

Job2

-Qu'est-ce qu'un réseau ?

Un réseau est un ensemble des systèmes connectés les uns aux autres permettant l'échange de données et le partage de ressources communes.

- À quoi sert un réseau informatique ?

Un réseau informatique sert à connecter différents dispositifs informatiques (ordinateurs, serveurs, imprimantes, routeurs, etc.) afin de leur permettre de communiquer et de partager des ressources et des informations.

- Quel matériel avons-nous besoin pour construire un réseau ?

Pour construire un réseau informatique, il est essentiel de comprendre le rôle de chaque composant matériel. Voici une liste détaillée de des composants matériels nécessaires pour construire un réseau, ainsi que leurs fonctionnements respectifs :

- **Ordinateurs et périphériques réseau :**

Fonction : Les ordinateurs et les périphériques sont les dispositifs finaux du réseau, tels que les postes de travail, les ordinateurs portables, les imprimantes, les scanners, les caméras IP, etc. Ils utilisent le réseau pour partager des données, des ressources et accéder à des services.

- **Switches :**

Fonction : Les commutateurs réseau sont des dispositifs qui relient de manière intelligente les périphériques du réseau local (LAN). Ils fonctionnent au niveau de la couche 2 du modèle OSI et acheminent le trafic en utilisant les adresses MAC.

- **Routeurs :**

Fonction : Les routeurs connectent différents réseaux, y compris l'accès à Internet. Ils acheminent le trafic entre les sous-réseaux en utilisant des adresses IP. Ils agissent comme des passerelles entre les réseaux.

- **Câbles réseau :**

Fonction : Les câbles Ethernet, tels que Cat 5e, Cat 6 ou Cat 7, servent à établir des connexions filaires entre les périphériques réseau. Les câbles de fibre optique sont utilisés pour des connexions haut débit sur de plus longues distances.

- **Points d'accès sans fil (WAP) :**

Fonction : Les WAP permettent aux périphériques de se connecter au réseau sans fil (Wi-Fi). Ils diffusent un signal Wi-Fi pour que les appareils sans fil puissent se connecter au réseau.

- **Serveurs :**

Fonction : Les serveurs sont des ordinateurs puissants qui fournissent des services et des ressources aux utilisateurs et aux dispositifs du réseau. Ils peuvent héberger des services tels que les sites web, les bases de données, le stockage de fichiers, la messagerie, etc.

- **Firewalls :**

Fonction : Les pare-feu sont des dispositifs ou des logiciels de sécurité qui contrôlent le trafic réseau entrant et sortant pour protéger le réseau contre les menaces, les attaques et les intrusions.

- **Modems :**

Fonction : Les modems permettent de se connecter à Internet via une ligne terrestre, DSL, câble, fibre optique, etc. Ils convertissent les signaux numériques de votre réseau en signaux analogiques pour la communication avec votre fournisseur d'accès Internet.

- **Équipement de sauvegarde :**

Fonction : Les équipements de sauvegarde, tels que les disques durs externes, les serveurs de sauvegarde, etc., permettent de sauvegarder et de protéger les données critiques du réseau.

- **Baies de brassage (rack) :**

Fonction : Les baies de brassage sont des armoires ou des racks utilisés pour monter et organiser les équipements réseau, tels que les commutateurs, les routeurs, les serveurs, les patch panels, etc.

- **Matériel de sécurité physique :**

Fonction : Les dispositifs de sécurité physique, tels que les serrures, les caméras de sécurité et les systèmes d'alarme, protègent l'accès physique aux équipements réseau.

- **Onduleurs (UPS) :**

Fonction : Les onduleurs fournissent une alimentation de secours pour garantir que le réseau continue de fonctionner en cas de panne de courant, en évitant les perturbations.

- **Câblage structuré :**

Fonction : Le câblage structuré organise et gère les câbles pour une installation propre et organisée. Il simplifie également la maintenance et les modifications ultérieures.

- **Outils réseau :**

Fonction : Les outils réseau, tels que les testeurs de câble, les pinces à sertir, les tournevis, etc., sont utilisés pour installer et entretenir le réseau.

- **Logiciels de gestion réseau :**

Fonction : Les logiciels de gestion réseau sont utilisés pour surveiller, gérer, configurer et diagnostiquer l'infrastructure réseau.

Job3

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

★ Automatically choose connection type (choix automatique du type de connexion) :

Les câbles de connexion automatiques, également connus sous le nom de câbles MDIX (Medium Dependent Interface Crossover), sont conçus pour simplifier la connectivité réseau en adaptant automatiquement la configuration du câblage en fonction des périphériques connectés. Ils jouent un rôle essentiel dans l'élimination de la nécessité de choisir entre des câbles droits et croisés, simplifiant ainsi la configuration des réseaux.

Job4

- Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est une adresse numérique unique attribuée à chaque périphérique connecté à un réseau informatique qui utilise le protocole IP pour communiquer. Les adresses IP sont utilisées pour identifier et localiser les périphériques sur un réseau, que ce soit sur Internet ou sur un réseau local (LAN).

- À quoi sert un IP ?

Une adresse IP sert à identifier de manière unique un périphérique sur un réseau, qu'il s'agisse d'un ordinateur, d'un smartphone, d'un serveur, d'une imprimante, ou tout autre appareil réseau. Les adresses IP permettent le routage des données sur le réseau, en spécifiant l'expéditeur et le destinataire de chaque paquet de données.

- Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est une adresse matérielle unique attribuée à chaque carte réseau ou interface réseau d'un périphérique. Contrairement aux adresses IP, les adresses MAC sont liées au matériel et ne changent généralement pas. Elles sont utilisées au niveau de la couche liaison de données pour l'acheminement des données à travers un réseau local.

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

Une adresse IP publique est une adresse attribuée à un périphérique qui est directement accessible depuis Internet. Les serveurs web, les routeurs, et d'autres dispositifs accessibles publiquement ont généralement des adresses IP publiques.

Une adresse IP privée est utilisée à l'intérieur d'un réseau local, comme un réseau domestique ou d'entreprise, et n'est pas directement accessible depuis Internet. Les adresses IP privées sont utilisées pour permettre aux périphériques du réseau local de communiquer entre eux et d'accéder à Internet via une adresse IP publique attribuée au routeur ou au pare-feu du réseau. Les adresses IP privées sont généralement attribuées selon des plages définies, telles que 192.168.0.0 à 192.168.255.255 (IPv4).

- Quelle est l'adresse de ce réseau ?

Pour déterminer l'adresse d'un réseau, il est important de connaître le préfixe de sous-réseau (ou masque de sous-réseau) et l'adresse IP de l'un des périphériques du réseau.

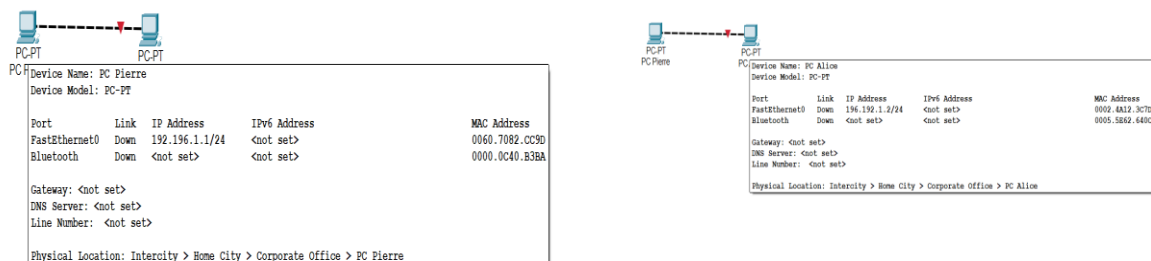
PC Pierre : 192.168.1.1

PC Alicia : 192.168.1.2

Les adresses IP qu'on a utilisées sont dans la plage 192.168.1.0/24, où "24" est la notation du masque de sous-réseau. Un masque de sous-réseau de 24 bits signifie que les 24 premiers bits de l'adresse IP sont réservés pour le réseau, et les 8 bits restants (32 bits au total pour une adresse IPv4) sont disponibles pour les hôtes.

Pour identifier l'adresse du réseau, on doit considérer les bits réservés pour le réseau. Dans ce cas, les 24 premiers bits, soit 192.168.1.0, forment l'adresse du réseau.

Donc, l'adresse du réseau est 192.168.1.0.



Job5

- Quelle ligne de commande avez-vous utilisée pour vérifier l’ID des machines ?

On a utilisé la commande ‘**ipconfig**’ qui affiche les informations de configuration réseau du PC, y compris l’adresse IP, le masque de sous-réseau, la passerelle par défaut, etc.

```
Command Prompt

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

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:70FF:FE82:CC9D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.196.1.1
    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 PC Pierre

```
Command Prompt

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

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:4AFF:FE12:3C7D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 196.192.1.2
    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:\>
```

ipconfig PC Alice

Job6

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

La commande ping est utilisée pour tester la connectivité entre des ordinateurs en envoyant des paquets de données ICMP (Internet Control Message Protocol) à l’adresse IP de la machine de destination. Elle est couramment utilisée pour vérifier si un ordinateur peut communiquer avec un autre sur un réseau.

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

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

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

Job7

```
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),
```

Lorsqu'un PC est éteint, il ne peut pas répondre aux requêtes ICMP (Internet Control Message Protocol) telles que le ping. Par conséquent, si on éteint le PC de Pierre et qu'on utilise le terminal du PC d'Alicia pour envoyer un ping à l'adresse IP du PC de Pierre, les paquets envoyés par Alicia ne seront pas reçus par le PC de Pierre. Le ping échouera car le PC de Pierre est hors ligne.

Le PC de Pierre n'a pas la possibilité de répondre aux requêtes ICMP lorsque son alimentation est coupée, ce qui est la raison pour laquelle le ping d'Alicia ne réussira pas.

Lorsque l'on effectue un ping vers un ordinateur qui est éteint ou déconnecté du réseau, nous obtiendrions des réponses du type "Destination Host Unreachable" ou "Request Timed Out" pour indiquer que l'hôte cible n'a pas pu être atteint. Cela est dû au fait que le PC de Pierre n'a pas répondu aux requêtes ICMP en raison de son état hors ligne.

Sur Cisco Packet Tracer, il n'est pas possible d'éteindre directement un périphérique comme on le ferait avec un ordinateur réel. Cisco Packet Tracer est principalement un simulateur pour la conception et la configuration de réseaux, et il ne simule pas l'alimentation des ordinateurs ou leur état de marche.

Job8

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

Un hub est un dispositif de la couche physique du modèle OSI qui propage les données à tous les ports sans se soucier de l'adresse MAC de destination. Tous les périphériques connectés à un hub voient le trafic de tous les autres périphériques, tandis qu'un switch (un dispositif de la couche liaison de données du modèle OSI) apprend les adresses MAC des périphériques connectés à ses ports et transmet le trafic uniquement vers le port où se trouve la destination. Il isole le trafic entre les périphériques connectés, améliorant ainsi l'efficacité et la sécurité du réseau.

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

Un hub propage simplement les trames (paquets de données) à tous les ports.

L'avantage d'un hub c'est qu'il est facile à installer et moins coûteux que les switches.

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

Un switch transmet le trafic uniquement aux ports où il est nécessaire en fonction des adresses MAC.

- On trouve des avantages telles que l'haute performance, meilleure sécurité, gestion du trafic et absence de collisions.
- En comparaison avec les hubs, le switch a un coût plus élevé et, la configuration d'un switch est plus complexe.

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

Un switch apprend les adresses MAC des périphériques connectés en écoutant le trafic du réseau.

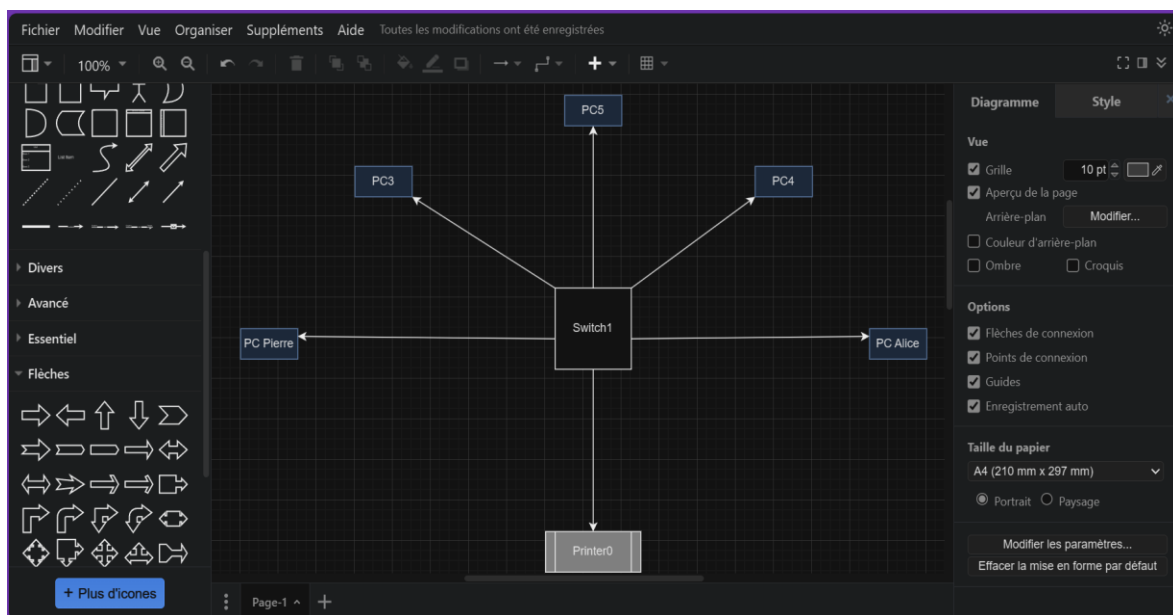
Il utilise une table de commutation (table MAC) pour mémoriser les ports associés à chaque adresse MAC ; lorsqu'il reçoit des trames, il les transmet uniquement vers les ports où se trouve la destination, en utilisant la table MAC pour prendre la décision de transfert.

Job9

- identifiez au moins trois avantages importants d'avoir un schéma.

Dans ce point, on parlera de trois aspects :

- **Clarté et Compréhension** : Un schéma de réseau permet de visualiser la topologie du réseau, ce qui facilite la compréhension de la manière dont les composants sont connectés.
- **Dépannage** : En cas de problème réseau, un schéma permet de repérer plus rapidement les éventuelles défaillances, de suivre le cheminement du trafic et d'identifier les composants impliqués.
- **Documentation** : Un schéma de réseau sert de documentation précieuse pour les administrateurs et les techniciens réseau. Il facilite la gestion et la maintenance du réseau, y compris l'ajout de nouveaux composants comme l'imprimante.



Job10

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

La principale différence réside dans la manière dont les adresses IP sont obtenues et gérées. Les adresses IP statiques sont configurées manuellement et restent constantes, tandis que les adresses IP

attribuées par DHCP sont obtenues automatiquement et peuvent changer au fil du temps. Le choix entre les deux dépend des besoins spécifiques de l'appareil et du réseau.

Job12

Couche OSI	Description	Matériels/protocoles associés
Couche 7-Application	Fournit des services d'application aux utilisateurs. C'est la couche la plus proche de l'utilisateur final	<i>HTML, FTP, SSL/TLS</i>
Couche 6-Présentation	Fournit des services d'application aux utilisateurs. C'est la couche la plus proche de l'utilisateur final	<i>SSL/TLS, HTML</i>
Couche 5-Session	Établit, gère et termine les sessions de communication entre les applications.	<i>PPTP</i>
Couche 4-Transport	Gère le contrôle de bout en bout de la communication, garantissant la fiabilité et le contrôle de flux.	<i>TCP, UDP, TCP</i>
Couche 3-Réseau	Gère la transmission de données à travers le réseau, le routage et la commutation.	<i>IPv4, IPv6, routeur</i>
Couche 2-Liaison de données	Gère la communication entre les périphériques du même réseau, gère l'accès au support de transmission	<i>Ethernet, MAC, Wi-Fi, câble RJ45</i>
Couche 1-Physique	Gère les caractéristiques physiques du support de transmission.	<i>Fibre optique, câble RJ45</i>

Job13

- Quelle est l'architecture de ce réseau ?

- Adresse IP du réseau : 192.168.10.0
- Masque de sous-réseau : 255.255.255.0
- Il s'agit d'un réseau de classe C.

- Indiquer quelle est l'adresse IP du réseau ?

- L'adresse IP du réseau est 192.168.10.0. C'est l'adresse utilisée pour identifier le réseau lui-même.

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

Avec un masque de sous-réseau de 255.255.255.0 (ou /24 en notation CIDR), il y a 256 adresses IP possibles dans le réseau.

Cependant, certaines adresses sont réservées. L'adresse réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255) ne peuvent pas être utilisées par les machines.

Donc, le nombre de machines qui peuvent être branchées sur ce réseau est de $256 - 2 = 254$.

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

L'adresse de diffusion pour ce réseau est 192.168.10.255. C'est l'adresse utilisée pour envoyer des données à toutes les machines du réseau en même temps.

Ainsi, l'architecture de ce réseau est de classe C avec l'adresse IP du réseau 192.168.10.0, un masque de sous-réseau de 255.255.255.0, permettant jusqu'à 254 machines, et une adresse de diffusion de 192.168.10.255.

Job14

-Convertissez les adresses IP suivantes en binaires :

➤ **145.32.59.24** = 10010001.00100000.00111011.00011000

→ **145 en binaire** : 10010001.

→ **32 en binaire** : 00100000.

→ **59 en binaire** : 00111011.

→ **24 en binaire** : 00011000.

➤ **200.42.129.16** = 11001000.00101010.10000001.00010000

→ **200 en binaire** : 11001000.

→ **42 en binaire** : 00101010.

→ **129 en binaire** : 10000001.

→ **16 en binaire** : 00010000.

➤ **14.82.19.54** = 00001110.01010010.00010011.00110110

→ **14 en binaire** : 00001110.

→ **82 en binaire** : 01010010.

→ **19 en binaire** : 00010011.

→ **54 en binaire** : 00110110.

Job15

- Qu'est-ce que le routage ?

Le routage est le processus de transmission des données d'un réseau à un autre à travers un ensemble de dispositifs appelés routeurs. Ils déterminent le chemin optimal pour les données afin qu'elles atteignent leur destination. Le routage est essentiel pour permettre aux données de circuler efficacement sur Internet et à travers des réseaux interconnectés.

- Qu'est-ce qu'un Gateway ?

Une passerelle, ou Gateway en anglais, est un dispositif ou un logiciel qui relie deux réseaux différents et leur permet de communiquer entre eux. Les passerelles sont souvent utilisées pour connecter un réseau local (LAN) à un réseau plus vaste, comme Internet. Elles traduisent les protocoles et les adresses entre les deux réseaux pour assurer la compatibilité. Par exemple, un routeur peut servir de passerelle entre un réseau local et Internet.

- Qu'est-ce qu'un VPN ?

Un VPN est un réseau privé virtuel qui permet de créer un tunnel sécurisé sur un réseau public (comme Internet) pour transmettre des données de manière sécurisée. Les VPN sont largement utilisés pour protéger la confidentialité des données et la sécurité de la communication, en cryptant le trafic entre les points d'extrémité du réseau. Les VPN sont couramment utilisés pour accéder à distance à des réseaux d'entreprise, contourner la censure sur Internet et assurer la confidentialité en ligne.

- Qu'est-ce qu'un DNS ?

Le DNS est un système qui associe les noms de domaine (par exemple, www.exemple.com) aux adresses IP des serveurs sur Internet. Plutôt que de se souvenir des adresses IP numériques, les utilisateurs peuvent utiliser des noms de domaine plus conviviaux. Le DNS effectue la résolution des noms en traduisant ces noms de domaine en adresses IP correspondantes. Il est essentiel pour la navigation web, la messagerie électronique et d'autres activités en ligne.