

Runtrack Réseau



Cisco Packet Tracer est un logiciel permettant de simuler le fonctionnement d'un réseau informatique. Avec Cisco Packet Tracer, vous pouvez concevoir, configurer et dépanner des réseaux informatiques simples et complexes.

JOB 2

1. Qu'est-ce qu'un réseau ?

→ Un réseau est un groupe d'appareils connectés qui peuvent partager des informations. Par exemple, un réseau local (LAN) à la maison relie des ordinateurs, des smartphones et des imprimantes pour partager des fichiers. Internet est un réseau mondial qui relie des milliards d'ordinateurs à travers le monde pour permettre l'accès à des sites web et la communication.

2. À quoi sert un réseau informatique ?

→ Le réseau informatique offre différentes fonctionnalités :

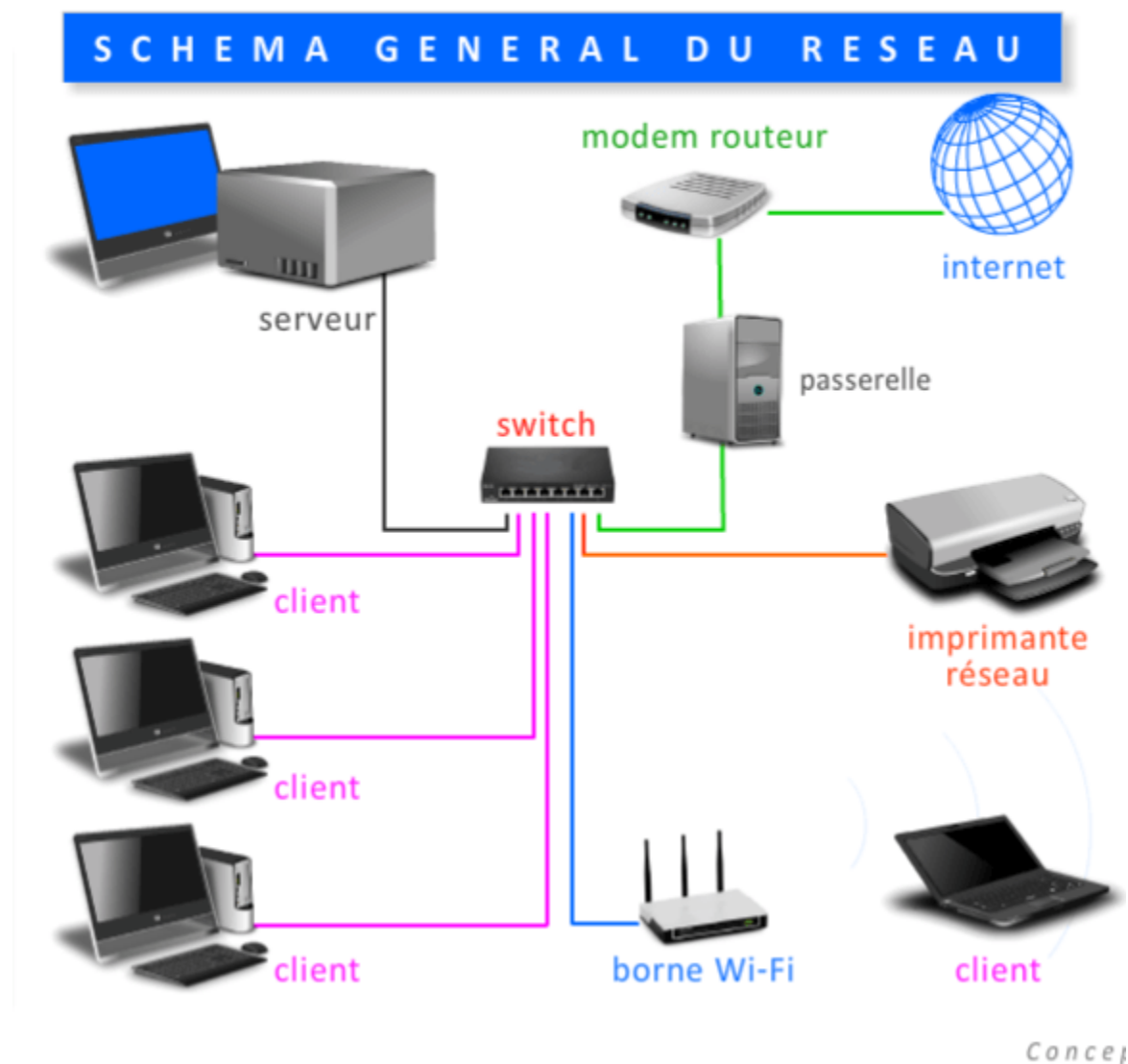
- Partage de données
- Partage de ressources physiques : imprimantes etc.
- Partage d'application et logiciel ne nécessitant donc pas leur installation
- Stockage et sauvegarde centralisé des données
- Recherche d'informations (internet)
- Communication à distance
- Le partage de la puissance de calcul et la capacité de stockage
- Etc

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

→ matériel pour construire un réseau :

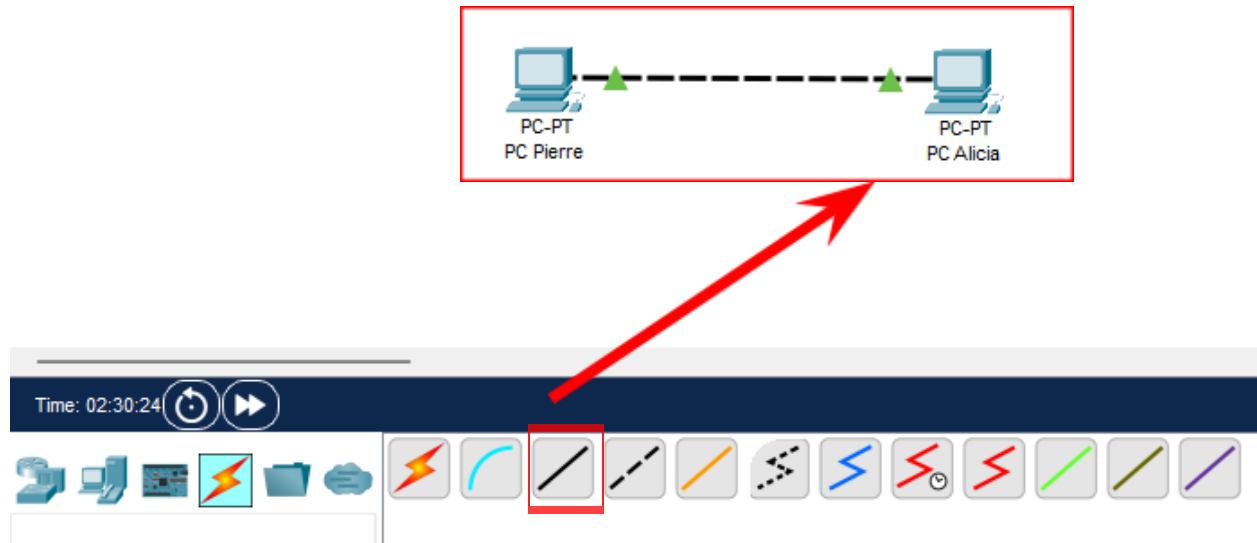
Appareils finaux	dispositifs individuels se connectent au réseau (ordinateurs, des smartphones, des imprimantes, des tablettes). Ils génèrent et consomment des données.
Routeur	dirige le trafic entre les appareils finaux et de gérer les adresses IP. Il connecte le réseau local à d'autres réseaux, notamment Internet.
Commutateur (Switch)	Un commutateur est utilisé pour connecter plusieurs appareils au sein du réseau local. Il agit en tant que point de distribution pour transférer des données directement entre les appareils connectés, réduisant ainsi le trafic inutile.
Câbles	utilisés pour connecter les appareils au réseau. Ils transmettent les données sous forme de signaux électriques.

Points d'accès	utilisés pour fournir une connexion sans fil (Wi-Fi), . Les points d'accès permettent aux appareils Wi-Fi de se connecter au réseau câblé.
Modem	convertit les signaux numériques de votre réseau en signaux analogiques pour se connecter à Internet via votre fournisseur de services Internet (FAI).
Serveurs	stockent des données ou des services que les autres appareils du réseau peuvent utiliser. Par exemple, un serveur de fichiers stocke des fichiers partagés, tandis qu'un serveur web héberge des sites web.



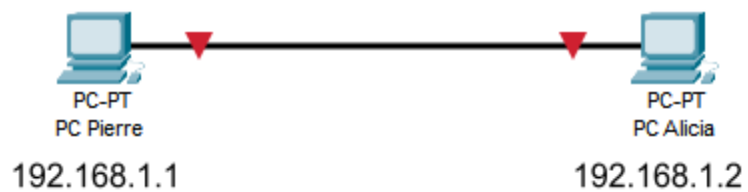
JOB 3

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



J'ai choisie le câble (Copper Straight-Through) parce-que c'est l'option qui permet de choisir le type de connection entre les 2 PC en "Fast Ethernet", on peut choisir l'option du câble (Automatically Choose Connection Type) est indiqué le type de connection ethernet.

JOB 4



→ Qu'est-ce qu'une adresse IP ?

Le terme « Adresse IP » désigne une « adresse de protocole Internet ». Le protocole Internet est un ensemble de règles qui régissent la communication sur Internet, qu'il s'agisse d'envoyer des messages, de diffuser des vidéos ou de se connecter à un site Web. **Une adresse IP identifie un réseau ou un appareil sur Internet. Chaque adresse IP ne peut être attribuée qu'une seule fois au même moment au sein d'un réseau.**

→ À quoi sert un IP ?

Il sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC est un identifiant unique attribué à un contrôleur d'interface réseau pour servir d'adresse réseau dans les communications au sein d'un segment de réseau. Cette utilisation est courante dans la plupart des technologies de mise en réseau IEEE 802, y compris Ethernet, Wi-Fi et Bluetooth.

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

Une adresse **IP publique** vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse **IP privée** est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

Adresses IP privées	
• Non routable	
Classe	Plage d'adresse IP privée
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

→ Quelle est l'adresse de ce réseau ?

192.168.1.1 en binaire : 11000000.10101000.00000001.00000001

255.255.255.0 en binaire : 11111111.11111111.11111111.00000000

en utilisant une opération de "ET logique entre les deux on obtient :

11000000.10101000.00000001.00000000 conversion en décimal 192.168.1.0

voilà l'adresse de ce réseau.

JOB 5

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:BCFF:FEA1:2825
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

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

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:43FF:FE36:2E5B
    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
```

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

ligne de commande utilisée : `ipconfig` cette commande nous affiche les informations du réseau sélectionné.

JOB 6

teste de connectivité entre le PC de Pierre et celui d'Alicia, en utilisant la commande Ping.
Ping depuis le PC Pierre vers PC Alicia

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

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

Ping depuis le PC Alicia vers PC Pierre

```
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
```

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

ligne de commande utilisée : **ping** cette commande nous permet d'envoyer des paquet vers un autre réseau pour vérifier la communication entre les deux ordinateurs.

JOB 7

```
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.

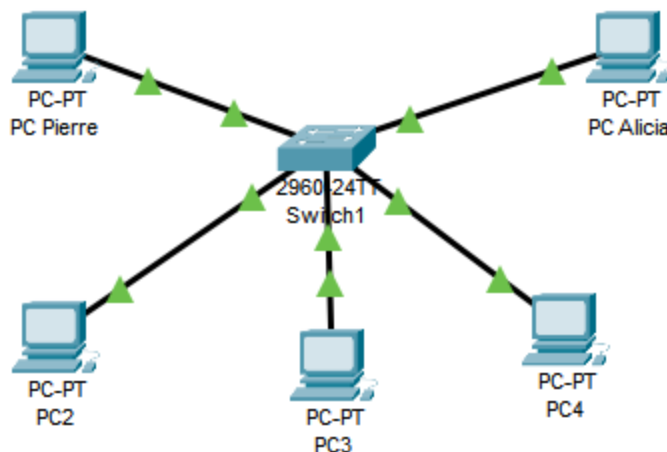
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

Non le PC de Pierre ne reçoit aucun paquets de la part d'Alicia, on observe que le taux de Packets Lost est de 100% (Lost=4).

explication : pour que le PC de Pierre reçoive les paquets "ping" envoyés par Alicia, il doit être allumé et connecté au réseau. Lorsque vous éteignez un ordinateur, son interface réseau est désactivée, ce qui signifie qu'il ne peut pas répondre aux requêtes réseau, y compris les requêtes "ping".

JOB 8



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

Hub : Un dispositif de couche 1 (couche physique) du modèle OSI. Il fonctionne en répétant simplement les signaux entrant à tous les ports, sans se soucier de leur destination. Cela signifie que toutes les données reçues par un port du hub sont diffusées à tous les autres ports.

Switch : Un dispositif de couche 2 (couche liaison de données) du modèle OSI. Il examine l'adresse MAC de chaque paquet de données entrant et décide sur quel port envoyer le paquet en fonction de cette adresse. Il maintient une table de correspondance des adresses MAC des appareils connectés et utilise ces informations pour acheminer efficacement les données vers le port de destination approprié.

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

Fonctionnement d'un hub : Un hub est essentiellement un répéteur. Lorsqu'il reçoit des données sur un port, il répète ces données à tous les autres ports sans aucune intelligence ou traitement.

1. Un appareil connecté à un port du hub envoie des données.
2. Le hub reçoit ces données et les répète à tous les autres ports, sans se soucier de la destination.
3. Tous les appareils connectés au hub, y compris le destinataire réel et tous les autres, reçoivent ces données.

Avantages: Simplicité, coût.

Inconvénients: Collisions, Bande passante partagée, Manque de sécurité, Obsolescence.

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

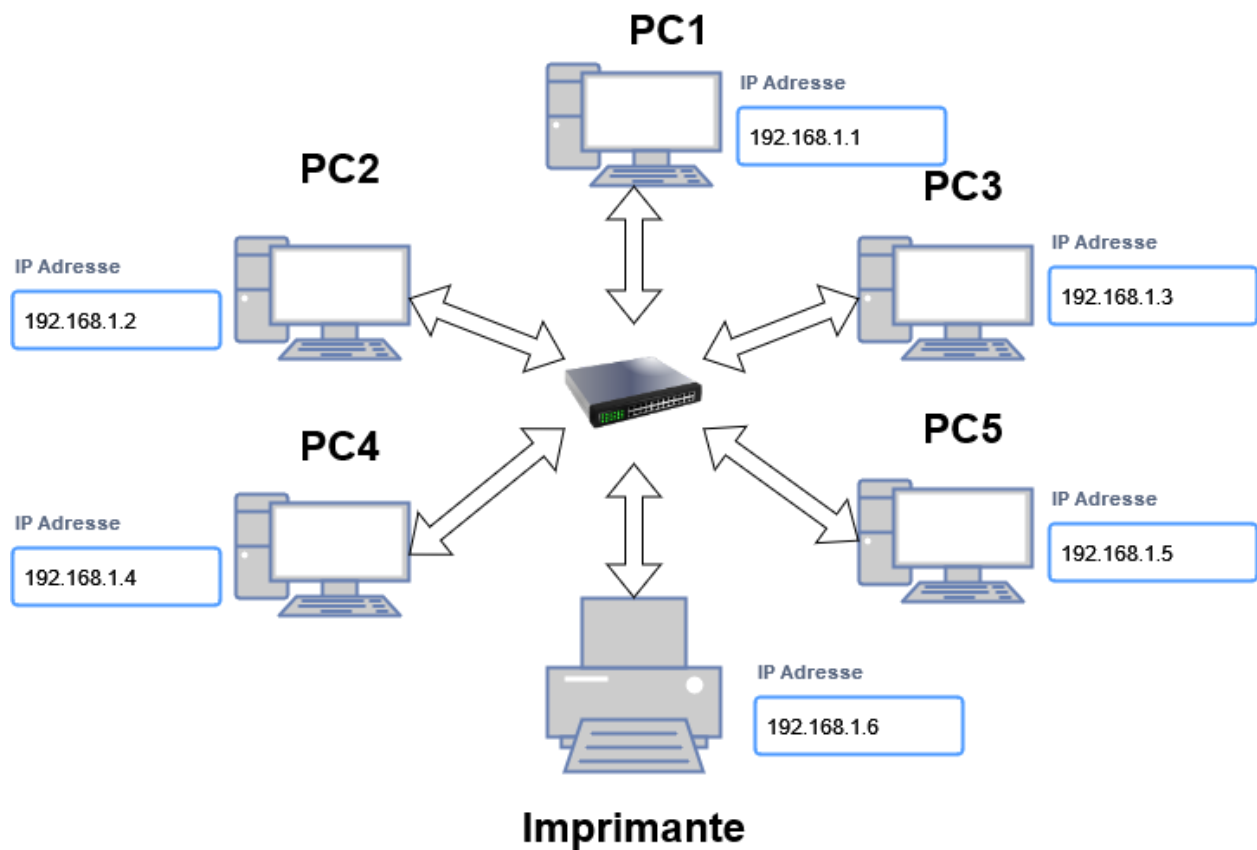
Avantages d'un switch: Acheminent efficacement le trafic réseau, offrent de meilleures performances par rapport aux hubs, fournissent une sécurité de base car ils ne diffusent pas de données à tous les ports, isolent le trafic entre les ports, ce qui signifie que les problèmes sur un port (comme les collisions) n'affectent pas les autres ports, gèrent une table de correspondance des adresses MAC des appareils connectés, extensibles, ce qui signifie que vous pouvez connecter plusieurs switches ensemble pour étendre votre réseau.

Inconvénients d'un switch: Généralement plus chers que les hubs, nécessitent une configuration plus avancée que les hubs, nécessitent une gestion active pour garantir le bon fonctionnement du réseau, Bien que les switches aient des performances élevées, ils peuvent être surchargés si trop de trafic est généré simultanément.

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

En général, un switch gère le trafic réseau en apprenant les adresses MAC des appareils connectés à ses ports, les associant à des ports spécifiques dans une table de correspondance, puis acheminant les trames de données uniquement vers les ports appropriés en fonction de l'adresse MAC de destination, minimisant ainsi le trafic inutile. Il évite les boucles grâce à des protocoles de prévention de boucles, améliore la sécurité en limitant la diffusion, et garantit des performances efficaces en réduisant les collisions et en optimisant l'utilisation de la bande passante, faisant des switches des composants essentiels des réseaux modernes.

JOB 9



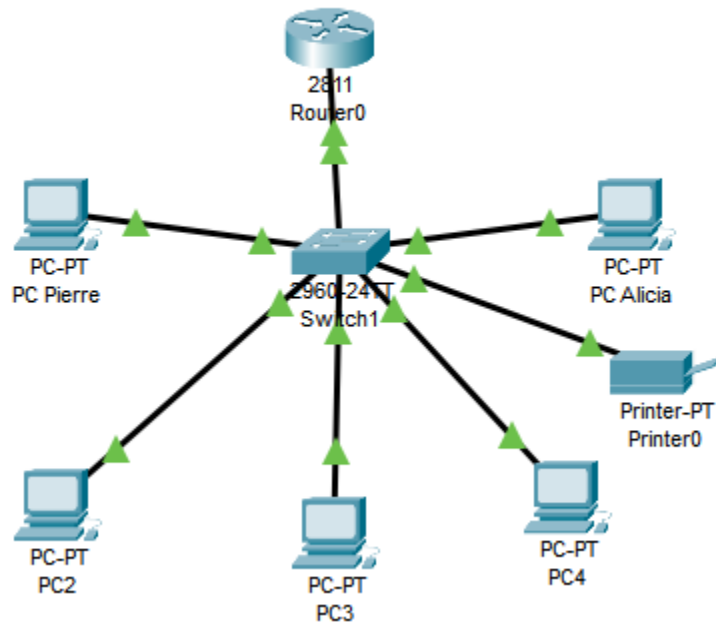
Un schéma de réseau offre une visualisation claire, une documentation précise et facilite le dépannage, ce qui en fait un outil essentiel pour la gestion et la maintenance des infrastructures réseau.

Visualisation claire : Un schéma de réseau offre une représentation visuelle de l'ensemble de votre infrastructure, y compris les appareils, les connexions et la topologie.

Documentation précise : Un schéma de réseau sert de documentation précise de votre infrastructure.

Dépannage facilité : En cas de problèmes ou de pannes réseau, un schéma bien conçu permet d'identifier rapidement la source du problème.

JOB 10



Configuration du DHCP:

Sur le routeur, configurez l'interface fa0/0 pour qu'elle serve de passerelle par défaut pour notre réseau local.

Dans le serveur, nous définirons un pool DHCP d'adresses IP à attribuer aux hôtes, une passerelle par défaut pour le réseau local et un serveur DNS.

```
Router(config)#ip dhcp pool MY_LAN
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.10
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

Nous pouvons ajouter la commande `ip dhcp excluded-address` à notre configuration afin de configurer le routeur pour qu'il exclue les adresses 192.168.1.1 à 192.168.1.10 lors de l'attribution d'adresses aux clients. La commande `ip dhcp excluded-address` peut être utilisée pour réserver des adresses qui sont attribuées de manière statique à des hôtes clés.

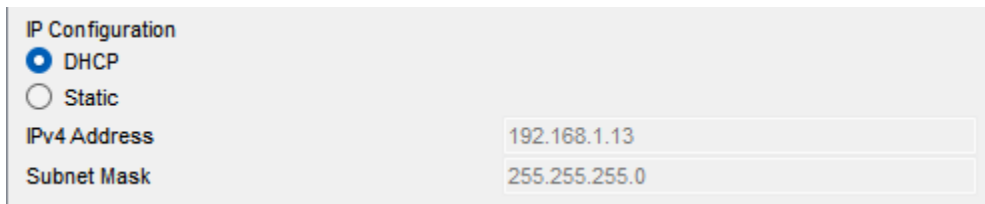
Allez maintenant sur chaque PC et dans leurs onglets de configuration IP, activez DHCP. Chaque PC devrait pouvoir obtenir une adresse IP, une passerelle par défaut et un serveur DNS.

Exemple :

The screenshot shows the 'IP Configuration' window for 'PC Pierre'. Under 'IP Configuration', the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The 'IPv4 Address' field contains the value '192.168.1.11', and the 'Subnet Mask' field contains the value '255.255.255.0'.

IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	192.168.1.11
Subnet Mask	255.255.255.0

PC Pierre

The screenshot shows the 'IP Configuration' window for 'PC Alicia'. Under 'IP Configuration', the 'DHCP' radio button is selected, and the 'Static' radio button is unselected. The 'IPv4 Address' field contains the value '192.168.1.13', and the 'Subnet Mask' field contains the value '255.255.255.0'.

IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	192.168.1.13
Subnet Mask	255.255.255.0

PC Alicia

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

La principale différence réside dans le mode d'attribution des adresses IP. Les adresses IP statiques sont configurées manuellement et restent constantes, tandis que les adresses IP attribuées par DHCP sont gérées de manière dynamique par un serveur DHCP, ce qui simplifie la gestion, réduit les risques de conflits d'adresses et optimise l'utilisation des adresses IP. Le choix entre les deux dépend des besoins spécifiques du réseau et de la complexité de la gestion des adresses.

JOB 11

Plan d'adressage.

- 10.0.0.0/28 (12 hôtes)
- 10.0.0.16/27 (30 hôtes)
- 10.0.0.48/27 (30 hôtes)
- 10.0.0.80/27 (30 hôtes)
- 10.0.0.112/27 (30 hôtes)

- 10.0.0.144/25 (120 hôtes)
- 10.0.0.192/25 (120 hôtes)
- 10.0.0.240/25 (120 hôtes)
- 10.0.1.0/25 (120 hôtes)
- 10.0.1.128/25 (120 hôtes)
- 10.0.1.0/24 (160 hôtes)
- 10.0.1.1/24 (160 hôtes)
- 10.0.1.2/24 (160 hôtes)
- 10.0.1.3/24 (160 hôtes)
- 10.0.1.4/24 (160 hôtes)

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

l'adresse IP 10.0.0.0 de classe A a été choisie en raison de sa grande capacité d'adressage et de sa réservation pour une utilisation interne dans des réseaux privés.

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

Les adresses IP se divisent en adresses publiques et privées, où les premières identifient les appareils directement connectés à Internet, tandis que les secondes sont utilisées à l'intérieur de réseaux privés, comme les réseaux locaux d'entreprises. Les adresses IP publiques sont gérées et allouées à l'échelle mondiale, tandis que les adresses privées ne sont pas routables sur Internet. De plus, les adresses IP peuvent être statiques (assignées manuellement et ne changent pas) ou dynamiques (attribuées automatiquement et changeantes). En outre, il existe deux versions principales d'adresses IP : IPv4 (32 bits) et IPv6 (128 bits), cette dernière étant introduite en raison de l'épuisement des adresses IPv4. En résumé, ces différentes catégories d'adresses IP servent à répondre aux besoins de communication à différentes échelles, que ce soit à l'échelle locale, globale ou pour gérer les réseaux privés.

JOB 12

Modèle OSI	Rôle	Matériels / Protocoles
Couche 7 - La couche d'application	la couche supérieure et la plus proche de l'utilisateur. Elle comprend les applications réseau elles-mêmes, comme les navigateurs web, les clients de messagerie et d'autres logiciels qui interagissent directement avec l'utilisateur.	FTP (File Transfer Protocol) HTML
Couche 6 - La couche de présentation	se charge de la traduction, de la compression et du chiffrement des données.	SSL/TLS (Secure Sockets Layer/Transport Layer Security)
Couche 5 - La couche session	établit, maintient et termine les sessions de communication entre les applications. Elle gère la synchronisation et la reprise en cas de perte de connexion.	PPTP (Point-to-Point Tunneling Protocol)
Couche 4 - La couche de transport	responsable du contrôle de bout en bout de la communication. Elle assure la fiabilité des données, effectue le contrôle de flux et la segmentation (division) des données si nécessaire.	TCP (Transmission Control Protocol) UDP (User Datagram Protocol)
Couche 3 - La couche réseau	s'occupe de l'acheminement des données à travers le réseau. utilise des adresses IP pour déterminer la meilleure route entre l'expéditeur et le destinataire.	IPv4 IPv6 Routeur

Couche 2 – La couche de liaison de données	communication entre des appareils directement connectés.	MAC (Media Access Control) Wi-Fi
Couche 1 – La couche physique	transmission brute des données sur le support physique du réseau, que ce soit un câble en cuivre, une fibre optique ou des ondes radio.	Ethernet Fibre optique Cable RJ45

JOB 13

→ Quelle est l'architecture de ce réseau ?

Cette architecture réseau est un réseau local (LAN) simple utilisant des adresses IP privées de classe C (192.168.x.x) avec un masque de sous-réseau 255.255.255.0. Les appareils sur ce réseau sont tous regroupés dans le même sous-réseau, ce qui permet une communication directe entre eux sans passer par un routeur.

→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est 192.168.10.0. C'est la première adresse utilisable de la plage d'adresses IP 192.168.10.0 à 192.168.10.254 avec un masque de sous-réseau de 255.255.255.0.

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

Pour déterminer le nombre de machines qu'on peut brancher sur ce réseau : 255.255.255.0 ou /24, ce masque signifie que les 24 premiers bits de l'adresse IP sont réservés pour l'identification du réseau, laissant 8 bits pour l'identification des hôtes

$2^8 - 2 = 254$, normalement c'est 256 mais on soustrait 2 parce que l'adresse réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255) ne sont généralement pas attribuées aux machines.

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

L'adresse de diffusion de ce réseau est 192.168.10.255.

JOB 14

Conversion des adresses IP suivantes en binaires :

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 essentiel de transmission de données d'un réseau à un autre, ou au sein du même réseau, en déterminant le meilleur chemin pour que ces données atteignent leur destination. Les routeurs jouent un rôle central dans ce processus, en consultant leurs tables de routage et en utilisant des protocoles de routage pour décider comment acheminer les données vers la destination souhaitée. Cela permet aux données de circuler efficacement à travers de multiples réseaux, de sauter d'un routeur à l'autre, et finalement d'atteindre leur destinataire, contribuant ainsi au fonctionnement fluide d'Internet et d'autres réseaux informatiques.

Qu'est-ce qu'un gateway ?

Une passerelle, également connue sous le nom de "gateway", est un dispositif matériel ou logiciel essentiel qui relie et permet la communication entre deux réseaux informatiques distincts, qu'ils utilisent différents protocoles de communication ou qu'ils appartiennent à des domaines de gestion différents. Les passerelles jouent divers rôles, notamment la traduction de protocoles, la gestion de la sécurité, la gestion des adresses IP, la fourniture d'accès distant via des VPN, le routage des données entre réseaux, et plus encore, facilitant ainsi l'interconnexion, la sécurité et la communication efficace entre réseaux informatiques.

Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel, est un outil de sécurité et de confidentialité en ligne qui établit une connexion sécurisée entre votre appareil et un serveur distant, chiffrant ainsi toutes les données échangées. Cela permet de masquer votre adresse IP et de protéger vos informations contre l'interception par des tiers, garantissant une navigation internet plus confidentielle. Les VPN sont couramment utilisés pour accéder à Internet de manière anonyme, contourner les restrictions géographiques, sécuriser les connexions Wi-Fi publiques et permettre l'accès distant sécurisé aux réseaux d'entreprise.

Qu'est-ce qu'un DNS ?

Un DNS, ou Système de Noms de Domaine, est un service essentiel d'Internet qui traduit les noms de domaine, tels que www.google.com, en adresses IP compréhensibles par les ordinateurs. Il agit comme un annuaire de l'Internet, permettant aux utilisateurs d'accéder aux sites web en utilisant des noms conviviaux au lieu de devoir se souvenir des adresses IP numériques associées. Les serveurs DNS sont responsables de la résolution des noms de domaine en adresses IP, facilitant ainsi la navigation sur le Web et l'accès à divers services en ligne.