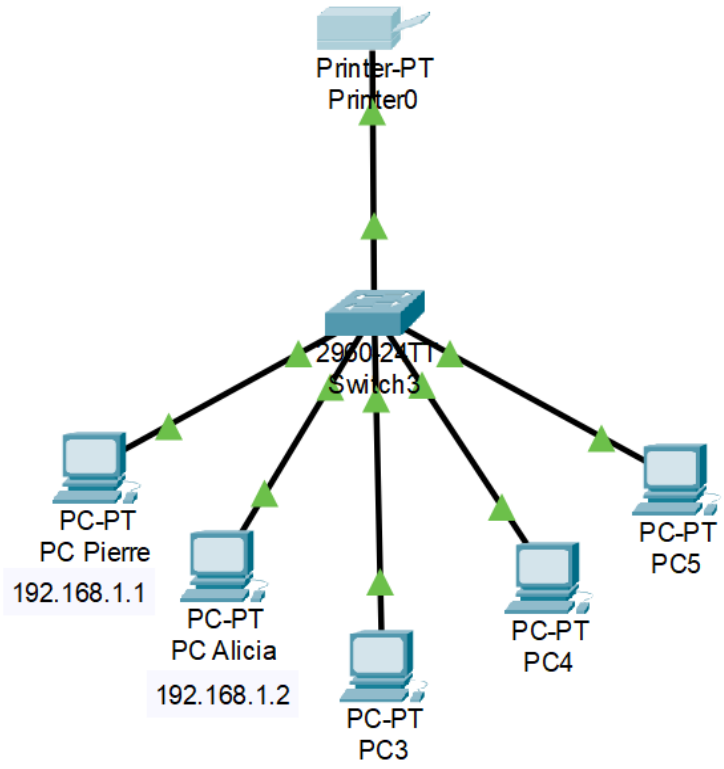
→Quelle est la différence entre un hub et un switch ?
La principale différence entre un hub et un swtich réside dans leur façon de gérer le trafic réseau, les Hubs diffusent les données à tous les ports, tandis que les switchs envoient les données uniquement aux ports concernés de manière sélective. Les switchs sont donc plus rapides et efficaces, ce qui les rend plus adaptés aux réseaux modernes.

→Comment fonctionne un hub et quels sont ses avantages et ses inconvénients?
Un hub fonctionne en répétant les données reçues a tous les appareils connectés, comme un amplificateur de signal (les données entrent et sont amplifiées à tous les ports). Ils sont peu coûteux mais créent un trafic réseau inutile.

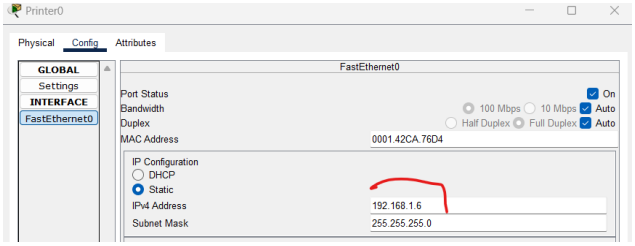
→Quels sont les avantages et inconvénients d'un switch ?
Un switch est un dispositif de liaison de données plus intelligent qu'un hub, il prend compte des adresses MAC (ce qui n'est pas le cas d'un Hub) et achemine les données sélectivement. Il transmet les données donc uniquement au port nécessaire et évite en grande partie le trafic réseau inutile. Ce qui rend un switch plus utilisé dans les réseaux modernes.

→Comment un switch gère-t-il le trafic réseau ?
Un switch est plus efficace en termes de bande passante car il transmet les données au port nécessaire uniquement ce qui minimise le trafic réseau inutile. Pour cela il crée une table d'adressage (MAC) pour savoir sur quel port se trouve chaque appareil en fonction de son adresse MAC.

Job 09



J'ajoute l'imprimante au réseau et je la relie au Switch avec un câble Copper Straight-Through (screen ci-dessus). Pour vérifier qu'elle est bien connectée j'attribue une adresse IPv4 (screen ci-dessous) et j'effectue un ping (screen ci-dessous).



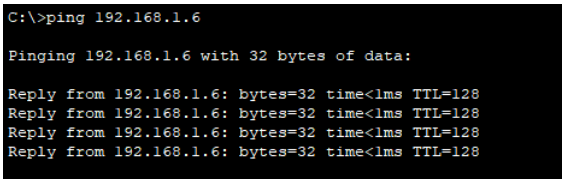
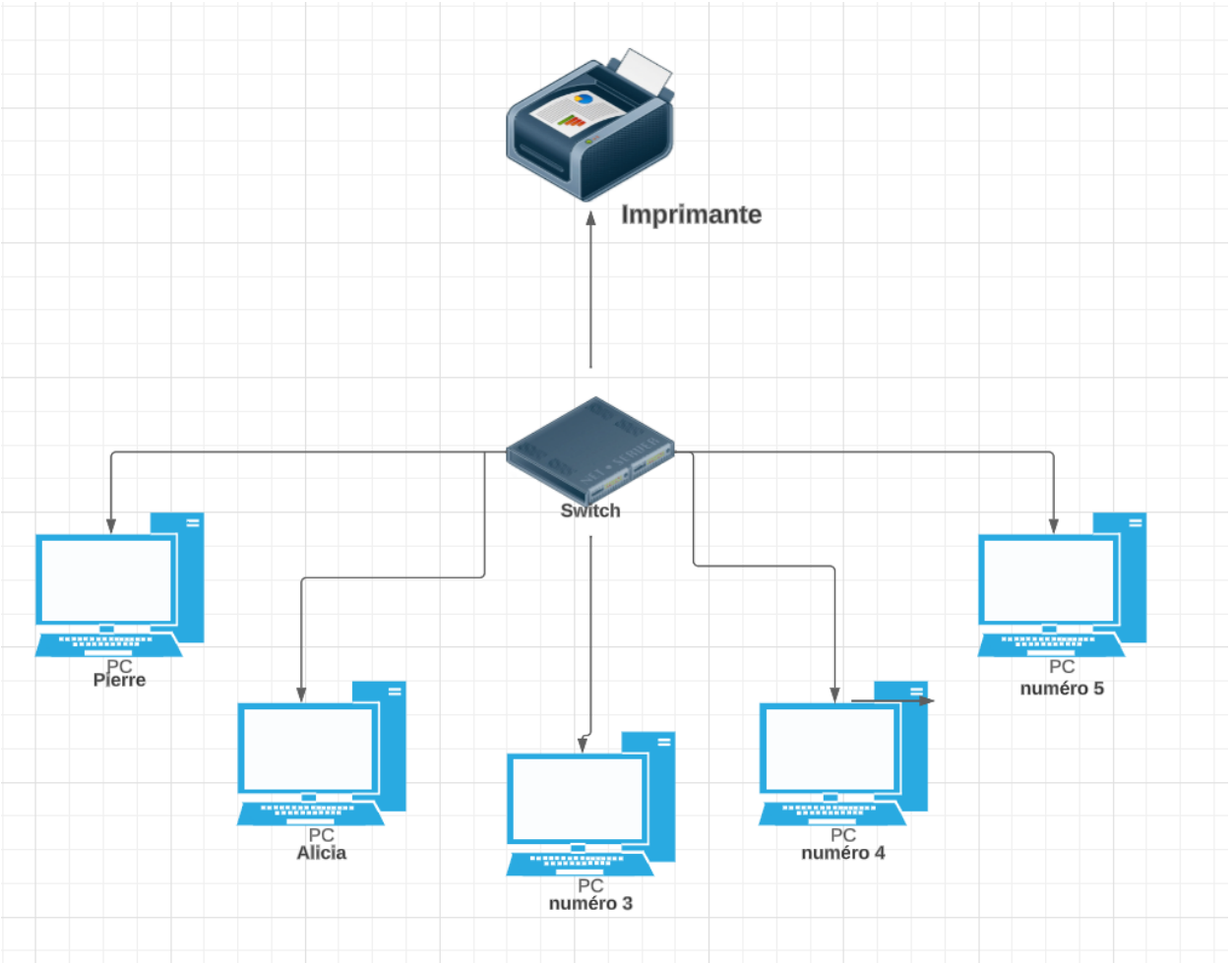


Schéma de mon réseau sur Lucidchart ci-dessous.

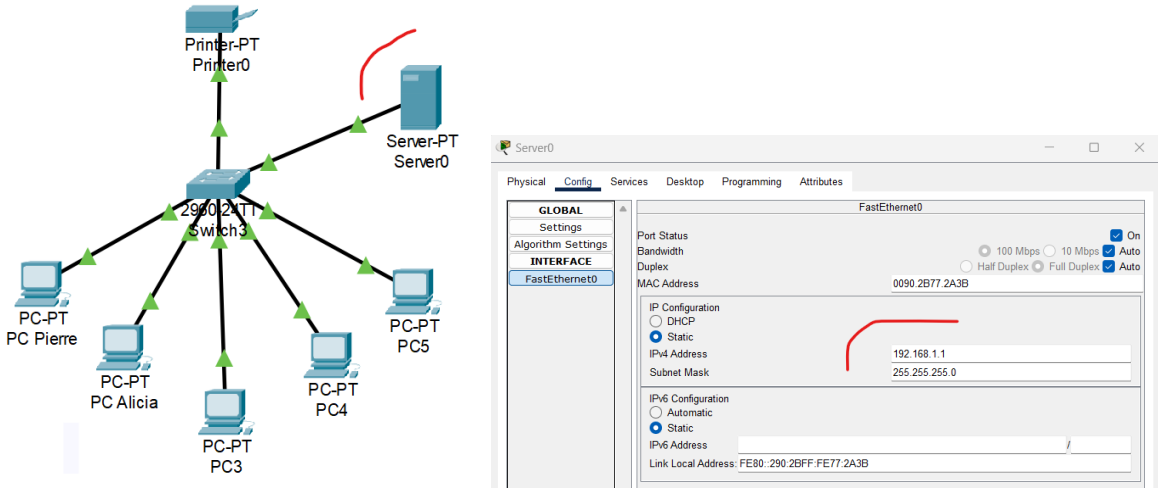


Les avantages de faire un schéma sont de faire travailler notre mémoire grâce aux informations visuelles, le schéma est également simplifié il permet donc une meilleure visualisation des éléments qui le composent et nous donne une vue d’ensemble grâce à l'utilisation d'éléments graphiques précis.

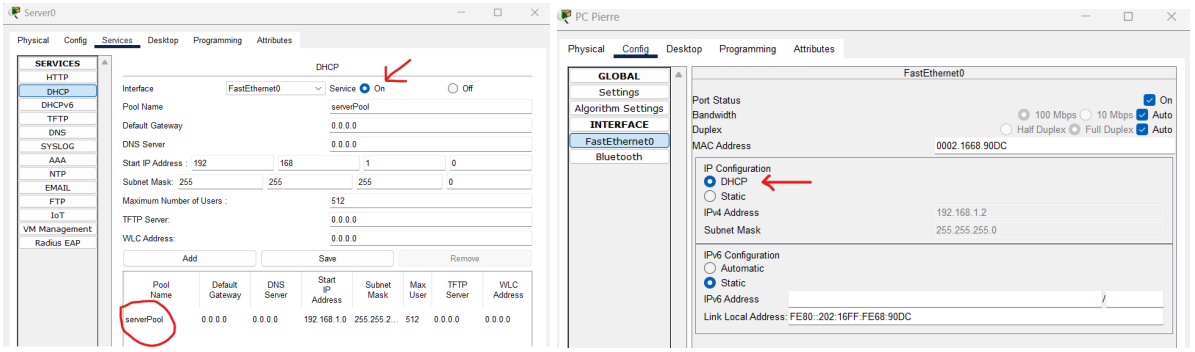
Job 10

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

L'adresse IP statique est configurée manuellement et reste constante, tandis que l'adresse IP attribuée par DHCP est assignée automatiquement par un serveur DHCP et peut changer chaque fois qu'un périphérique se connecte au réseau. Le choix entre les deux dépend des besoins spécifiques de votre réseau et de la facilité de gestion des adresses IP.



Ajouter un serveur et le relier avec un câble et lui attribuer une adresse ip au serveur (ci-dessus).



Une fois cela fait dans Services, configurer le Serveur pour qu'il attribue les adresses IP à chaque appareil, pour cela chaque appareil doit être configuré en DHCP (ci-dessous).

Job 11

sous-réseau 1	10.0.0.1	10.0.0.13	255.0.0.0
sous-réseau 2	10.0.0.14	10.0.0.44	255.0.0.0
sous-réseau 3	10.0.0.45	10.0.0.106	255.0.0.0
sous-réseau 4	10.0.0.76	10.0.0.137	255.0.0.0
sous-réseau 5	10.0.0.107	10.0.0.137	255.0.0.0
sous-réseau 6	10.0.0.138	10.0.0.168	255.0.0.0
sous-réseau 7	10.0.0.169	10.0.1.34	255.0.0.0
sous-réseau 8	10.0.1.35	10.0.1.155	255.0.0.0
sous-réseau 9	10.0.1.156	10.0.2.21	255.0.0.0
sous-réseau 10	10.0.2.22	10.0.2.142	255.0.0.0
sous-réseau 11	10.0.2.143	10.0.3.8	255.0.0.0
sous-réseau 12	10.0.3.9	10.0.3.169	255.0.0.0
sous-réseau 13	10.0.3.170	10.0.4.75	255.0.0.0
sous-réseau 14	10.0.4.76	10.0.4.236	255.0.0.0
sous-réseau 15	10.0.5..143	10.0.5.142	255.0.0.0
sous-réseau 16	10.0.5.143	10.0.6.48	255.0.0.0

→Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?
L'utilisation de l'adresse 10.0.0.0 de classe A pour les réseaux privés offre une grande flexibilité en termes de gestion des adresses IP et répond aux besoins de nombreux réseaux locaux, ce qui en fait un choix populaire pour les environnements privés et internes.

→Quelle est la différence entre les différents types d'adresses ?
Elles sont classées en 5 classes principales : A,B,C,D et E.
Les classes A,B et C sont utilisées pour les réseaux IPv4 tandis que les D et E ont des utilisations spéciales comme la multidiffusion, ou à des fins expérimentales et de recherche.

Job 12

Couche OSI	Descriptions de rôles	Matériels
Couche application	Cette couche est responsable de l'interface entre l'application utilisateur et le reste du modèle OSI. Elle gère les protocoles de haut niveau utilisés pour des applications telles que la messagerie électronique, la navigation web, etc.	HTTP (HTML), FTP, SSL/TLS
Couche 1 (Physique)	La couche physique s'occupe du transfert de bits bruts sur un support de transmission. Elle gère les caractéristiques matérielles, telles que le type de câble, la fibre optique, etc.	Fibre optique, câble RJ45
Couche 2 (Liaison de données)	Cette couche gère la communication entre des nœuds directement connectés. Elle divise les données en trames et gère les adresses MAC pour la livraison des trames.	Ethernet, Wi-Fi, cable RJ45
Couche 3 (Réseau)	La couche réseau est responsable du routage des données entre différents réseaux. Elle utilise des adresses IP pour diriger les paquets vers leur destination.	IPv4, IPv6, routeur
Couche 4 (Transport)	Cette couche assure la fiabilité et le contrôle du flux de bout en bout de la communication. Elle gère également la segmentation et le réassemblage des données.	TCP, UDP
Couche 5 (Session)	La couche de session établit, gère et termine les sessions de communication entre deux applications. Elle gère également la synchronisation entre les applications.	PPTP
Couche 6 (Présentation)	La couche de présentation gère la traduction, la compression et le chiffrement des données pour assurer que les applications des couches supérieures puissent interpréter correctement les informations. SSL/TLS, HTML (pour la présentation)	SSL/TLS, HTML

Job 13

→Quelle est l'architecture de ce réseau ?
L'architecture est une architecture de classe C masque de sous-réseau par défaut de 255.255.255.0 et leur premier octet est compris entre 192 et 223.

→Indiquer quelle est l'adresse IP du réseau ?
L'adresse IP du réseau est 192.168.10 car le masque de sous réseau 255.255.255.0 (les 3 premiers octets de l'adresse IP sont réservés pour le réseau, et le dernier pour les hôtes).

→Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?
On peut brancher 253 machines sur ce réseau.

→Quelle est l'adresse de diffusion de ce réseau ?
L'adresse de diffusion de ce réseau est 192.168.10.255, car tous les bits d'hôtes sont définis à 1 dans le dernier octet (255 en décimal), ce qui signifie que c'est l'adresse de diffusion pour le réseau 192.168.10.0/24.

Job 14

Convertissez les adresses IP suivantes en binaires :
● 145.32.59.24
145 en binaire : 10010001
32 en binaire : 00100000
59 en binaire : 00111011
24 en binaire : 00011000
Donc, 145.32.59.24 en binaire est : 10010001.00100000.00111011.00011000

● 200.42.129.16
200 en binaire : 11001000
42 en binaire : 00101010
129 en binaire : 10000001
16 en binaire : 00010000
Donc, 200.42.129.16 en binaire est : 11001000.00101010.10000001.00010000

● 14.82.19.54
14 en binaire : 00001110
82 en binaire : 01010010
19 en binaire : 00010011
54 en binaire : 00110110
Donc, 14.82.19.54 en binaire est : 00001110.01010010.00010011.00110110

Job 15

→***Qu'est-ce que le routage ?***
Le routage est le processus de sélection du chemin optimal pour acheminer des données d'un point à un autre à travers un réseau, en particulier sur Internet. Il s'agit de la décision prise par des routeurs et des commutateurs pour diriger le trafic vers sa destination.

→***Qu'est-ce qu'un gateway ?***
Un gateway est un périphérique ou un logiciel qui relie deux réseaux informatiques différents, permettant ainsi la communication entre eux. Les gateways jouent un rôle essentiel dans le transfert de données entre des réseaux hétérogènes, en convertissant parfois les protocoles de communication pour assurer la compatibilité.

→***Qu'est-ce qu'un VPN ?***
Un Virtual Private Network ou VPN est un réseau privé virtuel qui permet de sécuriser et d'anonymiser la connexion à Internet. Il crée un tunnel chiffré entre l'ordinateur ou le dispositif de l'utilisateur et un serveur VPN distant, masquant ainsi l'adresse IP de l'utilisateur. Les VPN sont largement utilisés pour renforcer la sécurité en ligne, protéger la vie privée, accéder à des ressources réseau distantes de manière sécurisée, contourner la censure et géoblocage, etc.

→***Qu'est-ce qu'un DNS ?***
Domain Name System ou DNS est un système de noms de domaine utilisé pour traduire les noms de domaine en adresses IP numériques compréhensibles par les ordinateurs. Il agit comme un annuaire pour le réseau, facilitant la localisation des serveurs et des services en fonction des noms de domaine.