Runtrack Réseau

Job 1

Installation de cisco packet tracer.

Job 2

Qu'est-ce qu'un réseau ?

Un réseau informatique est un ensemble de dispositifs interconnectés qui permettent l'échange de données et de ressources entre eux. Ces dispositifs peuvent être des ordinateurs, des serveurs, des imprimantes, des routeurs, des commutateurs, des points d'accès. Un réseau est une infrastructure qui permet à des dispositifs électroniques de communiquer et de partager des informations entre eux. Il peut être filaire, où les dispositifs sont reliés physiquement par des câbles, ou sans fil, utilisant des ondes radio pour la transmission des données.

À quoi sert un réseau informatique ?

Un réseau informatique permet de réaliser diverses tâches, telles que :

-Partage de ressources : Il permet de partager des fichiers, des imprimantes, des connexions Internet.

-Communication : Il facilite la communication entre les utilisateurs via des services tels que la messagerie électronique, la visioconférence, les appels vocaux.

-Accès à des services distants : Il permet d'accéder à des serveurs et services situés à distance, comme les sites web, les bases de données.

-Sécurité et gestion des données : Il permet de mettre en place des stratégies de sécurité pour protéger les données et les ressources partagées.

Matériel nécessaire pour construire un réseau et leurs fonctions détaillées :

1. Ordinateurs et Dispositifs Clients :

Ce sont les utilisateurs finaux du réseau qui accèdent aux ressources partagées.

2. Serveurs :

Les serveurs fournissent des services ou des ressources aux clients. Par exemple, un serveur de fichiers stocke et partage des fichiers, un serveur de messagerie gère les e-mails, etc.

3. Routeur :

Il dirige le trafic entre différents réseaux. Il prend des décisions en fonction de l'adresse de destination des données.

4. Commutateur (Switch) :

Il relie les dispositifs au sein d'un même réseau local (LAN) et permet un transfert de données plus rapide et plus efficace que les concentrateurs (hubs).

5. Point d'Accès (Access Point) :

Il permet aux dispositifs sans fil de se connecter à un réseau câblé à travers une connexion sans fil.

6. Câbles et Connecteurs :

Ils assurent la connexion physique entre les dispositifs du réseau. Les câbles Ethernet (catégorie 5e, 6, etc.) sont couramment utilisés pour les réseaux filaires.

7. Cartes Réseau (NIC - Network Interface Card) :

Elles permettent aux ordinateurs et autres dispositifs de se connecter physiquement au réseau.

8. Modem :

Il permet de convertir les signaux numériques des ordinateurs en signaux analogiques pour les transmettre sur des lignes téléphoniques ou vice versa.

9. Pare-feu (Firewall) :

Il protège le réseau en filtrant le trafic entrant et sortant pour prévenir les accès non autorisés.

10. Equipements de Sécurité (Antivirus, IDS/IPS) :

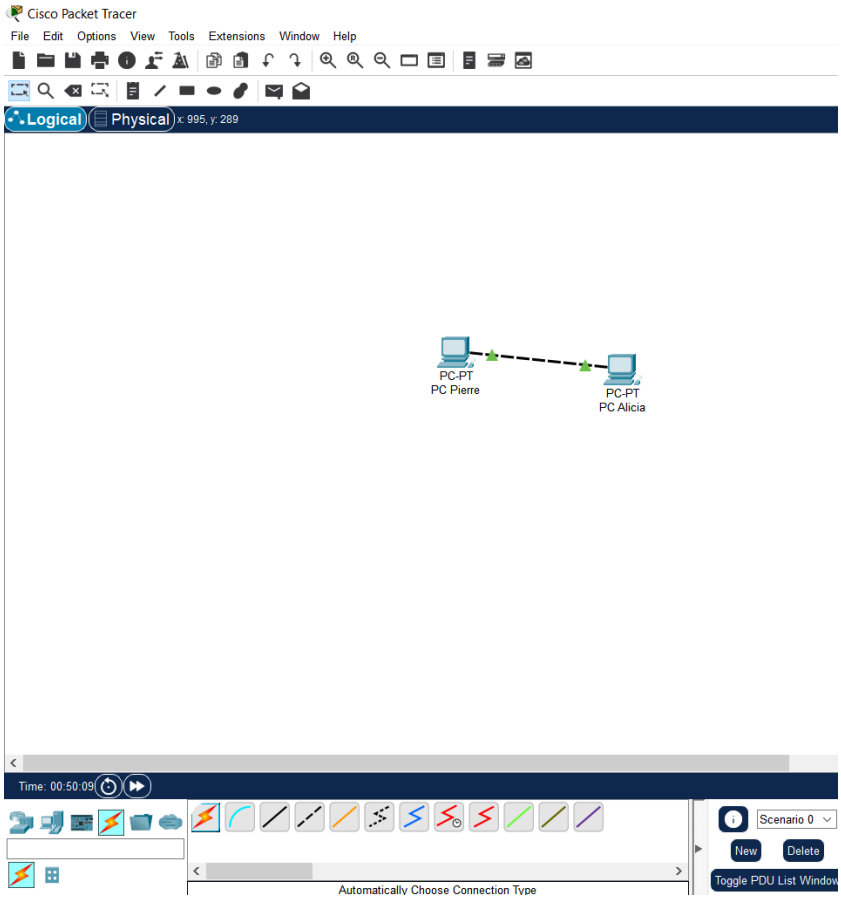
Ils protègent le réseau contre les menaces telles que les virus, les malwares et les intrusions.

11. Panneaux de Brassage et Prises Murales :

Ils organisent et distribuent les câbles réseau au sein d'un bâtiment ou d'un espace.

Chaque composant joue un rôle crucial dans la construction et le bon fonctionnement d'un réseau informatique.

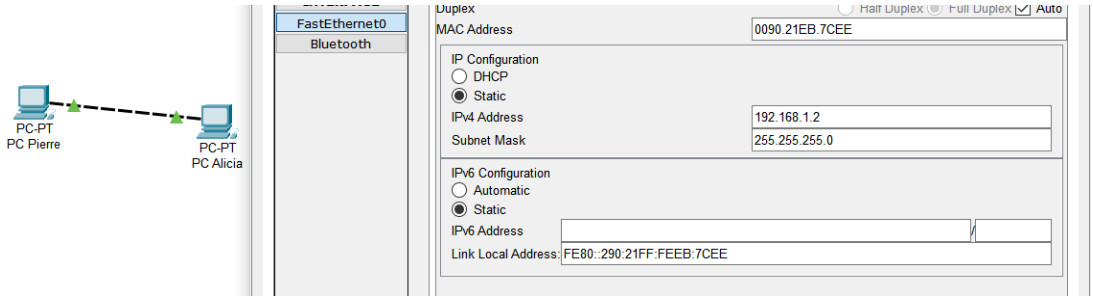
Job 3

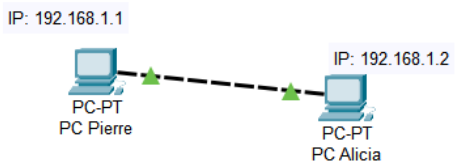


J’ai choisi un câble crossover(croisé) pour relier les deux ordinateurs.

Cela offre une connexion directe en plus d’éviter l’utilisation d’un commutateur. C’est un gain de temps et d’argent en plus d’être une solution simple pour établir une connexion point à point de manière directe.

Job 4





Qu’est-ce qu’une adresse IP ?

Une adresse IP (Internet Protocol) est une série de chiffres qui identifie de manière unique un périphérique sur un réseau IP. Il existe deux versions principales d'adresses IP : IPv4 (composée de quatre groupes de chiffres, par exemple 192.168.1.1) et IPv6 (qui utilise une notation alphanumérique plus complexe pour gérer la croissance exponentielle des dispositifs connectés à Internet).

À quoi sert un IP ?

Une adresse IP permet d'identifier et de localiser un périphérique sur un réseau, que ce soit sur Internet ou un réseau local. Cela permet aux appareils de communiquer entre eux en envoyant et recevant des paquets de données.

Qu’est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est une identifiant unique attribué à chaque carte réseau d'un périphérique. Contrairement à l'adresse IP, qui peut être changée, l'adresse MAC est assignée par le fabricant et est utilisée pour l'identification au niveau matériel.

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

Adresse IP Publique : Une adresse IP publique est accessible depuis Internet et permet de communiquer avec des périphériques sur le réseau mondial. Chaque appareil qui se connecte directement à Internet doit avoir une adresse IP publique unique.

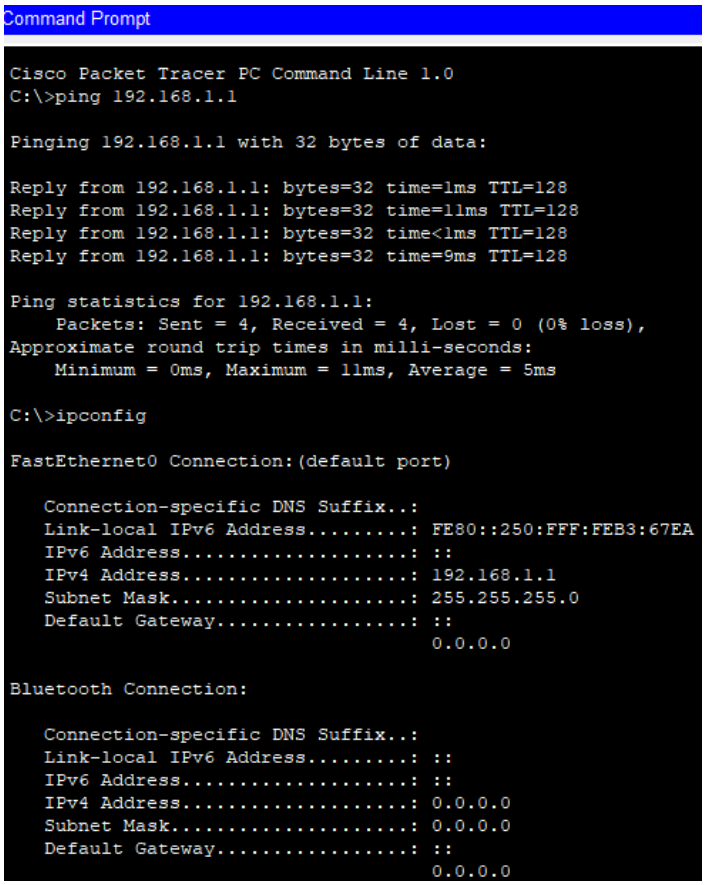
Adresse IP Privée : Une adresse IP privée est utilisée à l'intérieur d'un réseau local (LAN). Ces adresses ne sont pas routables via Internet et sont souvent utilisées pour connecter plusieurs appareils à un réseau domestique ou d'entreprise. Elles sont réservées et ne sont pas accessibles depuis l'extérieur du réseau local.

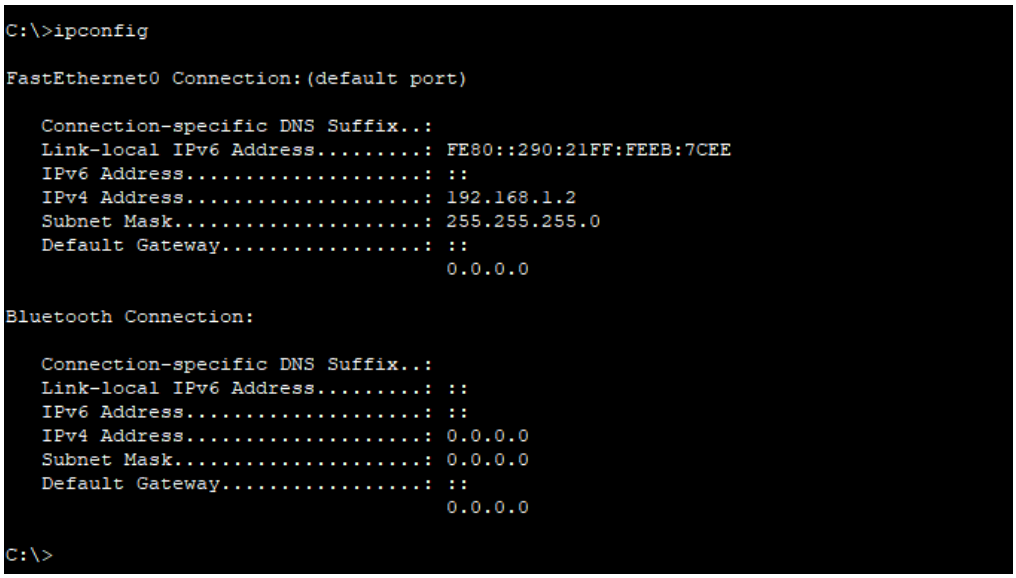
Quelle est l’adresse de ce réseau ?

Pour fournir une adresse de réseau précise, il faudrait des informations supplémentaires telles que la classe d'adresse IP (A, B, C), le masque de sous-réseau et éventuellement des informations de routage. Sans ces détails, il n'est pas possible de déterminer l'adresse d'un réseau spécifique. Si vous avez des informations supplémentaires, je pourrais vous aider à calculer l'adresse de réseau.

Job 5

Il faut d’abord se rendre dans command Prompt en cliquant sur le dekstop du PC.





J’ai utilisé ipconfig pour vérifier l’ip des deux PC.

Job 6

Sur le PC de 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=3ms 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 = 3ms, Average = 0ms

C:\>
```

Sur le PC de 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
Reply from 192.168.1.1: bytes=32 time=3ms 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 = 3ms, Average = 0ms

C:\>
```

La commande pour effectuer un ping entre des PC est ‘ping’ suivie de l’adresse IP de la destination.

Job 7

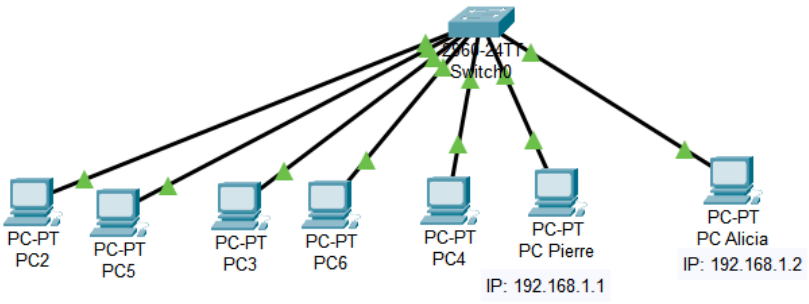
```
C:\>ping 192.168.1.1

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 ne recevra pas les paquets envoyés par Alicia. Cela est dû au fait que le PC de Pierre est éteint. Lorsqu'un appareil est éteint, il ne peut pas recevoir de données ou répondre à des requêtes.

Le ping est un outil qui envoie des paquets de données vers une adresse IP spécifiée et attend une réponse en retour. Si l'ordinateur cible est éteint, il ne peut pas répondre. Le ping n'indique pas seulement si l'adresse est correcte, mais aussi si la machine est active et capable de répondre.

Donc, dans ce cas, si le PC de Pierre est éteint, les pings d'Alicia n'obtiendront pas de réponse.

Job 8



Hub :

Un hub est un dispositif de couche 1 (physique) du modèle OSI. Il transmet les données à tous les ports sans distinction, ce qui signifie que tous les appareils connectés au hub reçoivent les données, même si elles ne leur sont pas destinées. Cela peut entraîner une congestion et une inefficacité du réseau.

Fonctionnement :

Un hub est un dispositif simple qui agit comme un amplificateur de signal. Il prend un signal et le renvoie à tous les ports.

Avantages :

-Facilité d'installation et d'utilisation.

-Moins cher que les switches.

-Peut être utile dans des réseaux très petits ou dans des cas spécifiques.

Inconvénients :

-N'offre pas de segmentation du réseau, ce qui signifie que tout le trafic est diffusé à tous les ports, augmentant ainsi la congestion.

-Les collisions de données peuvent se produire, surtout dans les réseaux plus grands.

Switch :

Un switch fonctionne à la couche 2 (liaison) du modèle OSI.

Il analyse l'adresse MAC (Media Access Control) des appareils connectés et transmet les données uniquement à l'appareil destinataire, évitant ainsi la congestion inutile du réseau.

Les switches sont plus intelligents et plus efficaces que les hubs.

Gestion du trafic réseau par un switch :

Un switch gère le trafic réseau en apprenant les adresses MAC des appareils connectés à ses ports. Il crée une table de correspondance entre les adresses MAC et les ports physiques. Lorsqu'il reçoit des données, il regarde dans cette table pour déterminer à quel port il doit transmettre les données. Cela permet d'envoyer les données uniquement à l'appareil destinataire, évitant ainsi la diffusion inutile à tous les ports comme c'est le cas avec un hub.

Avantages :

Filtre et envoie les données uniquement à l'appareil destinataire, ce qui réduit la congestion et améliore les performances du réseau.

Permet la création de domaines de diffusion (broadcast domains) distincts.

Idéal pour les réseaux de taille moyenne à grande.

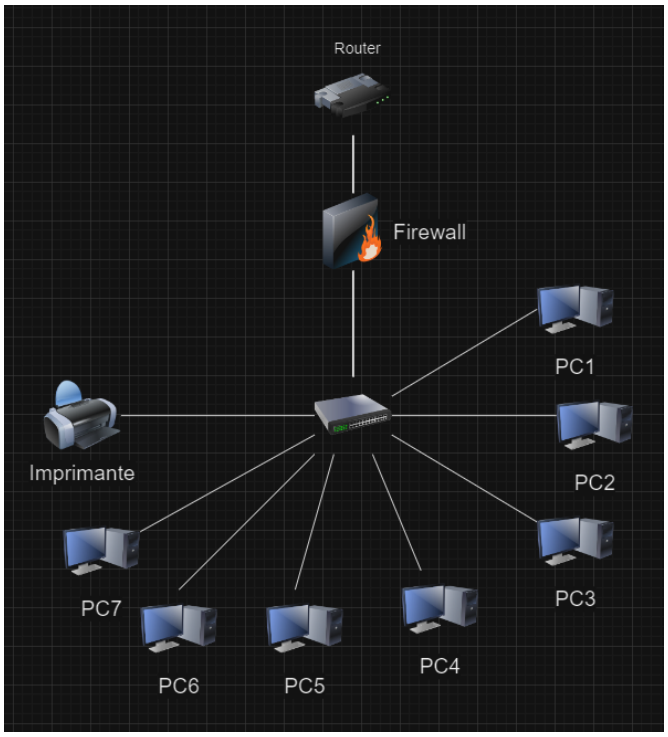
Inconvénients :

-Plus cher qu'un hub.

-Plus complexe à configurer.

Job 9

Schéma via draw.io :



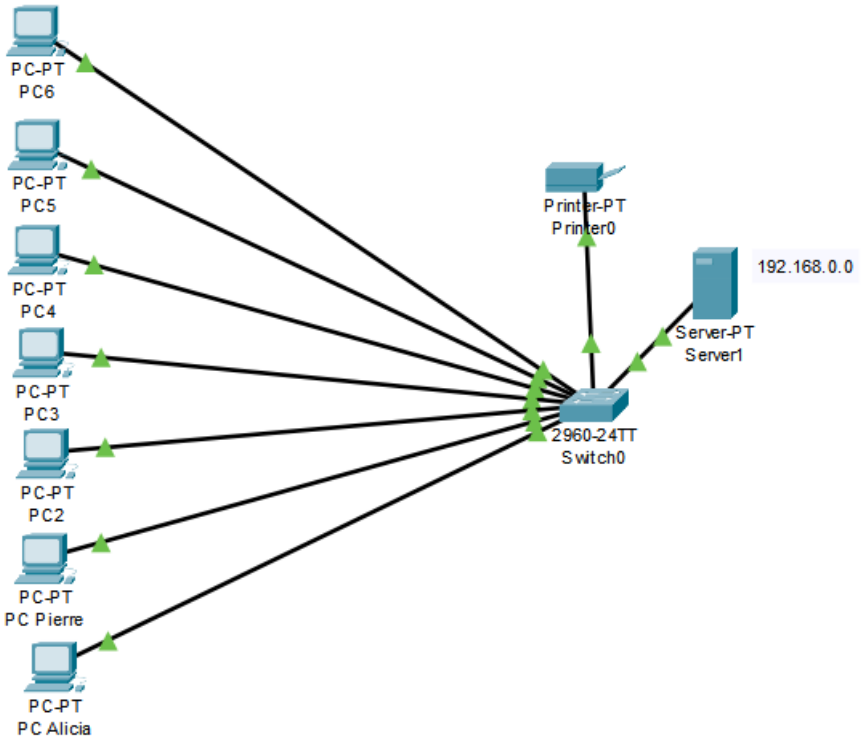
Avantages d'avoir un schéma de réseau

Clarté : Un schéma de réseau offre une vue visuelle de la configuration du réseau, ce qui facilite la compréhension de la topologie et des connexions.

Facilité : En cas de problème ou de panne, un schéma bien documenté permet de localiser rapidement les composants impliqués et d'identifier les points de défaillance potentiels.

Planification : Un schéma aide à planifier l'expansion du réseau en visualisant les composants actuels et en identifiant où de nouveaux appareils peuvent être ajoutés.

Job 10



Différences principales :

-Configuration :

Statique : L'adresse IP est configurée manuellement sur l'appareil.

DHCP : L'adresse IP est attribuée automatiquement par un serveur DHCP.

-Stabilité de l'Adresse IP :

Statique : L'adresse IP reste la même jusqu'à ce que l'administrateur la modifie.

DHCP : L'adresse IP peut changer à chaque connexion au réseau, en fonction des disponibilités du serveur DHCP.

-Gestion et Maintenance :

Statique : Chaque appareil doit être configuré individuellement, ce qui peut être fastidieux pour de grands réseaux.

DHCP : Le serveur DHCP gère automatiquement l'attribution des adresses IP, ce qui simplifie la gestion, surtout dans les grands réseaux.

-Flexibilité et Évolutivité :

Statique : Moins flexible, car chaque changement d'adresse nécessite une configuration manuelle.

DHCP : Plus flexible, car les adresses peuvent être gérées dynamiquement en fonction des besoins du réseau.

-Conflits d'Adresses IP :

Statique : Les conflits d'adresses IP peuvent se produire si deux appareils ont la même adresse.

DHCP : Le serveur DHCP gère l'attribution des adresses pour éviter les conflits.

En résumé, l'attribution d'adresses IP statiques est recommandée pour les périphériques qui doivent toujours avoir la même adresse IP (comme les serveurs), tandis que l'utilisation du DHCP est plus adaptée pour les appareils qui n'ont pas besoin d'une adresse IP fixe (comme les ordinateurs, les smartphone).

Job 11

Plan d'adressage :

Sous-réseau de 12 hôtes :

Nombre de sous-réseaux : 1

Nombre d'hôtes par sous-réseau : 12

Masque de sous-réseau : 255.255.255.240 (/28)

Plage d'adresses utilisable : de 10.0.0.1 à 10.0.0.14

Adresse de réseau : 10.0.0.0

Adresse de diffusion : 10.0.0.15

Sous-réseaux de 120 hôtes (5 sous-réseaux) :

Nombre de sous-réseaux : 5

Nombre d'hôtes par sous-réseau : 120

Masque de sous-réseau : 255.255.255.128 (/25)

Plage d'adresses utilisable par sous-réseau : de 10.0.0.129 à 10.0.0.254, de 10.0.1.1 à 10.0.1.126, ...

Adresse de réseau : varie pour chaque sous-réseau

Adresse de diffusion : varie pour chaque sous-réseau

Sous-réseaux de 160 hôtes (5 sous-réseaux) :

Nombre de sous-réseaux : 5

Nombre d'hôtes par sous-réseau : 160

Masque de sous-réseau : 255.255.255.224 (/27)

Plage d'adresses utilisable par sous-réseau : de 10.0.0.33 à 10.0.0.62, de 10.0.0.65 à 10.0.0.94, ...

Adresse de réseau : varie pour chaque sous-réseau

Adresse de diffusion : varie pour chaque sous-réseau

Pourquoi une adresse de classe A (10.0.0.0) ?

Une adresse de classe A offre un très grand nombre d'adresses (environ 16 millions) et est appropriée pour les grandes organisations ou les fournisseurs de services Internet. Dans ce cas, elle est utilisée car elle permet de créer une grande variété de sous-réseaux pour répondre aux besoins spécifiques.

Différences entre les types d'adresses :

Classe A : Le premier octet est utilisé pour le réseau, les trois autres pour les hôtes. Offre un très grand nombre d'adresses réseau, mais chaque réseau peut contenir un grand nombre d'hôtes.

Classe B : Les deux premiers octets sont utilisés pour le réseau, les deux autres pour les hôtes. Adaptée aux organisations moyennes.

Classe C : Les trois premiers octets sont utilisés pour le réseau, le dernier pour les hôtes. Convient aux petites organisations.

Classe D : Réservée à un usage multicast.

Classe E : Réservée à des fins expérimentales ou de recherche.

Une adresse de classe A a été choisie car elle offre la flexibilité nécessaire pour créer des sous-réseaux de différentes tailles et répondre aux besoins spécifiques de l'organisation.

Job 12

Couche OSI	Elément/Protocole	Description
Application	HTTP	Protocole de transfert de données pour le web.
Présentation	SSL/TLS	Protocole de sécurisation des communications.
Session	PPTP	Protocole pour la mis en place de connexions VPN.
Transport	TCP UDP	Assure la fiabilité de la communication.
Réseau	IPv4 IPv6	Adresse IP version 4. Adresse IP version 6.
Liaison	Ethernet, Wifi, MAC, Fibre optique, câble RJ45	Contrôle d'accès au médium (support physique par lequel les données sont transmises sur le réseau). Contrôle de la liaison physique.
Physique	Routeur Cable	Transmission des bits sur le support physique. Support de transmission (RJ45).

Job 13

Architecture du Réseau :

Tous les appareils (PCs et serveurs) sont connectés au même réseau local (LAN) et utilisent le même sous-réseau défini par le masque de sous-réseau 255.255.255.0. Cela signifie qu'ils sont tous dans la même plage d'adresses IP (192.168.10.x).

Adresse IP du Réseau :

L'adresse IP du réseau est déterminée en utilisant le "ET logique" entre l'adresse IP d'un appareil et le masque de sous-réseau. Cela garantit que seuls les bits du réseau sont conservés.

Par exemple, pour PC0 : 192.168.10.6 ET 255.255.255.0 donne 192.168.10.0, qui est l'adresse réseau.

Nombre de Machines :

Avec un masque de sous-réseau de 255.255.255.0, cela signifie qu'il y a 2^8 - 2 = 254 adresses IP utilisables. La soustraction de 2 (le réseau et la diffusion) est due au fait que ces adresses ne sont pas utilisables par les appareils.

Adresse de Diffusion :

L'adresse de diffusion est la dernière adresse dans la plage d'adresses IP du réseau. Avec un masque de sous-réseau de 255.255.255.0, cela signifie que l'adresse de diffusion est 192.168.10.255.

Job 14

Pour convertir une adresse IP en binaire, chaque octet (groupe de 8 bits) doit être converti individuellement.

145.32.59.24

145 => 10010001

32 => 00100000

59 => 00111011

24 => 00011000

Adresse IP en binaire : 10010001.00100000.00111011.00011000

200.42.129.16

200 => 11001000

42 => 00101010

129 => 10000001

16 => 00010000

Adresse IP en binaire : 11001000.00101010.10000001.00010000

14.82.19.54

14 => 00001110

82 => 01010010

19 => 00010011

54 => 00110110

Adresse IP en binaire : 00001110.01010010.00010011.00110110

Job 15

Qu’est-ce que le routage ?

Le routage est le processus par lequel des données sont acheminées entre différents réseaux informatiques pour atteindre leur destination. Cela implique la sélection du meilleur chemin à emprunter à travers un réseau complexe de dispositifs (comme des routeurs) afin d'acheminer efficacement les paquets de données d'un point à un autre. Le routage repose sur des tables de routage, qui contiennent des informations sur les réseaux et les chemins disponibles.

Qu’est-ce qu’un gateway ?

Un gateway (ou passerelle en français) est un dispositif matériel ou logiciel qui relie deux réseaux différents et permet la communication entre eux. Il agit comme une sorte de point d'entrée ou de sortie pour les données entre ces réseaux. Par exemple, un routeur peut faire office de gateway entre un réseau local (LAN) et Internet.

Qu’est-ce qu’un VPN ?

Un VPN (Virtual Private Network ou réseau privé virtuel) est une technologie qui crée un tunnel sécurisé sur un réseau public, comme Internet, permettant ainsi à des utilisateurs ou des systèmes distants de se connecter à un réseau privé de manière sécurisée. Il est largement utilisé pour protéger la confidentialité des données, contourner la censure en ligne, ou permettre l'accès à des ressources réseau d'une organisation depuis l'extérieur.

Qu’est-ce qu’un DNS ?

Le DNS (Domain Name System ou système de noms de domaine) est un système qui traduit les noms de domaine (comme www.exemple.com) en adresses IP numériques que les ordinateurs peuvent comprendre. Il s'agit essentiellement d'un annuaire qui permet aux utilisateurs d'accéder à des sites web et à d'autres ressources en utilisant des noms conviviaux plutôt que de devoir se rappeler des adresses IP numériques complexes.