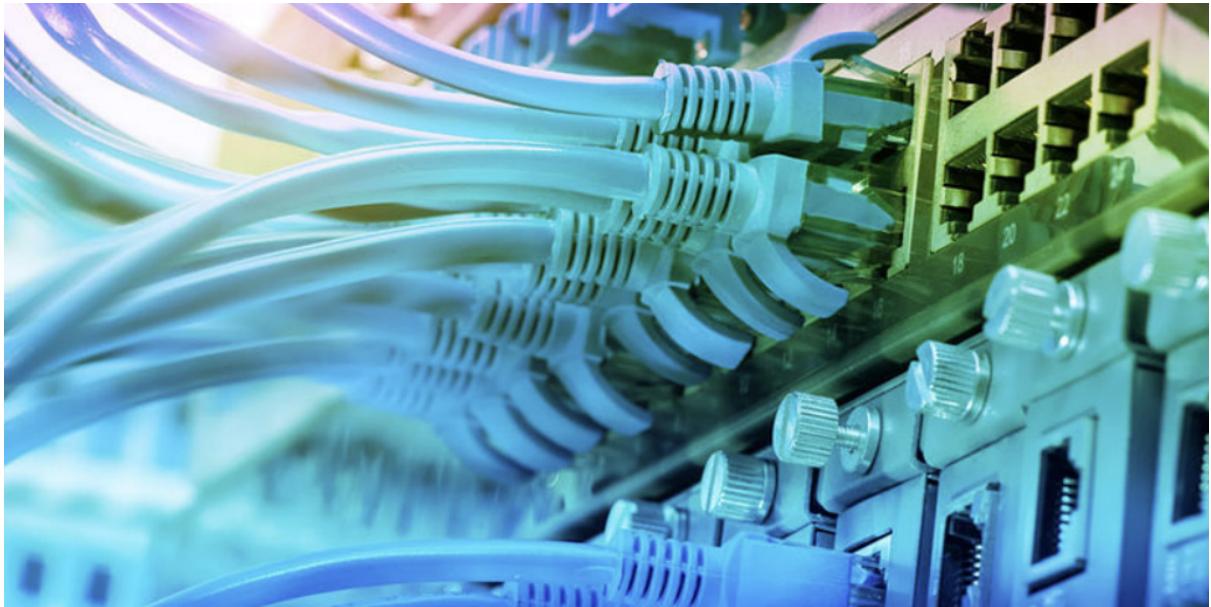


Runtrack Réseau



Job 01 :

On commence par télécharger notre logiciel Cisco, qui va nous permettre de continuer de travailler l'exercice, pour cela il suffit de le télécharger via ce lien [Télécharger la version 64 bits](#), qui va nous installer Packet Tracer.

Job 02 :

Qu'est ce qu'un réseau ?

Un réseau est un ensemble d'entités interconnectées qui communiquent entre elles. Ces entités peuvent être des ordinateurs, des appareils électroniques...

Les réseaux sont utilisés pour permettre la transmission de données, de ressources et d'informations d'un point à un autre. En général, les réseaux permettent aux entités de partager des ressources, de collaborer, de communiquer et d'accéder à des informations de manière plus efficace, ce qui les rend cruciaux dans le monde moderne.

À quoi sert un réseau informatique ?

Un réseau informatique sert à connecter des ordinateurs, des périphériques et des systèmes informatiques pour permettre la communication, le partage de ressources, l'accès à l'information et la collaboration.

Les réseaux informatiques permettent de partager des ressources telles que des imprimantes, des disques durs, des scanners, des fichiers et des applications. Cela permet aux utilisateurs d'accéder aux ressources partagées à partir de n'importe quel endroit du réseau.

Les réseaux facilitent la communication entre les utilisateurs. Les utilisateurs peuvent échanger des informations rapidement et efficacement.

De nombreux réseaux informatiques sont connectés à Internet, ce qui permet aux utilisateurs d'accéder à une vaste quantité d'informations en ligne, de naviguer sur le Web, de consulter des courriels, de télécharger des fichiers, etc.

Les réseaux permettent de stocker des données de manière centralisée. Les utilisateurs peuvent accéder aux données stockées sur des serveurs depuis n'importe quel appareil connecté au réseau.

Gestion de systèmes : Les administrateurs réseau utilisent les réseaux pour surveiller, gérer et maintenir les systèmes informatiques. Ils peuvent effectuer des mises à jour, résoudre des problèmes, gérer la sécurité et les autorisations, etc.

En somme, les réseaux informatiques sont un élément essentiel de l'infrastructure technologique moderne, facilitant la communication, la collaboration, le partage de ressources et l'accès à l'information, ce qui les rend indispensables dans les entreprises, les établissements d'enseignement, les foyers et de nombreux autres environnements.

Quel matériel avons-nous besoin pour construire un réseau ?

Pour construire un réseau informatique, on a besoin de divers composants matériels pour établir les connexions et permettre la communication entre les appareils. Voici les composants matériels de base nécessaires pour construire un réseau :

- Dispositifs réseau

Routeur : Un routeur relie différents réseaux et dirige le trafic entre eux. Il est essentiel pour la connexion à Internet et le routage du trafic au sein du réseau local.

Commutateur : Les commutateurs permettent de relier plusieurs appareils au sein du réseau local. Ils dirigent le trafic de manière plus efficace que les hubs en envoyant les données uniquement là où elles sont nécessaires.

- Câbles

Câbles Ethernet : Les câbles Ethernet sont utilisés pour connecter les ordinateurs, les commutateurs, les routeurs, etc.

- Points d'accès sans fil

Points d'accès sans fil : Les AP Wi-Fi permettent la connectivité sans fil, ils sont utilisés pour créer un réseau local sans fil

- Modems

Modem DSL : Un modem est nécessaire pour établir la connexion à Internet via le fournisseur de services Internet. Il peut être intégré au routeur dans certains cas.

- Serveurs

Serveurs : Les serveurs sont des ordinateurs spécialement configurés pour fournir des services et des ressources au réseau. Ils peuvent être utilisés pour le stockage de données, le partage de fichiers, l'hébergement de sites web, la messagerie électronique, etc.

- Matériel de sécurité

Firewalls : Les pare-feu protègent le réseau en contrôlant le trafic entrant et sortant pour bloquer les menaces potentielles.

Systèmes de détection d'intrusion (IDS) : Les IDS surveillent le réseau à la recherche d'activités suspectes.

Systèmes de prévention des intrusions (IPS) : Les IPS identifient et bloquent les menaces potentielles.

- périphériques réseau

Imprimantes réseau : Les imprimantes équipées de capacités réseau peuvent être partagées sur le réseau.

Caméras IP : Les caméras de surveillance réseau utilisent le réseau pour la diffusion de vidéos et la gestion à distance.

Scanners réseau : Les scanners réseau permettent de numériser des documents directement vers des emplacements réseau.

- Alimentation électrique :

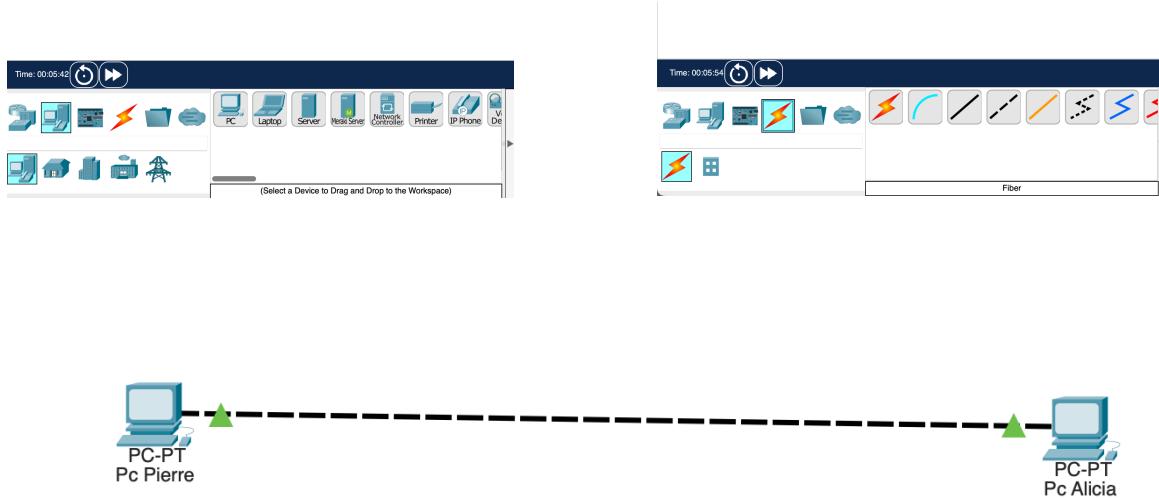
Il est important de fournir une alimentation électrique adéquate à tous les composants du réseau, y compris les onduleurs pour maintenir la disponibilité en cas de coupure de courant.

- Câblage structuré :

Le câblage structuré se compose de câbles Ethernet, de prises murales, de panneaux de brassage, de connecteurs, de goulottes de câbles, etc., et assure une organisation propre et efficace du câblage du réseau.

Job 03 :

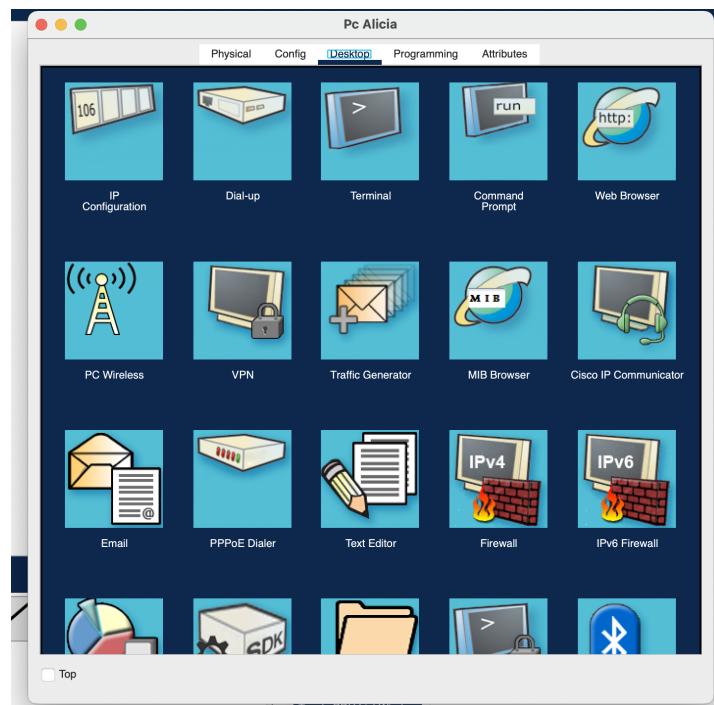
On va à présent rentrer directement dans notre exercice, et pour cela, nous allons ouvrir l'application que nous venons tout juste de télécharger. À présent nous devons connecter 2 PCs via un câble, on renomme nos PCs; Pc de Pierre et Pc d'Alicia.



En sélectionnant nos 2 PCs sur l'interface, il nous suffit de les lier via un câble, on a donc privilégié l'utilisation d'un câble croisé, car il est plus efficace que d'autres lorsqu'il est question de relier 2 ordinateurs entre eux.

Job 04 :

Maintenant que nos 2 PCs sont connectés, on va devoir maintenant les configurer, nous allons donc attribuer à chacun une adresse IP, celui de Pierre aura comme adresse 192.168.1.1 et celui d'Alicia aura comme adresse 192.168.1.2



Pc Pierre

Physical Config Desktop Programming Attributes

IP Configuration

Interface	FastEthernet0	X
IP Configuration		
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.1	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	
DNS Server	0.0.0.0	
IPv6 Configuration		
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static	/
IPv6 Address		
Link Local Address	FE80::2D0:BCFF:FEFF:B45C	
Default Gateway		
DNS Server		
802.1X		
<input type="checkbox"/> Use 802.1X Security		
Authentication	MD5	
Username		
Password		
<input type="checkbox"/> Top		

Pc Alicia

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

DHCP Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IP v6 Configuration

Automatic Static

IPv6 Address /

Link Local Address FE80::210:1FF:FE84:DCE7

Default Gateway

DNS Server

802.1X

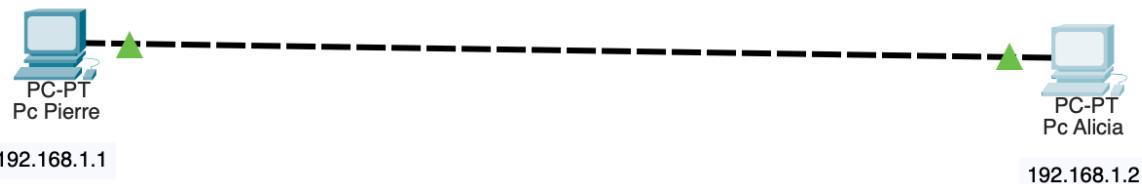
Use 802.1X Security

Authentication MD5

Username

Password

Top



Qu'est-ce qu'une adresse IP ?

Une adresse IP, ou adresse de protocole Internet, est un identifiant numérique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Les adresses IP permettent de localiser et d'identifier de manière unique un appareil sur un réseau, qu'il s'agisse d'un ordinateur, d'un smartphone, d'une imprimante, d'un routeur, ou de tout autre périphérique connecté à Internet ou à un réseau local.

À quoi sert un IP ?

Les adresses IP servent à deux fonctions principales :

- **Identification** : Chaque appareil sur un réseau a une adresse IP unique, ce qui permet de l'identifier de manière univoque. Cela permet d'acheminer le trafic réseau vers la bonne destination.
- **Localisation** : Les adresses IP permettent de localiser géographiquement un appareil sur Internet, bien que cela puisse être une information approximative en fonction de la manière dont l'adresse IP est attribuée.

Les adresses IP sont essentielles pour le fonctionnement d'Internet et des réseaux informatiques, car elles permettent aux appareils de se connecter, de communiquer et d'échanger des données.

Qu'est-ce qu'une adresse MAC ?

Une adresse MAC est un identifiant unique attribué à chaque carte réseau ou interface réseau d'un appareil ou d'un périphérique connecté à un réseau local ou à un réseau étendu. Contrairement à l'adresse IP, qui est utilisée pour identifier des appareils sur des réseaux IP, l'adresse MAC est spécifique au matériel et sert à identifier de manière unique une carte réseau particulière.

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

Adresse IP publique :

Une adresse IP publique est utilisée pour identifier un appareil sur Internet. Elle est accessible depuis l'ensemble du réseau mondial.

Chaque appareil connecté à Internet a généralement une adresse IP publique unique. Cela permet de router le trafic Internet vers l'appareil approprié, qu'il s'agisse d'un serveur web, d'une messagerie électronique ou d'un autre service en ligne.

Les adresses IP publiques sont nécessaires pour que les appareils communiquent sur Internet, car elles sont routables à travers le réseau mondial.

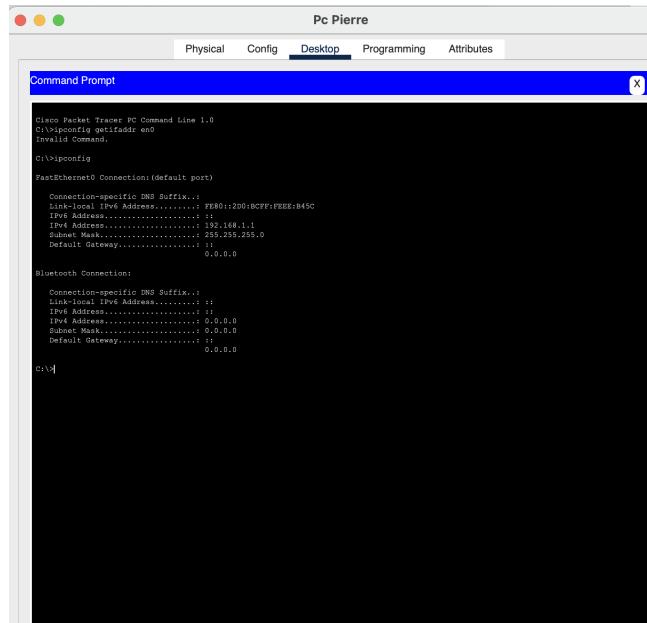
Adresse IP privée :

Une adresse IP privée est utilisée pour identifier un appareil au sein d'un réseau local ou d'un réseau privé d'entreprise. Elles ne sont pas routables sur Internet.

Les adresses IP privées sont souvent utilisées pour connecter plusieurs appareils dans un réseau local, permettant la communication interne entre eux. Cela offre un niveau de sécurité en évitant que ces appareils soient directement exposés à Internet.

Job 05 :

Nous allons maintenant vérifier que nos 2 PC ont bien l'adresse IP que nous voulons, pour cela, il nous suffit de nous rendre dans le terminal de notre application et taper la commande ipconfig, cela va permettre de nous afficher la configuration réseau de notre ordinateur.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /allifaddr en0
Invalid Command.

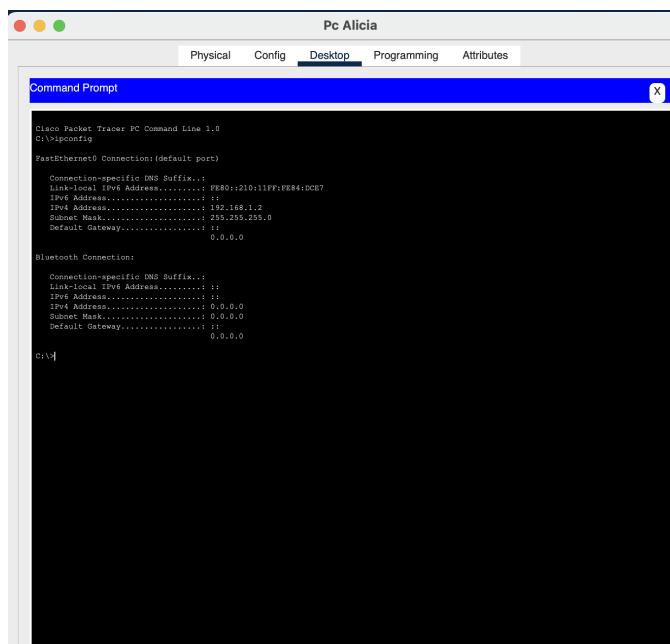
C:\>ipconfig

FastEthernet0 Connection:(default port)
  Connection-specific DNS Suffix.:
  Link-local IPv6 Address.....: FE80::2D0:BCFF%FEER:845C
  IPv4 Address.....: 192.168.1.1
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: 192.168.1.0

Bluetooth Connection:
  Connection-specific DNS Suffix.:
  Link-local IPv6 Address.....: FE80::2101:1FF%FE84:DCE7
  IPv4 Address.....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: 0.0.0.0

C:\>
```

Ainsi nous exécutons cette commande pour le PC de Pierre, et également pour le PC d'Alicia.



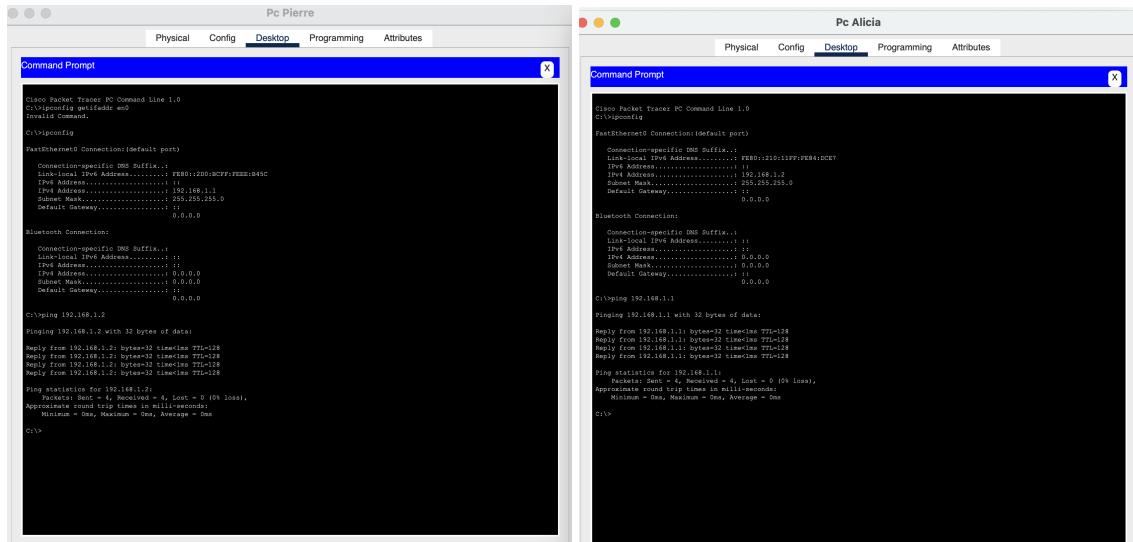
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /allifaddr en0
FastEthernet0 Connection:(default port)
  Connection-specific DNS Suffix.:
  Link-local IPv6 Address.....: FE80::2101:1FF%FE84:DCE7
  IPv4 Address.....: 192.168.1.2
  Subnet Mask.....: 255.255.255.0
  Default Gateway.....: 192.168.1.0

Bluetooth Connection:
  Connection-specific DNS Suffix.:
  Link-local IPv6 Address.....: FE80::2101:1FF%FE84:DCE7
  IPv4 Address.....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway.....: 0.0.0.0

C:\>
```

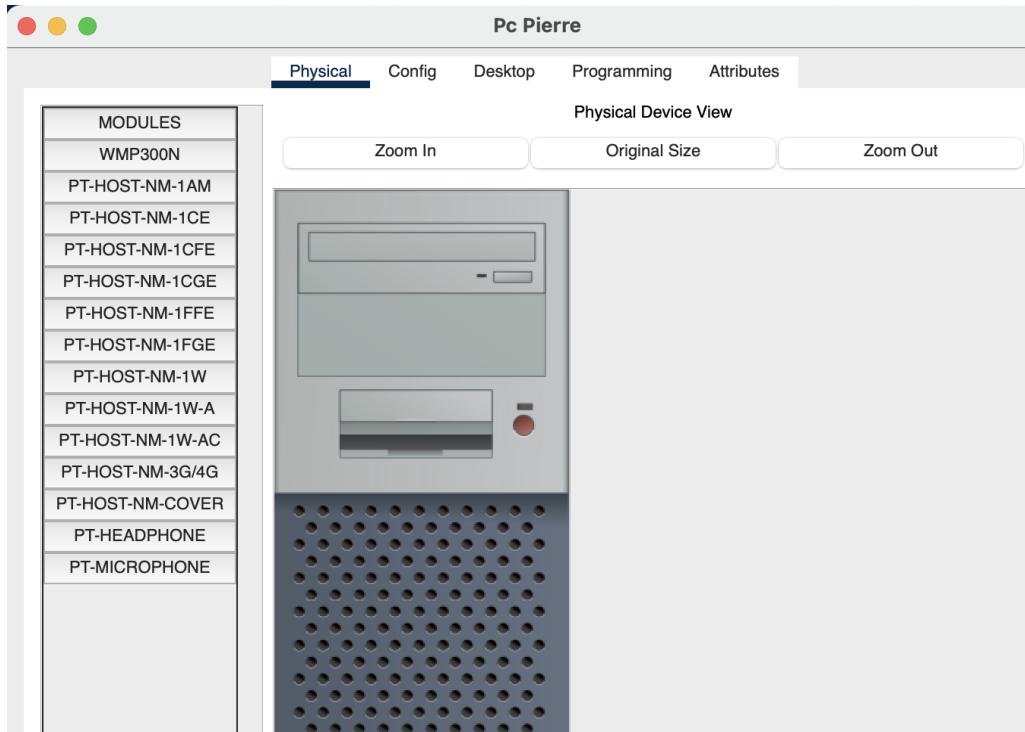
Job 06 :

Maintenant, nous allons envoyer un ping entre nos 2 PC pour vérifier leur connectivité, de ce fait il nous suffit de taper la commande ping dans le terminal suivi de l'adresse IP de l'ordinateur qui va recevoir ce ping.

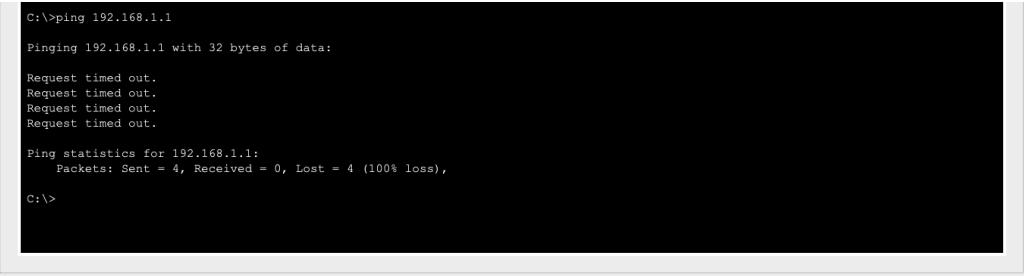


Job 07 :

Cela étant fait, nous avons décidé d'éteindre le PC de Pierre et de retenter l'expérience des pings depuis le PC d'Alicia, ainsi nous allons constater la différence.



On éteint donc le PC de Pierre depuis le menu physical, et on retape la commande du ping depuis le terminal du PC d'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),
C:\>
```

Top

Suite à cela, nous pouvons constater qu'aucun des pings envoyés depuis le PC d'Alicia n'a pas eu de réponses, en raison du fait que le PC de Pierre est éteint, ainsi il n'est pas connecté à un réseau, ainsi comme il est dit sur l'image les paquets ont été perdues car ils n'ont pas reçu de réponses et donc ne sont jamais revenus. Cela signifie que le ping a atteint le PC cible, mais il n'a pas reçu de réponse en retour, car l'ordinateur cible était hors ligne ou ne répondait pas.

Job 08 :

Pour ce job, nous allons agrandir notre réseau en connectant 5 ordinateurs, et pour cela nous allons avoir besoin soit d'un Hub soit d'un Switch, cela va permettre de relier les 5 ordinateurs entre eux et ensuite nous allons chercher leur connectivité.

Quelle est la différence entre un hub et un switch ?

Un hub et un switch sont deux types de dispositifs utilisés dans les réseaux informatiques pour interconnecter plusieurs appareils. Cependant, ils fonctionnent de manière très différente et ont des performances et des capacités distinctes.

Un hub est un dispositif de couche 1 (couche physique) du modèle OSI. Il transmet simplement les données reçues sur un port à tous les autres ports. En d'autres termes, il diffuse les données à l'ensemble du réseau.

Un switch est un dispositif de couche 2 (couche de liaison de données) du modèle OSI. Il examine l'adresse MAC des trames entrantes et décide de laquelle envoyer à un port spécifique, réduisant ainsi la congestion du réseau.

Un hub et un switch sont des dispositifs de réseau qui diffèrent principalement par leur façon de gérer le trafic. Les hubs sont moins chers mais moins performants, tandis que les switches offrent une gestion plus intelligente du trafic, une meilleure performance et une meilleure sécurité. Dans la plupart des réseaux modernes, les switches sont préférés aux hubs en raison de leurs avantages en termes de performances et de sécurité.

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

Un hub fonctionne de manière très simple. Lorsqu'il reçoit des données sur un port, il les répète sur tous les autres ports, diffusant ainsi les données à l'ensemble du réseau. Cela signifie que toutes les données envoyées à un hub sont retransmises à tous les appareils connectés à ce hub, quel que soit le destinataire prévu.

Contrairement à la switch, il ne prend pas en compte l'adresse MAC des appareils connectés, car il opère uniquement au niveau de la couche physique.

Les hubs sont simples à mettre en place et à utiliser. Il suffit de les brancher et de connecter les appareils, sans configuration complexe, ils sont généralement moins chers que les switches, ce qui en a fait un choix économique dans le passé.

Comme le hub diffuse les données à tous les ports, la bande passante est partagée entre tous les appareils connectés. Cela peut entraîner des collisions de données et une utilisation inefficace de la bande passante. Les données sont visibles par tous les appareils connectés au hub. Il n'y a aucune isolation entre les appareils, ce qui pose des problèmes de sécurité et de confidentialité. En raison des collisions potentielles, la latence est plus élevée dans un réseau basé sur un hub.

Quels sont les avantages et inconvénients d'un switch ?

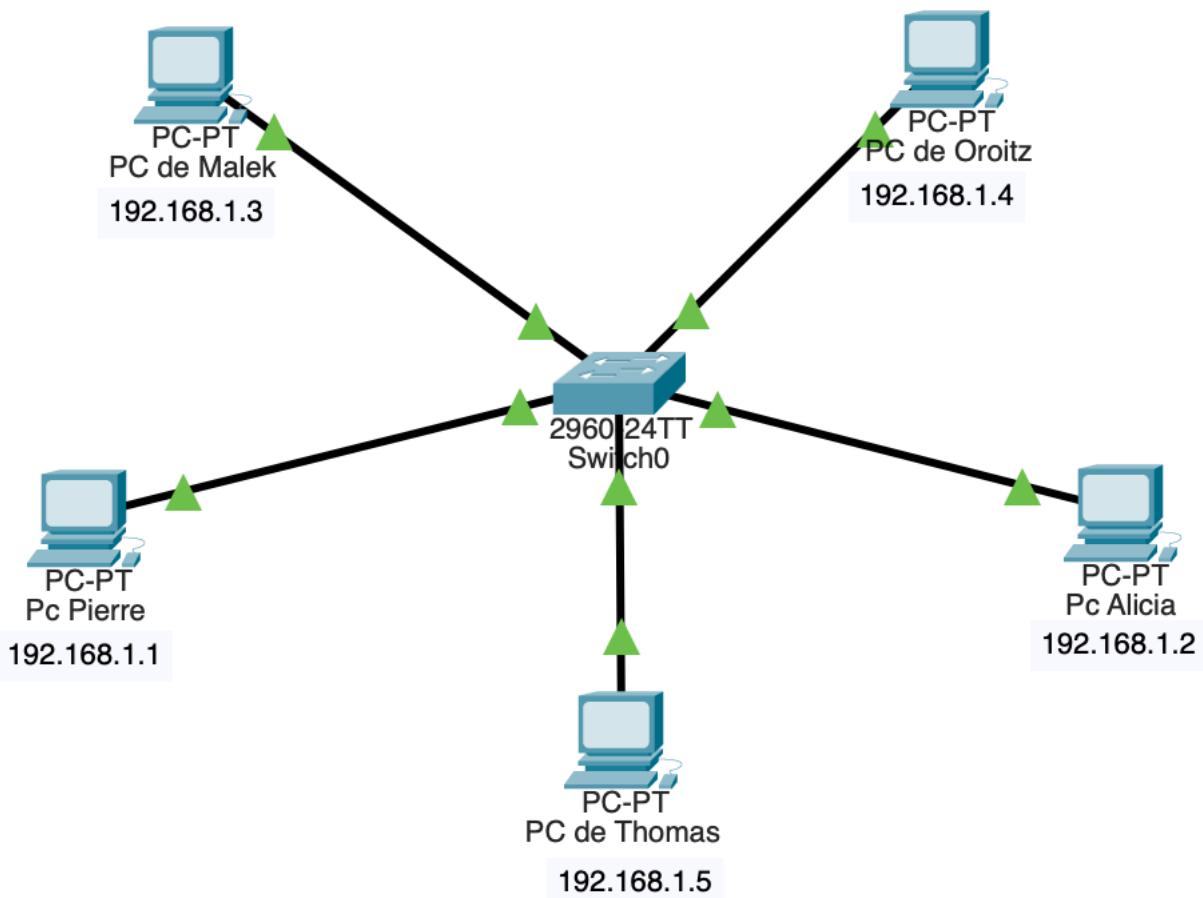
Les switches offrent une meilleure performance que les hubs, car ils prennent en charge la commutation. Ils acheminent intelligemment les données uniquement vers les ports des appareils destinataires, ce qui réduit les collisions et augmente l'efficacité de la bande passante. Ils isolent le trafic entre les ports, ce qui signifie que les données ne sont pas diffusées à l'ensemble du réseau. Cela renforce la sécurité et la confidentialité des données. Ils évitent les collisions de données courantes dans les réseaux hub-based, ce qui se traduit par une transmission plus rapide des données. Les switches permettent de segmenter le réseau en différents groupes de travail (VLANs), ce qui facilite la gestion et la sécurité du réseau, et offrent des fonctionnalités de gestion avancée, telles que la qualité de service (QoS), la surveillance du trafic, la gestion de la bande passante, et la configuration de règles de sécurité. Les switches peuvent être empilés ou connectés en cascade pour étendre la capacité du réseau, ce qui permet une expansion facile.

Cependant, les switches sont généralement plus coûteux que les hubs ou les dispositifs de réseau plus simples en raison de leurs fonctionnalités avancées. Ils peuvent être complexes à configurer, en particulier dans les environnements d'entreprise. Une mauvaise configuration peut entraîner des problèmes de réseau. La

gestion et la surveillance des switches peuvent nécessiter des compétences techniques et une administration continue pour maintenir un réseau efficace.

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

Un switch gère le trafic réseau en utilisant la commutation (switching) pour acheminer intelligemment les données entre les appareils connectés à ses ports. Lorsqu'un appareil se connecte à un port du switch, il gère le trafic réseau en apprenant les adresses MAC des appareils connectés à ses ports, en utilisant ces informations pour acheminer sélectivement les données vers les ports appropriés, en gérant la bande passante de manière efficace, en isolant le trafic entre les ports, et en maintenant une table d'adresses MAC mise à jour pour une gestion précise du trafic réseau. Cela améliore la performance, la sécurité et la gestion du réseau par rapport aux dispositifs de réseau plus anciens, tels que les hubs.



De ce fait, nous avons décidé que pour cet exercice, nous allons utiliser un switch au lieu d'un hub pour faciliter ce dernier, nous avons donc connecter 3 autres PC en plus

de celui de Pierre et d'Alicia, on a donc celui de Malek, d'Oroitz et de Thomas, chacun avec une adresse IP.

```
Pinging 192.168.1.1 with 32 bytes of data:
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

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

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 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:
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

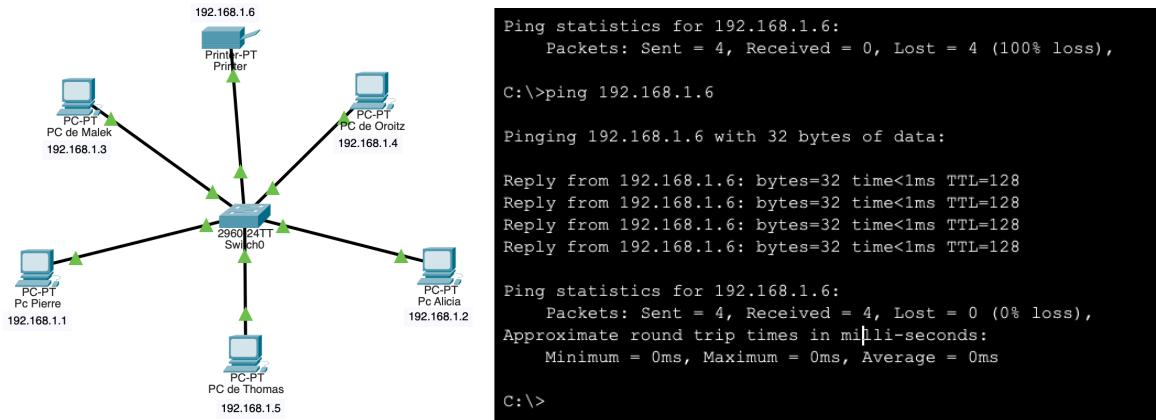
Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

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 = 0ms, Average = 0ms
```

Pour vérifier la compatibilité des ordinateurs entre eux, avec l'ordinateur de Malek nous avons envoyé un ping à chacun des pc connectés à la switch, de ce fait nous avons pu remarquer que tous les paquets sont arrivés à destination et donc que tous les ordinateurs sont bien connectés entre eux sans aucun problèmes.

Job 09 :

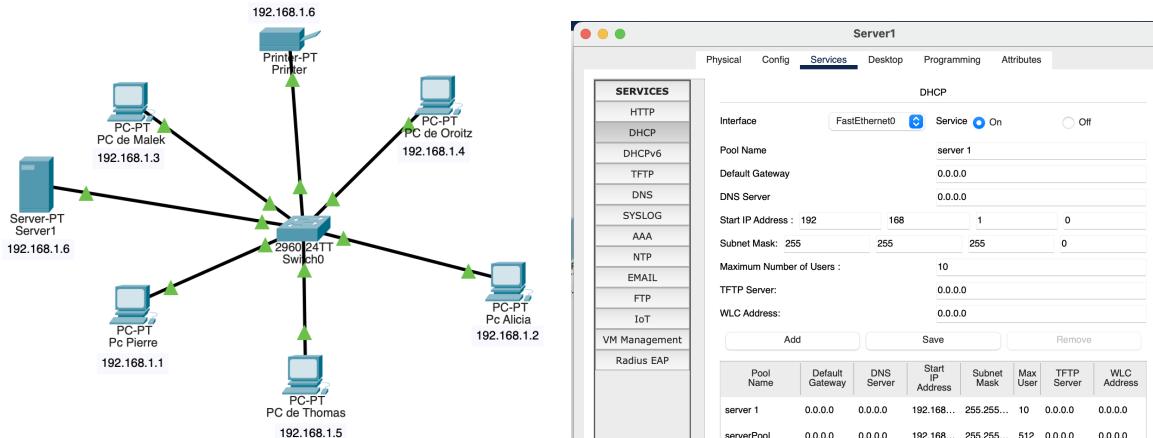
Nous souhaitons maintenant connecter une imprimante, de ce fait nous la relions à la switch et nous vérifions sa connectivité comme fait précédemment avec la commande ping depuis un ordinateur ou l'on attend le fait que le terminal nous dise que les paquets ont bien été reçus.



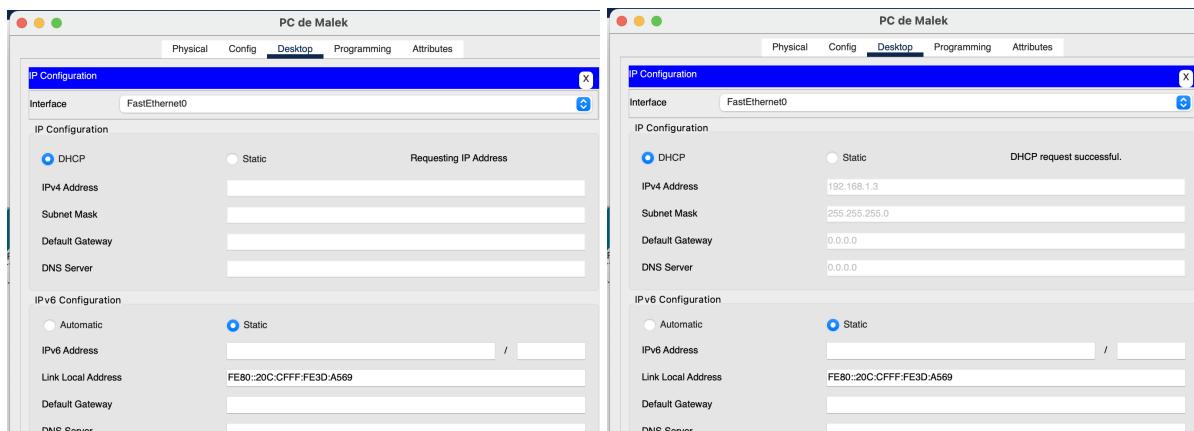
La visualisation d'un travail schématique est très efficace, il nous permet une communication de ce dernier de manière claire et simple, utile pour présenter le concept de manière compréhensible, la compréhension du sujet est donc également amélioré, permettant de regrouper des infos connexes, et enfin elle va nous permettre de résoudre plus facilement des problèmes rencontrés car elle permet d'organiser des idées de manière à distinguer ce qui n'a pas sa place ou ce qui peut manquer. De ce fait, on peut remarquer sur notre schéma que nous avons 5 ordinateurs connectés à notre switch, et que chacun à sa propre adresse ip écrit près de lui, de plus nous pouvons constater la présence de notre imprimante relié également directement à notre switch et donc à une connectivité avec nos autres appareils, avec en plus, son adresse ip écrit proche d'elle.

Job 10 :

Au fil des jobs, nous étions obligés à chaque fois de soumettre manuellement une adresse ip, de ce fait nous allons mettre en place un serveur DHCP pour fournir automatiquement les adresses IP aux périphériques. On lie donc le serveur mis en place à la switch qui relie tous les ordinateurs, et l'on fournit une adresse IP static pour pouvoir configurer le DHCP et ainsi fournir les adresses IP.



Suite à cela, nous pouvons configurer notre DHCP en lui fournissant comme adresse IP static 192.168.1.6, et nous activons le service de DHCP, on demande à ce qu'il s'appelle server 1 et qu'il puisse fournir des adresses IP à partir de l'adresse 192.168.1.0,, et comme sous masque l'adresse 255.255.255.0, avec un maximum d'utilisateurs du nombre de 10.



Ceci configuré, on peut se diriger vers l'ordinateur de Malek pour vérifier cela, nous allons demander une adresse IP via le DHCP, l'instruction est en cours, et quelques secondes après nous obtenons notre adresse IP.

Les adresses IP statiques et les adresses IP attribuées par le protocole DHCP sont deux méthodes de configuration des adresses IP des dispositifs dans un réseau.

Adresse IP statique :

Les adresses IP statiques sont configurées manuellement par un administrateur réseau. Chaque appareil doit être configuré individuellement avec une adresse IP spécifique. Une fois attribuée, une adresse IP statique reste constante, à moins qu'elle ne soit modifiée manuellement. Cela signifie que l'appareil conserve la même adresse IP chaque fois qu'il se connecte au réseau. Les administrateurs réseau ont un contrôle total sur les adresses IP statiques et peuvent déterminer quelles adresses IP sont attribuées à chaque appareil. Les adresses IP statiques sont utiles

pour les serveurs, les dispositifs réseau critiques et les appareils nécessitant une adresse IP constante. Elles facilitent également la configuration dans les réseaux plus petits et simplifient le suivi des appareils. La gestion des adresses IP statiques peut devenir fastidieuse dans les grands réseaux.

Adresse IP attribuée par DHCP :

Les adresses IP attribuées par le DHCP sont configurées automatiquement par un serveur DHCP. Lorsqu'un appareil se connecte au réseau, il envoie une demande au serveur DHCP pour obtenir une adresse IP. Les adresses IP attribuées par DHCP peuvent changer à chaque fois qu'un appareil se connecte au réseau, bien que le serveur DHCP puisse être configuré pour attribuer la même adresse IP à un appareil spécifique. Le DHCP simplifie la gestion des adresses IP dans les réseaux les plus importants. Il automatisé le processus d'attribution et de gestion des adresses IP. Le DHCP est efficace pour gérer les adresses IP dans les réseaux de grande taille. Il simplifie la configuration et la gestion en attribuant automatiquement les adresses IP aux appareils.

Job 11 :

Pour créer 21 sous-réseaux à partir de l'adresse réseau de classe A 10.0.0.0, il faut effectuer un partitionnement du réseau en sous-réseaux plus petits en fonction du nombre d'hôtes requis pour chaque sous-réseau. Pour ce faire, nous allons procéder étape par étape :

- Déterminer la classe d'adresse IP**

L'adresse réseau est de classe A, ce qui signifie que le préfixe réseau par défaut est de 8 bits (par exemple, 10.0.0.0/8).

- Identifier le nombre de bits de sous-réseau**

Pour créer 21 sous-réseaux, on aura besoin d'au moins 5 bits de sous-réseau ($2^5 = 32$). Cependant, on peut utiliser un nombre de bits de sous-réseau qui soit une puissance de 2 et qui soit suffisant pour tout couvrir. On peut donc choisir d'utiliser 8 bits de sous-réseau ($2^8 = 256$) pour plus de flexibilité.

- Créer les sous-réseaux

Avec 8 bits de sous-réseau, on peut créer 256 sous-réseaux (2^8). Cela dépasse le besoin de 21 sous-réseaux, mais cela donne de la marge pour la croissance future.

On peut répartir les sous-réseaux de la manière suivante :

- 1 sous-réseau pour 12 hôtes : (10.0.0.0/24 à 10.0.0.0/31)
- 5 sous-réseaux pour 30 hôtes chacun : (10.0.1.0/27 à 10.0.1.224/27)
- 5 sous-réseaux pour 120 hôtes chacun : (10.0.2.0/25 à 10.0.2.128/25)
- 5 sous-réseaux pour 160 hôtes chacun : (10.0.3.0/24 à 10.0.3.224/24)

- Attribution des plages d'adresses

Une fois que nous avons créé les sous-réseaux, on leur attribue des plages d'adresses IP spécifiques à chaque sous-réseau en veillant à ce que chaque adresse IP soit unique au sein du sous-réseau. Par exemple, dans le premier sous-réseau (12 hôtes), les adresses IP vont de 10.0.0.1 à 10.0.0.14, avec 10.0.0.0 comme adresse réseau et 10.0.0.15 comme adresse de diffusion.

Nous allons fournir toutes les informations complètes, dans un tableau regroupant toutes les données nécessaires.

G18							
	A	B	C	D	E	F	G
1	n° de sous-réseau	gateway	plage d'adresse	BIT	masque en binaire	masque de sous réseau	adresse de diffusion
2	Sous-réseau de 12 hôtes	10.0.0.0	10.0.0.1 - 10.0.0.14	2 ⁴	1111 1111.1111 1111.1111 1111.1111 0000	255.255.255.240 / 28	10.0.0.15
3	Sous-réseau de 30 hôtes	10.0.0.16	10.0.0.17 - 10.0.0.46	2 ⁵	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.47
4	Sous-réseau de 30 hôtes	10.0.0.48	10.0.0.49 - 10.0.0.78	2 ⁵	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.79
5	Sous-réseau de 30 hôtes	10.0.0.80	10.0.0.81 - 10.0.0.110	2 ⁵	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.111
6	Sous-réseau de 30 hôtes	10.0.0.112	10.0.0.113 - 10.0.0.142	2 ⁵	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.143
7	Sous-réseau de 30 hôtes	10.0.0.144	10.0.0.145 - 10.0.0.174	2 ⁵	1111 1111.1111 1111.1111 1111.1110 0000	255.255.255.224 / 27	10.0.0.175
8	Sous-réseau de 120 hôtes	10.0.0.176	10.0.0.177 - (10.0.0.255) - 10.0.1.46	2 ⁷	1111 1111.1111 1111.1111.1000 0000	255.255.255.128 / 25	10.0.1.47
9	Sous-réseau de 120 hôtes	10.0.1.48	10.0.1.49 - 10.0.1.174	2 ⁷	1111 1111.1111 1111.1111.1000 0000	255.255.255.128 / 25	10.0.1.175
10	Sous-réseau de 120 hôtes	10.0.1.176	10.0.1.177 - (10.0.1.255) - 10.0.2.46	2 ⁷	1111 1111.1111 1111.1111.1100 0000	255.255.255.128 / 25	10.0.2.47
11	Sous-réseau de 120 hôtes	10.0.2.48	10.0.2.49 - 10.0.2.174	2 ⁷	1111 1111.1111 1111.1111.1100 0000	255.255.255.128 / 25	10.0.2.175
12	Sous-réseau de 120 hôtes	10.0.2.176	10.0.2.177 - (10.0.2.255) - 10.0.3.46	2 ⁷	1111 1111.1111 1111.1111.1100 0000	255.255.255.128 / 25	10.0.3.47
13	Sous-réseau de 160 hôtes	10.0.3.48	10.0.3.49 - 10.0.4.46	2 ⁸	1111 1111.1111 1111.1111.1111.0000	255.255.255.0 / 24	10.0.4.47
14	Sous-réseau de 160 hôtes	10.0.4.48	10.0.4.49 - 10.0.5.46	2 ⁸	1111 1111.1111 1111.1111.1111.0000	255.255.255.0 / 24	10.0.5.47
15	Sous-réseau de 160 hôtes	10.0.5.48	10.0.5.49 - 10.0.6.46	2 ⁸	1111 1111.1111 1111.1111.1111.0000	255.255.255.0 / 24	10.0.6.47
16	Sous-réseau de 160 hôtes	10.0.6.48	10.0.6.49 - 10.0.7.46	2 ⁸	1111 1111.1111 1111.1111.1111.0000	255.255.255.0 / 24	10.0.7.47
17	Sous-réseau de 160 hôtes	10.0.7.48	10.0.7.49 - 10.0.8.46	2 ⁸	1111 1111.1111 1111.1111.1111.0000	255.255.255.0 / 24	10.0.8.47

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

L'adresse IP 10.0.0.0 a été choisie pour créer des sous-réseaux en raison de sa classe IP et de sa plage d'adresses disponibles. L'adresse IP 10.0.0.0 appartient à la classe A, qui est l'une des classes d'adresses IP réservées aux réseaux de grande taille. Les adresses de classe A ont un préfixe de réseau de 8 bits, ce qui signifie que les trois premiers octets (24 bits) sont réservés pour le réseau, offrant ainsi une grande plage d'adresses IP disponibles pour créer des sous-réseaux. Elle offre une large plage d'adresses IP de la flexibilité pour la création de sous-réseaux et la

confidentialité pour un usage interne, ce qui en fait un choix approprié pour diviser un réseau en plusieurs sous-réseaux en fonction des besoins.

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

Classe A

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

Classe B

Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

Classe C

Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

Job 12 :

Couche OSI	Description des rôles	Matériels/Protocoles associés
7. Application	Interface avec les applications utilisateur. Gère les interactions avec les logiciels et les services utilisateurs.	HTTP, FTP, HTML, SSL/TLS, PPTP
6. Présentation	Responsable de la traduction, de la compression, du chiffrement et du formatage des données pour assurer la compatibilité entre les systèmes.	SSL/TLS, HTML
5. Session	Gère l'établissement, la maintenance et la fermeture des sessions de communication entre les systèmes.	-
4. Transport	Assure la fiabilité de bout en bout de la communication. Gère le contrôle de flux, la segmentation et la réassemblage des données.	TCP, UDP
3. Réseau	Contrôle la transmission des données entre réseaux différents. Gère le routage, l'adressage et la détermination des chemins.	IPv4, IPv6, routeur
2. Liaison de données	Gère la communication entre dispositifs sur le même réseau local. Contrôle l'accès au support physique et assure la détection et la correction des erreurs.	Ethernet, MAC, Wi-Fi, cable RJ45
1. Physique	Gère les aspects matériels de la communication, tels que le câblage, les signaux électriques et les médias de transmission.	Fibre optique, cable RJ45

FTP : Il fournit des services de transfert de fichiers et d'interaction avec l'utilisateur. Cette couche est la plus proche de l'utilisateur final et gère les échanges entre les applications. FTP opère à un niveau d'abstraction plus élevé, permettant aux utilisateurs de naviguer dans les répertoires, télécharger et téléverser des fichiers, et effectuer des opérations de gestion des fichiers.

TCP :

La couche transport du modèle OSI se concentre sur deux protocoles, **TCP** (Transmission Control Protocol) et UDP (User Datagram Protocol). Les professionnels du secteur considèrent le **TCP** comme un protocole fiable ou orienté connexion.

SSL/TLS : fonctionne au niveau de la couche de transport pour sécuriser les connexions entre deux entités communicantes. Il s'agit principalement de sécuriser les échanges de données entre l'expéditeur et le destinataire, offrant une couche de chiffrement pour protéger la confidentialité et l'intégrité des données.

L'UDP : Se trouve à la couche 4 du modèle OSI, car c'est là qu'il gère la communication entre applications sur différents appareils. Il offre une méthode légère, rapide et sans connexion pour transmettre des données. L'UDP n'assure pas la livraison garantie des données, mais il est utilisé dans des situations où la rapidité est plus importante que la fiabilité, comme dans la diffusion en temps réel, les jeux en ligne, ou les applications de streaming vidéo.

IPv4 :

Le fait que l'IPv4 est dans la couche 3 s'explique par le rôle fondamental d'IPv4 dans la transmission de données sur un réseau et la fourniture d'un service de routage.

IPv6 : Est positionné à la couche 3 du modèle OSI en raison de son rôle fondamental dans la gestion des adresses IP, le routage des paquets, et l'encapsulation des données pour la transmission sur les réseaux.

Le routeur : Se situe à la couche 3 du modèle OSI, la couche réseau, car il joue un rôle clé dans le routage des paquets de données entre différents réseaux. En utilisant des adresses IP pour identifier les destinations, le routeur prend des décisions de routage pour diriger efficacement les paquets à travers des réseaux interconnectés.

L'éthernet : A pour rôle de découper les informations en trames ayant une certaine signification et la reconnaissance de ces trames à la réception. Elle a aussi pour rôle de gérer les erreurs sur le support physique.

MAC :

La couche MAC couvre l'adressage physique du périphérique réseau, comme l'adresse MAC des cartes d'interface. Il s'agit d'une adresse de 48 bits qui rend toutes les cartes uniques par rapport à toutes les autres cartes sur tous les autres périphériques.

Fibre optique : Cette couche est responsable de la gestion des erreurs et du contrôle d'accès au support. Dans le contexte de la fibre optique, cette couche peut être impliquée dans des aspects tels que la détection et la correction d'erreurs qui peuvent survenir lors de la transmission des données sur la fibre.

PPTP : utilise cette couche pour encapsuler les paquets PPP dans des trames de liaison de données, généralement sur des connexions de type point à point. Cela permet la création de tunnels virtuels pour transporter le trafic PPP sur des réseaux IP, tels qu'Internet.

Wi-Fi : Cela inclut la modulation des signaux radiofréquences pour la communication sans fil. Les aspects tels que la fréquence, la modulation, la puissance de transmission et d'autres caractéristiques physiques du signal Wi-Fi sont définis à cette couche.

Câble RJ45 :

Le câble RJ45 est une composante physique qui se situe à la couche 1 du modèle OSI, facilitant la transmission des données à travers les différentes couches du modèle OSI.

HTML :

HTML est principalement associé à la couche Application du modèle OSI. Il s'agit de la couche où les applications utilisateur interagissent avec le réseau. Les navigateurs Web utilisent HTML pour afficher le contenu Web, et les serveurs Web utilisent HTTP pour transmettre ce contenu aux navigateurs. Bien que HTML se concentre principalement sur la structure du contenu, la présentation visuelle est souvent gérée par les feuilles de style (CSS), qui sont liées aux pages HTML. Les CSS définissent l'apparence et la mise en page des éléments HTML. Ainsi, la présentation visuelle relève davantage de la couche 6.

Job 13 :

Quelle est l'architecture de ce réseau ?

L'architecture réseau décrite semble suivre un modèle de réseau en étoile. Dans cette architecture, tous les dispositifs du réseau (PC0, PC1, PC2, PC3, Serveur 1, Serveur 2) sont connectés à un point central. En tant que switch, il connecte tous les PCs et serveurs. Chaque dispositif est connecté directement à la switch.

Ce modèle de réseau en étoile présente certains avantages, notamment une facilité de gestion, car tous les câbles convergent vers un seul point, et la facilité de dépannage, car un problème sur un dispositif n'affecte pas nécessairement les autres.

Indiquer quelle est l'adresse IP du réseau ?

Pour déterminer l'adresse IP du réseau dans notre cas, on doit examiner l'adresse IP d'un des dispositifs dans le réseau et appliquer le masque de sous-réseau.

Prenons comme exemple ces données :

- PC0 : 192.168.10.6
- Masque de sous-réseau : 255.255.255.0

On va maintenant convertir de façon binaire nos 2 adresses, et les superposer, de cette manière nous allons calculer toujours en binaire, n'ayant que des résultats de 1 ou 0.

192.168.10.6 → 11000000.10101000.00001010.00000110

255.255.255.0 → 11111111.11111111.11111111.00000000

11000000.10101000.00001010.00000000 → 192.168.10.0

Donc, l'adresse IP du réseau est 192.168.10.0

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

Pour déterminer le nombre de machines que l'on peut brancher sur ce réseau, il faut utiliser le masque de sous-réseau. Le masque de sous-réseau est 255.255.255.0, ce qui équivaut à un masque de sous-réseau /24 en notation CIDR. Un masque /24 signifie que les 24 premiers bits de l'adresse IP sont réservés pour le réseau, et les 8 bits restants sont utilisés pour les hôtes.

Pour calculer le nombre de machines possibles:

Nombre de machines possibles = $2^{(\text{nombre de bits d'hôtes})} - 2$

Le "-2" dans la formule est pour soustraire l'adresse de réseau (où tous les bits d'hôtes sont à zéro) et l'adresse de diffusion (où tous les bits d'hôtes sont à un), car ces adresses ne sont généralement pas attribuées à des machines.

Il y a 8 bits d'hôtes donc le calcul serait :

Nombre de machines possibles = $2^8 - 2 = 256 - 2 = 254$

Il est donc possible de brancher jusqu'à 254 machines sur ce réseau avec l'adresse IP 192.168.10.0/24.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion d'un réseau est l'adresse spéciale qui permet d'envoyer des données à tous les dispositifs du réseau en même temps. Dans un réseau avec un masque de sous-réseau de 255.255.255.0, l'adresse de diffusion se trouve en mettant tous les bits d'hôtes à 1 dans l'adresse IP.

L'adresse IP du réseau est 192.168.10.0 avec un masque de sous-réseau de 255.255.255.0. Pour déterminer l'adresse de diffusion, il faut mettre tous les bits de l'octet d'hôtes à 1. Donc, l'adresse de diffusion serait : 192.168.10.255

Job 14 :

Pour convertir une adresse IP en binaire, il faut comprendre que les adresses IP sont des numéros décimaux et que le binaire est un système de numération en base 2. Chaque adresse IP est composée de quatre octets, et chaque octet est constitué de huit bits.

145.32.59.24

- En binaire, 145 s'écrit comme 10010001.
- En binaire, 32 s'écrit comme 00100000.
- En binaire, 59 s'écrit comme 00111011.
- En binaire, 24 s'écrit comme 00011000.

145.32.59.24 en binaire : 10010001.00100000.00111011.00011000

200.42.129.16

- En binaire, 200 s'écrit comme 11001000.
- En binaire, 42 s'écrit comme 00101010.
- En binaire, 129 s'écrit comme 10000001.
- En binaire, 16 s'écrit comme 00010000.

200.42.129.16 en binaire : 11001000.00101010.10000001.00010000

14.82.19.54

- En binaire, 14 s'écrit comme 00001110.
- En binaire, 82 s'écrit comme 01010010.
- En binaire, 19 s'écrit comme 00010011.
- En binaire, 54 s'écrit comme 00110110.

14.82.19.54 en binaire : 00001110.01010010.00010011.00110110

Job 15 :

Qu'est-ce que le routage ?

Le routage est le processus de transfert de données entre différents réseaux informatiques. Il s'agit de la méthode permettant de déterminer comment les données doivent être acheminées d'un point à un autre à travers un réseau, en utilisant des routeurs pour prendre des décisions sur la meilleure voie à suivre. Le routage est essentiel pour la connectivité et la communication efficace des dispositifs dans des réseaux complexes, tels qu'Internet et les réseaux d'entreprise. Le routage est le processus clé qui permet de déterminer comment les données sont acheminées à travers un réseau. Il est essentiel pour assurer une communication efficace et fiable dans des réseaux de toutes tailles, du réseau local (LAN) à l'Internet mondial.

Qu'est-ce qu'un gateway ?

Une passerelle, ou "gateway" en anglais, est un dispositif ou un logiciel qui relie deux réseaux informatiques distincts, leur permettant de communiquer et de transférer des données entre eux. Les passerelles jouent un rôle essentiel dans la mise en réseau et la connectivité, car elles facilitent la communication entre des réseaux ayant des protocoles ou des technologies différents. Une passerelle est un élément central pour la connectivité entre réseaux. Elle facilite la communication et le partage de données entre des réseaux différents tout en offrant des fonctionnalités de sécurité et de routage pour garantir un échange de données fiable et sécurisé.

Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel en français, est un service ou une technologie qui permet de créer une connexion sécurisée entre un utilisateur ou un réseau local et un serveur distant via Internet. Les VPN sont largement utilisés pour renforcer la sécurité, la confidentialité et l'anonymat des communications sur Internet, ainsi que pour accéder à des ressources réseau distantes de manière sécurisée. Un VPN est un outil puissant pour renforcer la sécurité et la confidentialité en ligne, permettant aux utilisateurs de surfer sur Internet de manière plus sécurisée, de contourner la censure, d'accéder à des ressources réseau à distance et de préserver leur anonymat en ligne.

Qu'est-ce qu'un DNS ?

Le DNS, ou Domain Name System, est un service essentiel d'Internet qui permet de traduire les noms de domaine conviviaux que nous utilisons en adresses IP numériques que les ordinateurs et les serveurs utilisent pour identifier et localiser d'autres dispositifs sur le réseau. En d'autres termes, le DNS agit comme un annuaire pour Internet, permettant de trouver les ressources en ligne en fonction de leur nom de domaine.