

Job 1

Installation de Cisco Packet Tracer :

Téléchargez Cisco Packet Tracer

Le meilleur moyen d'étudier la mise en réseau est de pratiquer.

Cisco Packet Tracer, un outil de simulation et de visualisation innovant, vous aide à mettre en pratique vos compétences en matière de réseau, d'IoT et de cybersécurité sans quitter votre bureau.

Utilisez Cisco Packet Tracer pour :

- Mettre vos connaissances en pratique
- Vous préparer aux examens de certification
- Affiner vos connaissances en vue d'un entretien d'embauche

Packet Tracer est un outil pédagogique essentiel utilisé pour des activités et pour évaluer vos connaissances dans la plupart des cours de la Cisco Networking Academy.

Les conditions minimales suivantes doivent être remplies pour l'installation et l'exécution de Packet Tracer 8.2 :

1. Cisco Packet Tracer 8.2 (64 bits) :

- Ordinateur équipé de l'un des systèmes d'exploitation suivants : Microsoft Windows 8.1, 10, 11 (64 bits), Ubuntu 20.04, 22.04 LTS (64 bits) ou MacOS 10.14 ou version ultérieure.
- Processeur amd64 (x86-64)
- 4 Go de RAM disponible
- 1,4 Go d'espace disque disponible

Bureau Windows, version 8.2.1 (anglais)

[Télécharger la version 64 bits](#)

[Télécharger la version 32 bits](#)

Job 2

→ Qu'est-ce qu'un réseau ?

Un **réseau** est un ensemble de dispositifs interconnectés qui communiquent entre eux pour partager des informations, des ressources et des services. Ces dispositifs peuvent inclure des ordinateurs, des serveurs, des routeurs, des commutateurs, des smartphones, des imprimantes, et bien d'autres appareils. Les réseaux permettent aux utilisateurs d'échanger des données, de collaborer, d'accéder à des ressources partagées et de se connecter à internet.

Il existe différents types de réseaux, notamment :

- Réseau local (LAN - Local Area Network)
- Réseau étendu (WAN - Wide Area Network)
- Réseau métropolitain (MAN - Metropolitan Area Network)
- Réseau sans fil (Wi-Fi) :
- Réseau social
- Réseau d'entreprise

Les réseaux utilisent divers protocoles de communication, tels que TCP/IP, pour faciliter la transmission des données. Ils peuvent être câblés (comme les réseaux Ethernet) ou sans fil (comme les réseaux Wi-Fi). Les réseaux jouent un rôle essentiel dans le monde moderne, facilitant la connectivité et l'accès aux ressources informatiques à l'échelle locale, nationale et internationale.

→ **À quoi sert un réseau informatique ?**

Les **réseaux informatiques** permettent le partage de ressources telles que des fichiers, des imprimantes, des scanners, des serveurs de stockage, des bases de données et des périphériques, facilitant ainsi l'accès aux informations et aux équipements pour les utilisateurs du réseau. Ils permettent la communication entre les utilisateurs via des services tels que la messagerie électronique, la messagerie instantanée et la vidéoconférence. De nombreux réseaux informatiques sont connectés à Internet, ce qui permet aux utilisateurs d'accéder à une vaste quantité d'informations, de services en ligne et de ressources, notamment des sites web, des e-mails, des médias sociaux, etc...

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

Pour construire un réseau informatique, nous avons besoin de divers composants matériels qui remplissent des fonctions spécifiques pour permettre la communication, le partage de ressources et la gestion du réseau. Voici les principaux composants et leurs fonctions :

Dispositifs de communication	<p>Ordinateurs : Les ordinateurs sont les points finaux du réseau et sont utilisés pour accéder aux ressources, partager des informations et communiquer.</p> <p>Serveurs : Les serveurs stockent des données et des services à partager avec les clients. Ils peuvent servir de serveurs de fichiers, de serveurs web, de serveurs de messagerie, etc.</p> <p>Smartphones et tablettes : Ces appareils se connectent également au réseau pour accéder à des données et des services.</p>
Composants de mise en réseau	<p>Routeurs : Les routeurs interconnectent différents réseaux, acheminant le trafic entre eux. Ils sont responsables de la prise de décision sur la meilleure route pour les données.</p> <p>Commutateurs (Switches) : Les commutateurs interconnectent les dispositifs au sein d'un même réseau local (LAN) et acheminent les données entre eux en fonction des adresses MAC (contrôle d'accès au support).</p> <p>Points d'accès sans fil (AP) : Ils permettent aux dispositifs sans fil de se connecter au réseau, étendant ainsi la connectivité sans fil (Wi-Fi).</p>
Câblage	<p>Câbles Ethernet : Ils sont utilisés pour connecter les dispositifs au réseau via des ports Ethernet. Les câbles</p>

La Plateforme

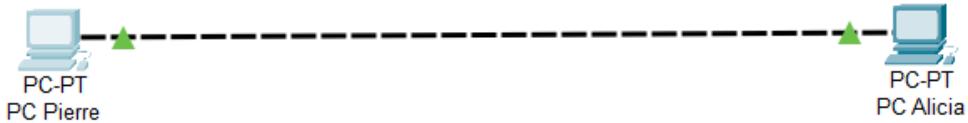
	<p>Ethernet sont couramment utilisés dans les réseaux filaires.</p> <p>Fibre optique : Pour les réseaux nécessitant une bande passante élevée sur de longues distances, la fibre optique est préférée en raison de sa capacité de transmission élevée et de sa résistance aux interférences.</p>
Serveurs	<p>Serveurs de fichiers : Stockent et partagent des fichiers avec d'autres dispositifs du réseau.</p> <p>Serveurs de messagerie : Gèrent les e-mails, permettant aux utilisateurs d'envoyer et de recevoir des courriels.</p> <p>Serveurs Web : Hébergent des sites web et délivrent des pages web aux navigateurs des utilisateurs.</p> <p>Serveurs de base de données : Stockent des données et permettent l'accès aux informations stockées.</p>
Périphériques de sécurité	<p>Firewalls : Protègent le réseau en bloquant le trafic non autorisé ou malveillant.</p> <p>Systèmes de détection des intrusions (IDS) et systèmes de prévention des intrusions (IPS) : Surveillent le trafic réseau pour détecter et prévenir les activités suspectes.</p> <p>Antivirus : Protège les dispositifs du réseau contre les logiciels malveillants.</p>
Serveurs d'authentification et d'autorisation	<p>Serveurs d'authentification : Vérifient l'identité des utilisateurs, généralement via des noms d'utilisateur et des mots de passe.</p> <p>Serveurs d'autorisation : Définissent les droits d'accès des utilisateurs aux ressources du réseau.</p>
Equipement d'alimentation et de refroidissement	<p>Les équipements réseau nécessitent souvent une alimentation électrique ininterrompue (UPS) pour éviter les pannes en cas de coupure de courant.</p> <p>Les dispositifs réseau génèrent de la chaleur, nécessitant une ventilation adéquate et des systèmes de refroidissement pour éviter la surchauffe.</p>

Bandé passante	Les connexions Internet à haut débit , telles que DSL, câble ou fibre optique, fournissent la bande passante nécessaire pour la communication entre le réseau local et Internet.
Logiciels de gestion et d'administration	Les logiciels de gestion de réseau permettent aux administrateurs de surveiller, gérer et configurer les dispositifs réseau, de définir des politiques de sécurité, etc.

Job 3

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

J'ai choisi d'utiliser un **copper crossover** (câble croisé en cuivre) pour relier directement les deux ordinateurs car les deux ordinateurs sont reliés sans passer par un routeur, un commutateur ou un autre dispositif réseau intermédiaire.



Job 4

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP, ou adresse de protocole Internet, est une série de numéros qui identifie de manière unique un périphérique ou un ordinateur sur un réseau IP (Internet Protocol). Ces adresses sont essentielles pour diriger le trafic réseau vers des destinations spécifiques, que ce soit à l'échelle d'un réseau local (LAN) ou à l'échelle d'Internet.

Il existe deux versions principales d'adresses IP :

- **IPv4 (Internet Protocol version 4)** : C'est la version la plus couramment utilisée d'adresses IP. Les adresses IPv4 sont représentées sous la forme de quatre nombres décimaux séparés par des points (par exemple, 192.168.1.1). Chaque numéro peut varier de 0 à 255, ce qui permet environ 4,3 milliards d'adresses uniques. Cependant, en raison de la croissance d'Internet, ces adresses s'épuisent.
- **IPv6 (Internet Protocol version 6)** : Conçu pour remédier à la pénurie d'adresses IPv4, IPv6 utilise une notation hexadécimale plus longue, composée de huit groupes de quatre caractères (par exemple, 2001:0DB8:85A3:0000:0000:8A2E:0370:7334). Cela permet une quantité astronomique d'adresses uniques, ce qui résout le problème de l'épuisement des adresses.

Les adresses IP sont utilisées pour acheminer les données sur un réseau, en indiquant l'expéditeur, le destinataire et les chemins intermédiaires. L'adresse IP d'un périphérique peut être statique (fixe) ou dynamique (attribuée automatiquement par un serveur DHCP). De plus, les adresses IP sont souvent associées à un masque de sous-réseau qui détermine la portée du réseau auquel l'adresse appartient.

→ À quoi sert un IP ?

Une adresse IP (Internet Protocol) sert principalement à identifier de manière unique un périphérique ou un ordinateur sur un réseau IP, permettant ainsi la communication et le routage des données.

→ Qu'est-ce qu'une adresse MAC ?

Une **adresse MAC** (Media Access Control) est une adresse unique attribuée à une carte réseau ou à une interface réseau d'un périphérique, comme un ordinateur, un smartphone, un routeur, ou un commutateur. Cette adresse est utilisée au niveau de la couche de liaison de données du modèle OSI (couche 2) pour identifier de manière unique un périphérique au sein d'un réseau local (LAN). Les adresses MAC sont attribuées par les fabricants de cartes réseau et sont généralement permanentes, c'est-à-dire qu'elles ne changent pas pendant la durée de vie du périphérique. Chaque adresse MAC est composée de 12 caractères hexadécimaux, soit 6 octets. Par exemple, une adresse MAC peut ressembler à ceci : 00:1A:2B:3C:4D:5E.

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

Les adresses IP publiques et privées sont deux concepts clés en réseau informatique, et elles servent à différencier les types d'adresses IP utilisés dans divers contextes. Voici une explication plus détaillée de chaque type d'adresse IP :

Adresse IP Publique :

- Une adresse IP publique est une adresse qui est visible sur Internet et peut être utilisée pour identifier un dispositif connecté à Internet de manière unique. Chaque périphérique connecté à Internet doit avoir une adresse IP publique unique pour être identifiable et accessible à d'autres dispositifs sur Internet.
- Les serveurs web, les serveurs de messagerie, les sites web, et d'autres ressources accessibles via Internet sont généralement associés à des adresses IP publiques pour permettre aux utilisateurs d'accéder à ces services depuis n'importe où dans le monde.
- Les adresses IP publiques sont nécessaires pour acheminer le trafic sur Internet, car elles permettent aux routeurs de diriger les données vers les destinations appropriées.

Adresse IP Privée :

- Une adresse IP privée est une adresse utilisée à l'intérieur d'un réseau local (LAN) ou d'une organisation pour identifier les périphériques connectés au réseau local. Ces adresses ne sont pas routables sur Internet et ne sont pas visibles depuis l'extérieur du réseau local.
- Les adresses IP privées sont définies dans certaines plages réservées spécifiquement à cet usage. Les plages d'adresses IP privées les plus couramment utilisées sont les suivantes :
 - 10.0.0.0 à 10.255.255.255 (plage privée de classe A)
 - 172.16.0.0 à 172.31.255.255 (plage privée de classe B)
 - 192.168.0.0 à 192.168.255.255 (plage privée de classe C)
- Les adresses IP privées sont utilisées pour attribuer des adresses aux dispositifs du réseau local et pour permettre la communication au sein du LAN. Les routeurs sont responsables de la traduction des adresses IP privées en adresses IP publiques lors de la communication avec Internet.
- Les adresses IP privées contribuent à renforcer la sécurité en limitant la visibilité des dispositifs du réseau local depuis Internet.

La Plateforme

→ Quelle est l'adresse de ce réseau ?

L'adresse du réseau est 192.168.1.0

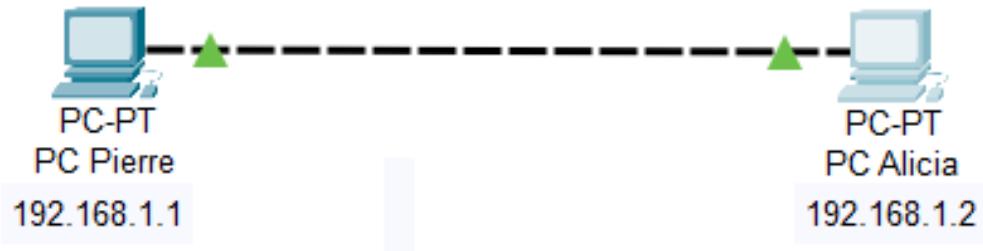
Adresse du PC Pierre :

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0

Adresse du PC Alicia :

IP Configuration	
<input type="radio"/> DHCP	
<input checked="" type="radio"/> Static	
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0

Communication entre le PC Pierre et le PC Alicia :



Job 5

Adresse IP du PC Pierre :

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

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::230:A3FF:FE26:CD2A
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
```

Adresse du PC Alicia :

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

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::203:E4FF:FE42:6B35
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:\>
```

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

Pour vérifier l'IP des machines, j'ai utilisé la commande ipconfig.

Job 6

Ping du 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

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
```

Ping du PC Alicia :

```
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

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
```

→ Quelle est la commande permettant de Ping entre des PC ?

Pour ping entre des PC, on utilise la commande ping suivie d'une adresse IP.

Job 7

Ping du PC Pierre éteint :

```
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, le PC de Pierre n'a pas reçu les paquets envoyés par Alicia.

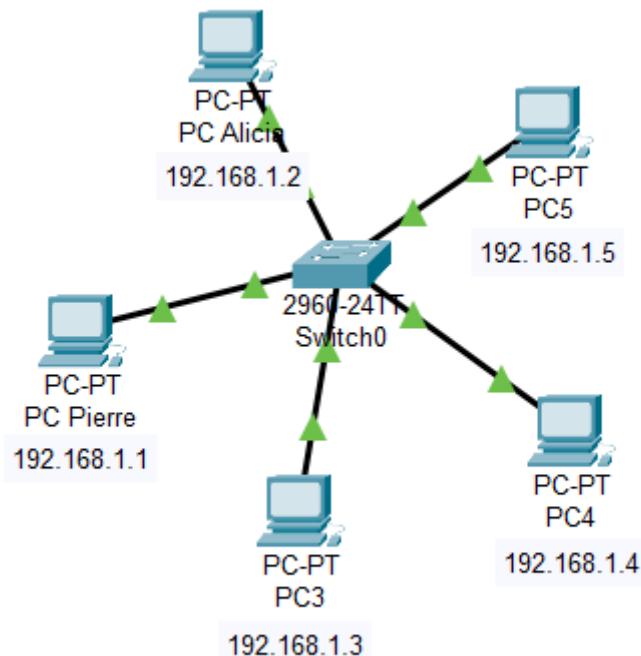
→ Expliquez pourquoi.

Le PC de Pierre n'a pas reçu les paquets envoyés par Alicia puisque le PC est éteint. Lorsque l'ordinateur est éteint, sa carte réseau et d'autres composants ne sont pas actifs et ne peuvent donc pas recevoir de données réseau. Il n'y a pas de moyen pour le PC de réagir aux paquets entrants tant qu'il est éteint.

La Plateforme

Job 8

Sous-réseau comprenant 5 PC et 1 switch :



Ping de chaque PC à partir du PC 3 :

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.255

Pinging 192.168.1.255 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.255:
    Packets: Sent = 4, Received = 24, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

Différences entre un hub et un switch :

• **Méthode de transmission des données**

- **Hub** : Un hub fonctionne au niveau physique (couche 1 du modèle OSI) et transmet les données à tous les périphériques connectés sur le même réseau, quelle que soit la destination des données. Cela signifie que lorsque des données sont envoyées à un périphérique via un hub, elles sont diffusées à tous les ports du hub, ce qui peut entraîner une utilisation inefficace de la bande passante et des collisions sur le réseau.
- **Switch** : Un switch fonctionne au niveau de la couche liaison de données (couche 2 du modèle OSI) et analyse l'adresse MAC (adresse matérielle) de chaque trame de données entrante pour décider vers quel périphérique spécifique elle doit être transmise. Les données sont acheminées uniquement vers le port du switch associé au périphérique de destination, ce qui permet d'économiser la bande passante et d'améliorer l'efficacité du réseau.

• **Efficacité et bande passante**

- **Hub** : En raison de sa méthode de diffusion des données, un hub peut entraîner un trafic inutile et des collisions, ce qui peut affecter la performance globale du réseau, en particulier lorsqu'un grand nombre de périphériques sont connectés.
- **Switch** : Un switch est beaucoup plus efficace car il achemine les données uniquement vers le périphérique de destination approprié, ce qui réduit les collisions et optimise la bande passante. Les réseaux basés sur des switches sont généralement plus rapides et plus efficaces.

• **Sécurité**

- **Hub** : Les données sont diffusées à tous les périphériques connectés, ce qui signifie que tous les dispositifs du réseau peuvent potentiellement intercepter les données destinées à un autre périphérique. Cela peut poser des problèmes de sécurité, en particulier dans un environnement où la confidentialité des données est importante.
- **Switch** : Les données sont acheminées uniquement vers le périphérique de destination, ce qui améliore la sécurité en limitant l'accès aux données aux seuls destinataires prévus.

• **Coût**

- **Hub** : Les hubs sont généralement moins chers que les switches en raison de leur simplicité et de leur méthode de fonctionnement.
- **Switch** : Les switches sont généralement plus coûteux que les hubs, mais offrent des performances et une efficacité supérieures, ce qui en fait un choix plus courant pour les réseaux modernes.

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

Fonctionnement d'un Hub :

Un hub fonctionne principalement au niveau de la couche physique (couche 1 du modèle OSI). Son rôle principal est de répéter les signaux entrants à tous les ports, ce qui signifie que toute donnée entrante sur un port est répliquée et envoyée à tous les autres ports. Contrairement à un commutateur qui prend en compte les adresses MAC pour diriger le trafic uniquement vers le port approprié, un hub n'a aucune connaissance des adresses MAC et ne prend pas de décisions de routage.

Avantages d'un Hub	Inconvénients d'un Hub
Simplicité : Les hubs sont simples à configurer et à utiliser. Il n'y a généralement pas de configuration complexe à effectuer.	Diffusion du trafic : Toutes les données envoyées à un périphérique sont diffusées à tous les autres périphériques, ce qui entraîne une utilisation inefficace de la bande passante. Cela peut entraîner des collisions de données, ce qui affecte les performances du réseau
Coût : Les hubs sont généralement moins chers que les commutateurs, ce qui en fait une option économique pour des réseaux de base.	Manque de sécurité : En raison de la diffusion du trafic, les données sensibles peuvent être interceptées par n'importe quel périphérique connecté au hub. Les hubs offrent peu de sécurité pour protéger les données.
	Performances limitées : Les performances des hubs sont généralement limitées en raison des collisions fréquentes et du partage de la bande passante.
	Obsolescence : Les hubs sont devenus obsolètes dans les réseaux modernes en raison de leurs limitations en termes de performances et de sécurité. Les commutateurs offrent une meilleure efficacité et sont désormais largement utilisés.

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

Avantages d'un Switch	Inconvénients d'un Switch
Efficacité du trafic : Les commutateurs analysent les adresses MAC (adresses matérielles) des dispositifs connectés pour acheminer le trafic uniquement vers le port approprié, ce qui évite la diffusion à tous les ports. Cela améliore l'efficacité du réseau en réduisant les collisions de données et en optimisant l'utilisation de la bande passante.	Coût : Les commutateurs sont généralement plus coûteux que les hubs, ce qui peut être un inconvénient pour les budgets limités. Cependant, leurs avantages en termes de performances et de sécurité justifient souvent ce coût supplémentaire.
Sécurité améliorée : Étant donné que les commutateurs acheminent les données uniquement vers le périphérique de destination approprié, cela limite la visibilité des données aux seuls destinataires prévus, améliorant ainsi la sécurité. De plus, des fonctionnalités de sécurité avancées, telles que la segmentation VLAN, peuvent être mises en œuvre sur un switch.	Complexité : Les commutateurs offrent de nombreuses fonctionnalités avancées, ce qui peut rendre leur configuration et leur gestion plus complexes. Cela nécessite des connaissances techniques pour les administrateurs réseau.
Meilleures performances : Les switches permettent des performances plus élevées que les hubs en minimisant les collisions de données. Cela signifie que les réseaux basés sur des commutateurs sont plus rapides et plus réactifs.	Surdimensionnement : Si un réseau est petit ou ne nécessite pas de performances ou de fonctionnalités avancées, un switch peut être considéré comme surdimensionné, ce qui entraîne un coût inutile.
Gestion plus avancée : Les switches offrent généralement des fonctionnalités de gestion avancées, telles que la qualité de service (QoS), la surveillance du trafic, la gestion des VLAN et la prise en charge de protocoles de routage. Cela permet de personnaliser et d'optimiser le réseau en fonction des besoins spécifiques.	
Extensibilité : Les commutateurs sont extensibles, ce qui signifie que vous pouvez les empiler pour augmenter le nombre de ports ou ajouter des fonctionnalités. Ils sont adaptés aux réseaux en croissance.	

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

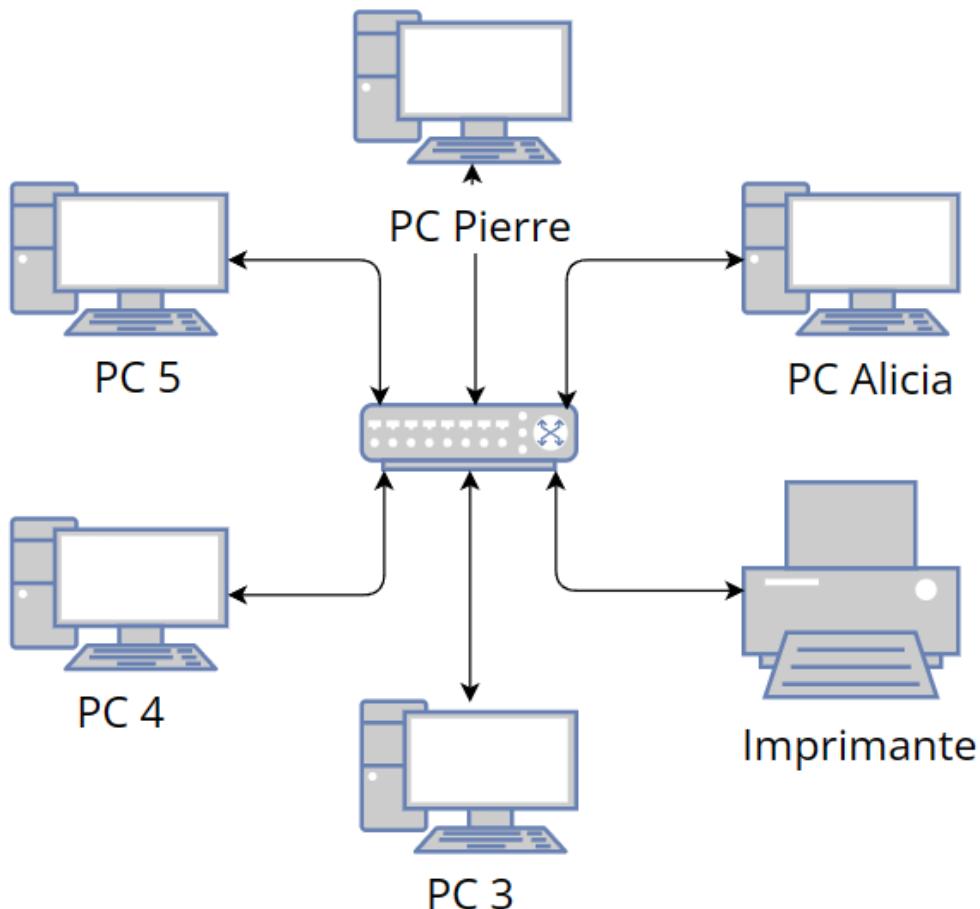
Un switch gère le trafic réseau en utilisant une approche basée sur la couche liaison de données (couche 2 du modèle OSI) pour diriger les données efficacement et précisément vers les périphériques de destination appropriés. Voici comment un switch gère le trafic réseau :

- **Apprentissage des adresses MAC** : Lorsque les dispositifs sont connectés à un switch, ce dernier commence par apprendre les adresses MAC de chaque périphérique en surveillant le trafic entrant. Chaque carte réseau (NIC) a une adresse MAC unique, qui est utilisée pour identifier de manière unique un périphérique sur le réseau.
- **Table de commutation (Switching Table)** : Le switch utilise une table de commutation (également appelée table d'adresses MAC) pour stocker les adresses MAC apprises associées aux ports du switch. Cette table est constamment mise à jour à mesure que le switch apprend de nouvelles adresses MAC. Elle indique quelles adresses MAC sont associées à quels ports du switch.
- **Acheminement des données** : Lorsqu'une trame de données arrive sur un port du switch, le switch examine l'adresse MAC de destination de la trame. En se référant à sa table de commutation, il détermine le port auquel la trame doit être acheminée pour atteindre le périphérique de destination. Il n'envoie pas la trame à tous les ports, mais uniquement au port approprié.
- **Diffusion (Broadcast)** : Si le switch ne trouve pas l'adresse MAC de destination dans sa table de commutation, il diffuse la trame à tous les ports, car il ne sait pas où se trouve le périphérique. Cette diffusion est similaire au comportement d'un hub, mais elle est limitée aux trames pour lesquelles le switch n'a pas d'information sur l'adresse MAC de destination.

La Plateforme

Job 9

Schéma d'un réseau comprenant 5 PC, 1 switch et 1 imprimante :



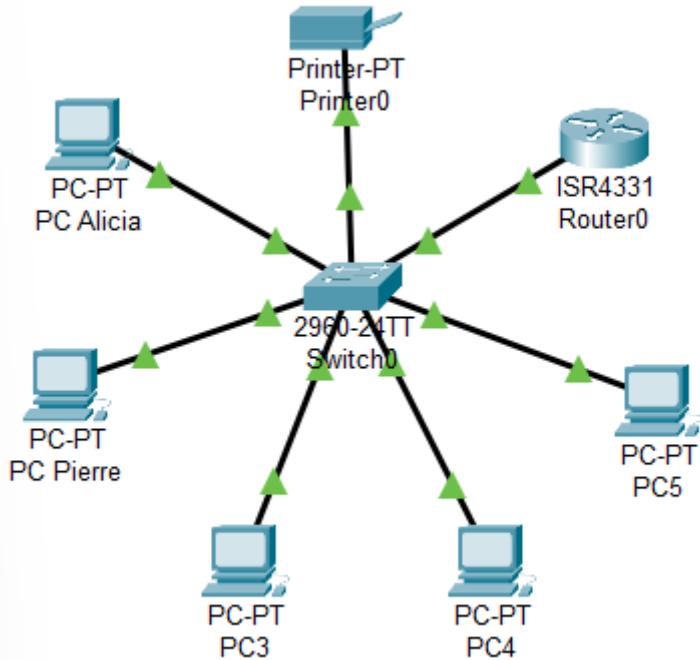
Faire un schéma pour un réseau est utile pour plusieurs raisons :

- Planifier la structure d'un réseau domestique ou professionnel
- Signaler et résoudre des problèmes de réseau
- Servir de documentation pour la communication externe, l'intégration, etc.

La Plateforme

Job 10

Réseau comprenant 5 PC, une imprimante, 1 switch et 1 routeur :



Configuration du routeur :

```
ip dhcp pool MonPool
Router(dhcp-config)#ip dhcp pool MonPool
Router(dhcp-config)# dns-server 8.8.8.8
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
```

Résultat du PC Pierre :

Gateway/DNS IPv4	
<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

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

Les adresses IP statiques et les adresses IP attribuées par DHCP (Dynamic Host Configuration Protocol) sont deux méthodes de configuration d'adresses IP pour les périphériques d'un réseau. Voici les principales différences entre les deux :

Adresse IP statique	Adresse IP attribuée par DHCP
<p>Configuration manuelle : Avec une adresse IP statique, l'administrateur réseau configure manuellement l'adresse IP pour chaque périphérique. Cela signifie que vous devez entrer l'adresse IP, le masque de sous-réseau, la passerelle par défaut et éventuellement les serveurs DNS manuellement sur chaque périphérique.</p>	<p>Configuration automatique : Avec le DHCP, le serveur DHCP attribue automatiquement une adresse IP à chaque périphérique lorsque celui-ci rejoint le réseau. Les clients DHCP obtiennent leur adresse IP, le masque de sous-réseau, la passerelle par défaut et les serveurs DNS sans intervention manuelle.</p>
<p>Stabilité : Les adresses IP statiques ne changent pas, sauf si elles sont modifiées manuellement. Cela garantit une stabilité dans les adresses IP des périphériques.</p>	<p>Dynamique : Les adresses IP attribuées par DHCP peuvent changer à chaque nouvelle connexion au réseau. Chaque fois qu'un périphérique se connecte, il peut recevoir une adresse IP différente, bien que le serveur DHCP puisse être configuré pour toujours attribuer la même adresse IP à un périphérique spécifique (ceci est appelé une "bail statique").</p>
<p>Prédéterminée : Chaque périphérique dispose d'une adresse IP spécifique qui est déterminée par l'administrateur. Cela peut être utile dans des cas où vous devez garantir que certains périphériques ont toujours la même adresse IP.</p>	<p>Évolutif : Le DHCP est particulièrement utile dans les réseaux où de nombreux périphériques se connectent et se déconnectent régulièrement, car il gère automatiquement l'attribution d'adresses IP.</p>
<p>Moins de trafic DHCP : L'utilisation d'adresses IP statiques réduit la charge sur le serveur DHCP, car il n'a pas besoin d'attribuer des adresses dynamiquement</p>	<p>Gestion centralisée : Le DHCP permet une gestion centralisée des adresses IP. Les administrateurs peuvent surveiller et gérer les adresses IP à partir du serveur DHCP.</p>

Job 11

Plan d'adressage :

Masque de sous-réseau	Gateway	Pool d'adresse user	Broadcast
255.255.255.240/28	10.0.0.0	10.0.0.1 à 10.0.0.14	10.0.0.15
255.255.255.224/27	10.0.0.16	10.0.017 à 10.0.046	10.0.0.47
255.255.255.224/27	10.0.0.48	10.0.0.49 à 10.0.0.78	10.0.0.79
255.255.255.224/27	10.0.0.80	10.0.0.81 à 10.0.0.110	10.0.0.111
255.255.255.224/27	10.0.0.112	10.0.0.113 à 10.0.0.142	10.0.0.143
255.255.255.224/27	10.0.0.144	10.0.0.145 à 10.0.0.174	10.0.0.175
255.255.255.128/25	10.0.1.0	10.0.1.1 à 10.0.1.126	10.0.1.127
255.255.255.128/25	10.0.1.128	10.0.1.129 à 10.0.1.254	10.0.1.255
255.255.255.128/25	10.0.2.0	10.0.2.1 à 10.0.2.126	10.0.2.127
255.255.255.128/25	10.0.2.128	10.0.2.129 à 10.0.2.254	10.0.2.255
255.255.255.128/25	10.0.3.0	10.0.3.1 à 10.0.3.126	10.0.3.127
255.255.255.0/24	10.0.4.0	10.0.4.1 à 10.0.4.254	10.0.4.255
255.255.255.0/24	10.0.5.0	10.0.5.1 à 10.0.5.254	10.0.5.255
255.255.255.0/24	10.0.6.0	10.0.6.1 à 10.0.6.254	10.0.6.255
255.255.255.0/24	10.0.7.0	10.0.7.1 à 10.0.7.254	10.0.7.255
255.255.255.0/24	10.0.8.0	10.0.8.1 à 10.0.8.254	10.0.8.255

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

Le choix de l'adresse 10.0.0.0 de classe se fait principalement pour sa large disponibilité d'adresse IP. En effet, les réseaux de classe A peuvent prendre en charge jusqu'à environ 16 millions d'hôtes.

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

Les différentes classes d'adresses IP (A, B, C, D et E) définissent des plages d'adresses IP spécifiques qui sont utilisées pour diverses fins dans le cadre du protocole Internet (IP). Chaque classe a ses propres caractéristiques et est destinée à des types de réseaux spécifiques. Voici un aperçu des principales différences entre les classes d'adresses IP :

Classe A	Plage d'adresses : 1.0.0.0 à 126.0.0.0 Masque de sous-réseau : 255.0.0.0 Utilisation : Les adresses de classe A sont principalement utilisées pour les réseaux de grande taille. Le premier octet identifie le réseau, tandis que les trois octets restants sont utilisés pour les hôtes. Les réseaux de classe A peuvent prendre en charge un grand nombre d'hôtes (environ 16 millions).
Classe B	Plage d'adresses : 128.0.0.0 à 191.0.0.0 Masque de sous-réseau : 255.255.0.0 Utilisation : Les adresses de classe B sont utilisées pour les réseaux de taille moyenne. Les deux premiers octets identifient le réseau, tandis que les deux derniers octets sont utilisés pour les hôtes. Les réseaux de classe B peuvent prendre en charge un nombre considérable d'hôtes (environ 65 000).
Classe C	Plage d'adresses : 192.0.0.0 à 223.0.0.0 Masque de sous-réseau : 255.255.255.0 Utilisation : Les adresses de classe C sont utilisées pour les réseaux de petite taille. Les trois premiers octets identifient le réseau, tandis que le dernier octet est utilisé pour les hôtes. Les réseaux de classe C prennent en charge un nombre limité d'hôtes (254 hôtes au maximum).
Classe D	Plage d'adresses : 224.0.0.0 à 239.0.0.0 Masque de sous-réseau : Non applicable Utilisation : Les adresses de classe D sont réservées pour la multidiffusion (broadcast sélectif) et ne sont pas utilisées pour l'adressage des hôtes individuels.
Classe E	Plage d'adresses : 240.0.0.0 à 255.0.0.0 Masque de sous-réseau : Non applicable Utilisation : Les adresses de classe E sont réservées à des fins expérimentales et ne sont pas couramment utilisées dans les réseaux publics.

Job 12

Modèle OSI :

Donnée	7 - Application Point d'accès aux services réseau	FTP, HTML,
Donnée	6 - Présentation Conversion et chiffrement des données	SSL/TLS
Donnée	5- Session Communication interhost	
Segment	4 - Transport Connexion de bout en bout et contrôle de flux (TCP)	TCP, UDP,
Paquet	3 - Réseau Détermine le parcours et l'adressage logique (IP)	IPv4, IPv6, routeur,
Trame	2- Liaison Adressage physique (MAC et LLC)	MAC, Ethernet, PPTP, Wi-Fi
Bit	1 - Physique Transmission binaire numérique ou analogique	fibre optique, câble RJ45

Job 13

→ Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau se compose des éléments suivants : une **Topologie en étoile** et de **Composant** (2 serveurs, 1 switch, 4 PC). Les différents dispositifs communiquent par Ethernet grâce à des câbles copper straight-through.

→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est 192.168.10.0/24

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

Pour obtenir le nombre de machines que l'on peut brancher source réseau, il faut d'abord prendre en compte les adresses IP déjà utilisées.

L'adresse réseau : 192.168.10.0

L'adresse de diffusion : 192.168.10.255

Les adresses IP des serveurs : 192.168.10.100 et 192.168.10.200

Il y a en tout 5 adresses IP déjà attribuées. Sachant que le réseau peut attribuer jusqu'à 256 adresses IP, il faut retirer 4 à ce nombre pour obtenir le nombre de machines que l'on peut brancher.

$$256 - 4 = 252$$

On peut donc brancher jusqu'à 252 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

Job 14

Calcul des adresses IP en binaire :

128	64	32	16	8	4	2	1	
1	0	0	1	0	0	0	1	
0	0	1	0	0	0	0	0	145.32.59.24
0	0	1	1	1	0	1	1	
0	0	0	1	1	0	0	0	
1	1	0	0	1	0	0	0	
0	0	1	0	1	0	1	0	200.42.129.16
1	0	0	0	0	0	0	1	
0	0	0	1	0	0	0	0	
0	0	0	0	1	1	1	0	
0	1	0	1	0	0	1	0	14.82.19.54
0	0	0	1	0	0	1	1	
0	0	1	1	0	1	1	0	

- 145.32.59.24 - 10010001.00100000.00111011.00011000
- 200.42.129.16 - 11001000.00101010.10000001.00010000
- 14.82.19.54 - 00001110.01010010.00010011.00110110

Job 15

→ Qu'est-ce que le routage ?

Le routage est le processus de transfert de données entre différents réseaux informatiques ou sous-réseaux. Il consiste à déterminer le chemin optimal pour faire parvenir les données d'un point de départ (source) à un point de destination (destination) à travers un réseau de dispositifs interconnectés. Le routage est essentiel dans les réseaux informatiques car il permet aux données de circuler efficacement entre les différents réseaux, qu'ils soient locaux ou étendus.

→ Qu'est-ce qu'un gateway ?

Une gateway (passerelle en français) est un dispositif ou un logiciel qui connecte deux réseaux informatiques différents, permettant ainsi la communication et le transfert de données entre ces réseaux. Les passerelles sont essentielles pour permettre la connectivité entre des réseaux qui utilisent des protocoles, des architectures ou des technologies différentes.

→ Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel (Virtual Private Network en anglais), est une technologie qui permet de créer un réseau sécurisé et chiffré, même à travers un réseau public comme Internet. Un VPN fonctionne en établissant une connexion sécurisée entre l'appareil de l'utilisateur (tel qu'un ordinateur ou un smartphone) et un serveur VPN. Les données sont ensuite acheminées de manière sécurisée à travers cette connexion, garantissant la confidentialité et la sécurité de la communication.

→ Qu'est-ce qu'un DNS ?

Le DNS, ou Domain Name System (Système de Noms de Domaine en français), est un protocole et un système informatique essentiel sur Internet. Son rôle principal est de traduire les noms de domaine conviviaux que nous utilisons pour accéder à des sites web, des services en ligne et d'autres ressources sur Internet en adresses IP, qui sont les identifiants numériques des serveurs et des dispositifs réseau.