

RunTrack Réseau

Job 2 :

Q.1 Qu'est ce qu'un réseau ?

Un réseau, dans le contexte de la technologie de l'information et de la communication, désigne généralement un ensemble d'appareils, d'ordinateurs, de périphériques ou de systèmes interconnectés qui communiquent entre eux pour partager des informations, des ressources ou des services. Les réseaux sont essentiels à la communication et à l'échange de données, que ce soit localement (dans une même pièce ou un même bâtiment) ou à l'échelle mondiale via Internet.

Il existe différents types de réseaux, notamment :

- **Les réseaux locaux (LAN, Local Area Network) :** Ils couvrent une petite zone géographique, comme un bureau, une maison ou un campus universitaire, et permettent la connexion d'ordinateurs et de périphériques pour le partage de fichiers, d'imprimantes et d'autres ressources.
- **Les réseaux étendus (WAN, Wide Area Network) :** Ils s'étendent sur de plus grandes distances, souvent à l'échelle d'une ville, d'un pays ou même du monde entier. Internet est un exemple de WAN.
- **Les réseaux sans fil (Wi-Fi) :** Ils permettent la connexion d'appareils sans l'utilisation de câbles physiques, facilitant la mobilité et l'accès à Internet via des points d'accès sans fil.
- **Les réseaux sociaux :** Ce sont des plateformes en ligne qui relient des individus ou des groupes à des fins de communication, de partage d'informations et d'interaction sociale.
- **Les réseaux informatiques d'entreprise :** Ils sont utilisés par les organisations pour connecter leurs systèmes informatiques, leurs serveurs, leurs bases de données et leurs postes de travail afin de faciliter la gestion des données et des processus internes.
- **Les réseaux peer-to-peer (P2P) :** Ils permettent à des pairs (utilisateurs individuels) de se connecter directement les uns aux autres pour partager des fichiers ou des ressources sans passer par un serveur central.

- **Les réseaux de télécommunications** : Ils englobent les infrastructures de télécommunication, y compris les réseaux de téléphonie fixe, mobile et les réseaux de communication par satellite.

Les réseaux sont fondamentaux dans notre société moderne et jouent un rôle central dans la connectivité, la collaboration, le partage d'informations et le fonctionnement des systèmes informatiques et de communication à l'échelle mondiale. Ils peuvent prendre de nombreuses formes, en fonction des besoins et des objectifs de communication de chaque entité ou individu.

Q.2 Qu'est ce qu'un réseau informatique?

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil.

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

Pour construire un réseau, j'aurais besoin de plusieurs composants matériels essentiels. Voici une liste des éléments principaux avec une brève explication de leurs fonctions :

Ordinateurs ou Dispositifs Clients : Ce sont les appareils qui se connectent au réseau pour accéder aux ressources partagées (comme des fichiers, des imprimantes, des serveurs, etc.) ou pour accéder à Internet.

Serveurs : Les serveurs sont des ordinateurs spécialisés qui fournissent des services aux autres dispositifs du réseau. Ils peuvent héberger des sites web, des bases de données, des fichiers, etc.

Routeurs : Les routeurs dirigent le trafic entre différentes parties d'un réseau, notamment entre le réseau local (LAN) et Internet. Ils utilisent des tables de routage pour prendre des décisions sur la meilleure façon d'envoyer les données.

Commutateurs (Switches) : Les commutateurs connectent différents dispositifs au sein d'un réseau local (LAN) et permettent la communication directe entre eux. Ils apprennent et stockent les adresses MAC pour optimiser la transmission des données.

Points d'Accès sans Fil (Access Points) : Les points d'accès permettent aux dispositifs sans fil de se connecter à un réseau câblé. Ils étendent la portée du réseau en fournissant une connexion Wi-Fi.

Modems : Les modems convertissent les signaux numériques de votre réseau en signaux analogiques compréhensibles par votre fournisseur de services Internet (FSI) et vice versa. Ils sont utilisés pour établir une connexion Internet.

Câbles et Connecteurs : Les câbles (comme les câbles Ethernet) sont utilisés pour connecter physiquement les dispositifs du réseau. Les connecteurs (comme les prises RJ45) sont utilisés pour brancher les câbles.

Cartes Réseau (NIC - Network Interface Cards) : Ces cartes sont installées dans les ordinateurs et leur permettent de se connecter au réseau, que ce soit via un câble Ethernet ou sans fil.

Firewalls : Les pare-feux sont des dispositifs de sécurité qui filtrent et surveillent le trafic réseau pour protéger le réseau contre les menaces externes et internes.

Équipement de Sécurité : Cela peut inclure des dispositifs tels que des systèmes de détection d'intrusion (IDS), des systèmes de prévention d'intrusion (IPS), des antivirus, etc., qui contribuent à protéger le réseau contre les menaces.

Onduleurs (UPS - Uninterruptible Power Supplies) : Les onduleurs fournissent une alimentation électrique de secours en cas de coupure de courant, assurant ainsi une disponibilité continue des services réseau.

Équipement de Sauvegarde : Cela peut inclure des dispositifs de stockage (comme des serveurs NAS) et des logiciels de sauvegarde pour garantir que les données du réseau sont régulièrement sauvegardées et récupérables en cas de besoin.

En fonction de la taille et de la complexité du réseau, d'autres composants spécifiques peuvent être nécessaires, tels que des commutateurs de niveau 3, des routeurs haute performance, des systèmes de stockage en réseau (SAN), etc. Il est important de concevoir le réseau en fonction des besoins spécifiques de l'organisation.

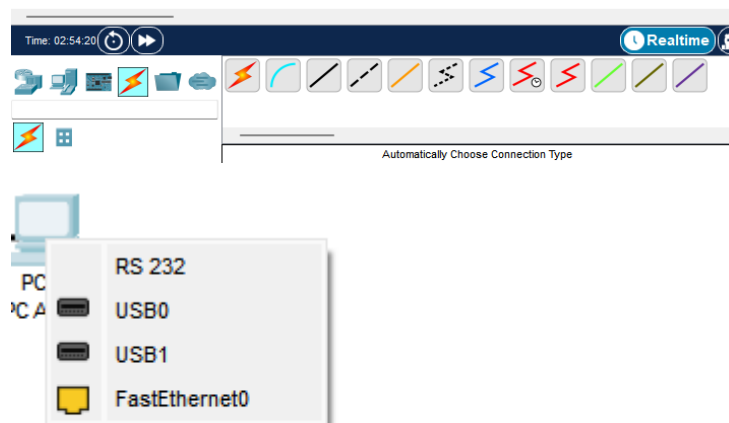
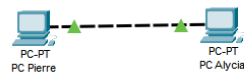
Job 3 :

Une fois la procédure d'instruction suivie, nous avons dû cliquer sur l'icône **End Devices** comme l'indique la consigne puis modifier les **PCs en Pierre et Alycia** et pour finir nous les avons reliés par un câble d'un certain modèle.

J'ai indiqué que le type de connexion est par "**Fast Ethernet**".

Q.4 Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

J'ai choisi le câble Ethernet Ethernet car je trouve que c'est plus simple de relier deux ordinateurs de bureau.



Job 4 :

J'ai configuré avec les indications données les adresses IP correspondant à la consigne ainsi que les masques sous-réseaux.

Pour Alycia :

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

Pour Pierre :

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

Q.1 Qu'est ce qu'une adresse IP ?

Une adresse IP est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet Protocol. L'adresse IP est à l'origine du système d'acheminement des paquets de données sur Internet.

Q.2 À quoi sert un IP ?

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

Q.3 Qu'est-ce qu'une adresse MAC ?

Une adresse MAC est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. Elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés.

Q.4 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.

Q.5 Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau comme l'indiquent les informations suivantes ci-dessous est la suivante : 10.10.2.21.

```
C:\ Invite de commandes
Carte réseau sans fil Connexion au réseau local* 2 :

Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . :

Carte Ethernet VMware Network Adapter VMnet1 :

Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . : fe80::1413:3e60:38df:76a9%12
Adresse IPv4. . . . . : 192.168.234.1
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :

Carte Ethernet VMware Network Adapter VMnet8 :

Suffixe DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . . : fe80::3310:26aa:83a8:d890%14
Adresse IPv4. . . . . : 192.168.30.1
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :

Carte réseau sans fil Wi-Fi :

Suffixe DNS propre à la connexion. . . : laplateforme.io
Adresse IPv6 de liaison locale. . . . : fe80::d80:d21b:c4fb:1156%21
Adresse IPv4. . . . . : 10.10.2.21
Masque de sous-réseau. . . . . : 255.255.0.0
Passerelle par défaut. . . . . : 10.10.0.1

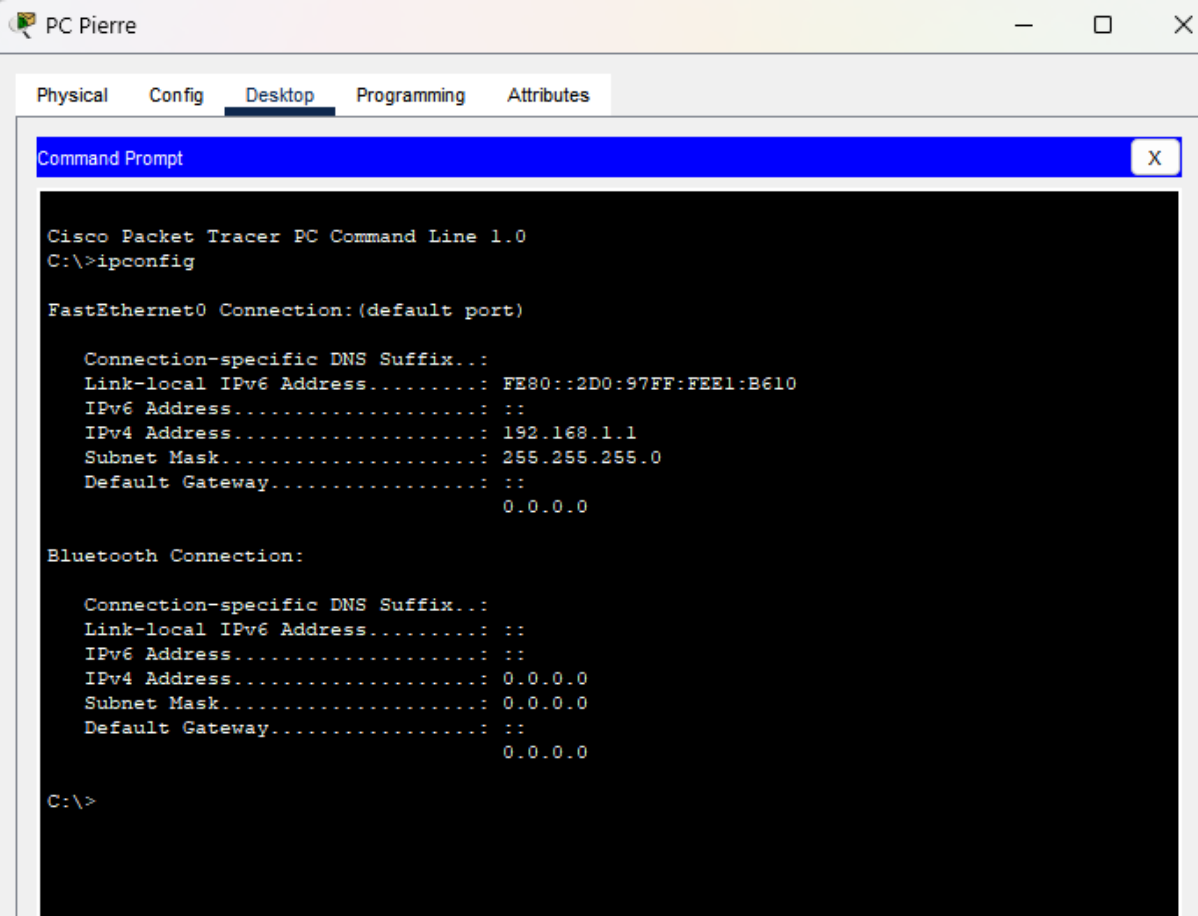
C:\Users\Utilisateur>
```

Job 5 :

Q.1 Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?

Pour vérifier l'adresse IP, il a fallu exécuter la commande **ipconfig**.

Voici l'adresse IP du PC de Pierre : **192.168.1.1**



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

FastEthernet0 Connection:(default port)

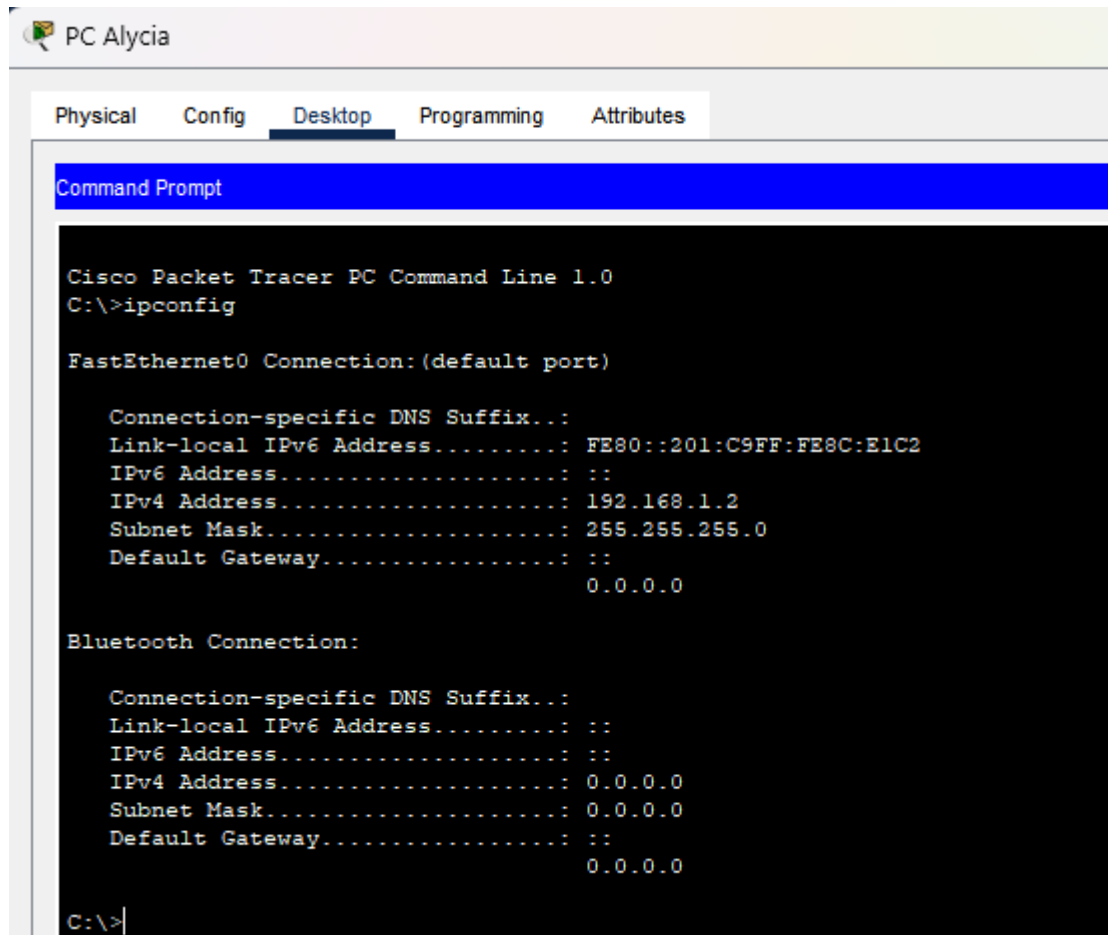
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address.....: FE80::2D0:97FF:FEE1:B610
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
                           0.0.0.0

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:\>
```

Et celui d'Alycia : **192.168.1.2**



Job 6 :

Q.1 Quelle est la commande permettant de Ping entre des PC ?

La commande permettant de pinguer entre les PC est la commande **ping** suivi de l'adresse IP d'un autre PC sur lequel nous souhaitons effectuer un ping.

```
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:\>
```

Le ping suivant est à partir du PC d'Alycia vers le PC de Pierre :

```
0.0.0.0

C:\> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

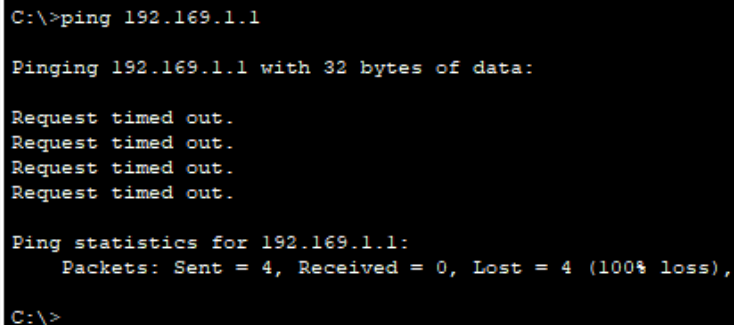
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

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

C:\>
```

Job 7 :

En réalisant le ping à partir du PC d'Alycia vers l'ordinateur hors tension de Pierre, cela donne les résultats suivants :



```
C:\>ping 192.169.1.1

Pinging 192.169.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.169.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Q.1 Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

Pierre n'a pratiquement reçu aucun paquet de la part du PC d'Alycia.

Q.2 Pourquoi ?

Lorsqu'un ordinateur est éteint, son interface réseau n'est plus active, et il n'a pas la capacité de recevoir ou de répondre à des paquets de données réseau. Le protocole ICMP (Internet Control Message Protocol), utilisé par "ping", nécessite une réponse de l'ordinateur cible pour fonctionner. Si l'ordinateur cible est hors tension, il ne peut pas répondre aux requêtes "ping", ce qui entraîne une absence de réponse.

En résumé, la commande "ping" ne peut vérifier la connectivité que lorsque l'ordinateur cible est actif et accessible sur le réseau. Si l'ordinateur que vous essayez de "ping" est éteint, vous ne recevrez pas de réponse à la commande "ping".

Job 8 :

Q.1 Quelle est la différence entre un hub et un switch ?

Avant de répondre à cette question, je dois savoir ce que le **Hub** et le **switch** signifie.

Le Hub : Un Hub est un périphérique qui connecte plusieurs périphériques Ethernet sur un même réseau et les faire fonctionner ensemble en un seul réseau. Un Hub ne collecte pas d'informations. Tandis qu'un switch est un périphérique réseau qui effectue le même travail que le Hub mais qui est considéré comme un Hub plus intelligent car il collecte des informations sur les paquets de données qu'il reçoit et les transmet au seul réseau auquel il était destiné.

Un switch : Un commutateur réseau, ou switch, est un équipement qui relie plusieurs segments dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage.

La grande différence entre le **hub** et le **switch** informatique est la façon dont les trames sont livrées. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée tandis que Le commutateur effectue un tri des trames afin de les orienter vers le bon port et donc vers le bon équipement.

Voici un tableau de comparaison qui différencie le hub et un switch :

	Hub	Switch
Couche	Couche physique. Les Hubs fonctionnent sur la couche 1 selon le modèle OSI.	Couche de liaison de données. Les Switch fonctionnent sur la couche 2 du modèle OSI.
Fonction	Pour connecter un réseau d'ordinateurs, vous pouvez les connecter via un hub central.	Autoriser les connexions à plusieurs périphériques, gérer les ports, gérer les paramètres de sécurité du VLAN
Les ports	4/12 ports	Le switch est un bridge multi-port ou de 24/48 ports
Type d'appareil	Périphérique passif (sans logiciel)	Périphérique actif (avec logiciel)
Utilisé dans	LAN	LAN
Adresse MAC	Un Hub ne peut comprendre ou stocker une adresse MAC.	Un Switch comprend et stocke les adresses MAC.
Mode de transmission	Half duplex	Half/Full duplex
Domaine de Broadcast	Hub a un domaine de Broadcast	Switch a un domaine de Broadcast, sauf si le VLAN est implémenté
La vitesse	10Mbps	10/100 Mbps, 1 Gbps
Catégorie de l'appareil	Dispositif non intelligent	Dispositif intelligent

Q.2 Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?

Avantages : Un hub contient plusieurs ports. Lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local puissent accéder à tous les paquets. Le hub sert comme point de connexion commun pour les périphériques d'un réseau.

Inconvénients : Comme un tel système ne peut être mis en quarantaine, le trafic de données n'est pas protégé. Les potentiels problèmes de sécurité ou les éventuelles préoccupations liées à la protection des données concernent forcément tous les hôtes connectés.

Q.3 Quels sont les avantages et inconvénients d'un switch ?

Avantages : Le switch présente plusieurs avantages dans la gestion de votre parc informatique. Il contribue à la sécurité du réseau et à la protection des données échangées via le réseau. D'autre part, il permet de connecter davantage de postes de travail sur le même réseau Ethernet.

Inconvénients :

- **Coûteux :** Ils sont plus coûteux que les étendues de réseau.
- **Problèmes de disponibilité difficiles :** Les problèmes de disponibilité du réseau sont difficiles à suivre via le changement d'organisation.
- **Problèmes de diffusion du trafic :** Le trafic de diffusion peut être problématique.
- **Sans défense :** Si les commutateurs sont en mode aveugle, ils sont sans défense contre les attaques de sécurité, par exemple la caricature d'adresse IP ou la capture de contours Ethernet.
- **Nécessité d'une planification appropriée :** Une planification et un agencement appropriés sont nécessaires pour traiter les colis multidiffusion.

Q.4 Comment un switch gère-t-il le trafic réseau ?

Un switch gère le trafic réseau en utilisant des informations contenues dans les trames de données pour prendre des décisions sur la manière de transmettre ces données aux périphériques appropriés.

Voici comment un switch gère le trafic réseau :

Apprentissage des adresses MAC : Lorsque des données arrivent sur un port du switch, le switch analyse la trame de données pour extraire l'adresse MAC source du périphérique émetteur. Il maintient ensuite une table de correspondance (table CAM - Content Addressable Memory) qui enregistre ces adresses MAC avec les ports correspondants.

Filtrage et commutation : Lorsque des données sont destinées à un périphérique spécifique, le switch utilise la table d'adresse MAC pour déterminer sur quel port se trouve ce périphérique. Il transmet ensuite la trame de données uniquement sur ce port, évitant ainsi de diffuser les données sur l'ensemble du réseau. Cela réduit la congestion du réseau.

Broadcast : Lorsque le switch reçoit une trame de diffusion (broadcast), il la transmet à tous les ports, car les diffusions sont destinées à tous les périphériques du réseau. Cependant, le switch n'envoie pas la trame de diffusion de retour sur le port source, car cela provoquerait une boucle de diffusion (broadcast storm).

Gestion des collisions : Les switches gèrent les collisions de manière efficace en isolant les appareils sur des segments distincts appelés "collision domaines." Cela signifie que les collisions sont rares, car chaque segment ne comporte que deux périphériques (un émetteur et un récepteur), ce qui améliore la performance du réseau.

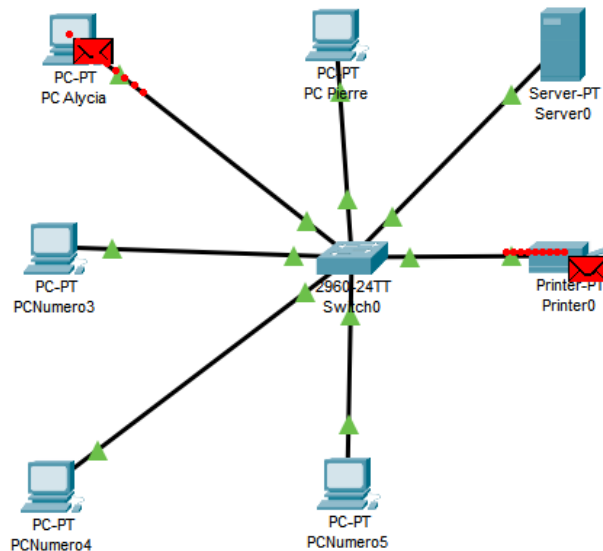
Mise à jour de la table CAM : La table CAM du switch est dynamique et s'adapte au trafic du réseau. Si le switch détecte qu'un périphérique a changé de port, il met à jour sa table d'adresses MAC en conséquence.

Agrégation de liens : Certains switches avancés prennent en charge l'agrégation de liens (link aggregation), ce qui permet de combiner plusieurs ports physiques en un seul canal logique pour augmenter la bande passante et la redondance. Dans l'ensemble, le switch assure une gestion efficace du trafic en acheminant les données uniquement vers les ports nécessaires en fonction de l'adresse MAC de destination, en minimisant les diffusions inutiles et en minimisant les collisions. Cela améliore considérablement les

performances du réseau par rapport à l'utilisation d'un hub, qui diffuse les données à tous les ports sans discernement.

Job 9 :

Le schéma est représenté comme celui-ci :



En ayant rajouté une imprimante puis l'avoir configurée en lui rajoutant une adresse IP connecté au routeur.

Un schéma, qu'il s'agisse d'un diagramme, d'une représentation graphique ou d'une structure visuelle, peut offrir plusieurs avantages importants dans divers contextes.

Voici trois avantages clés :

Clarté de la communication : Les schémas permettent de représenter des informations complexes de manière concise et visuelle. Ils simplifient la communication en transformant des idées abstraites ou des données complexes en une forme facilement compréhensible. Cela facilite la transmission d'informations entre les individus, en particulier lorsque des explications verbales pourraient être ambiguës.

Aide à la prise de décision : Les schémas peuvent être un outil précieux pour la prise de décision. Ils permettent de visualiser les relations entre les éléments d'un problème ou d'une situation, ce qui peut aider à identifier des tendances, des modèles ou des solutions potentielles. Par exemple, dans le domaine des affaires,

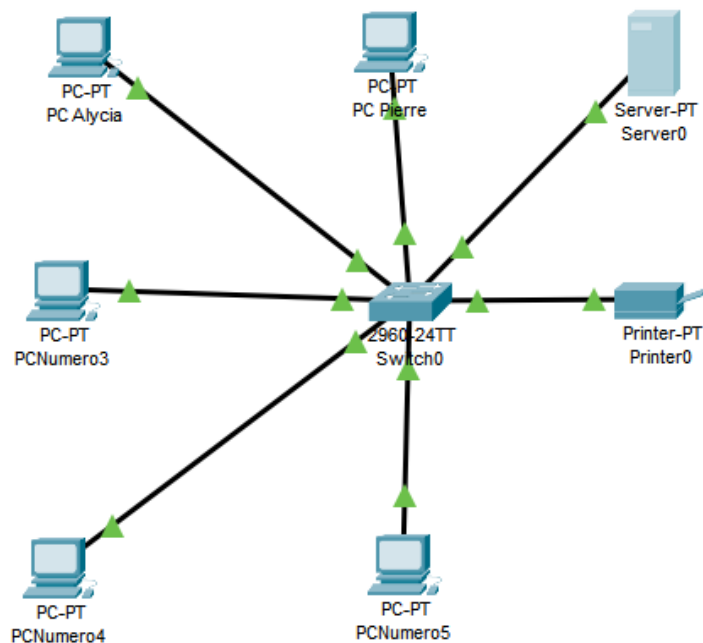
les diagrammes de flux, les organigrammes et les graphiques peuvent aider à planifier des processus, à hiérarchiser des tâches ou à présenter des données de manière à soutenir la prise de décision.

Mémorisation et compréhension accrues : Les êtres humains sont naturellement visuels, ce qui signifie que nous avons tendance à mieux retenir et à comprendre l'information lorsqu'elle est présentée sous forme de schéma. Les schémas aident à organiser l'information de manière logique et à la présenter de manière mémorable. C'est pourquoi les enseignants, les formateurs et les créateurs de contenu éducatif utilisent souvent des schémas pour faciliter l'apprentissage et la rétention des connaissances.

En résumé, les schémas sont des outils puissants pour simplifier la communication, faciliter la prise de décision et améliorer la compréhension et la rétention de l'information. Ils sont utilisés dans de nombreux domaines, de l'éducation à la gestion, en passant par la science et la technologie, pour aider à organiser des idées complexes et à les rendre accessibles.

Job 10 :

J'ai reliés le serveur à tous les ordinateurs existants sur le schéma représenté ci-dessous :



Q.1 Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

Comme l'adresse IP statique requiert des configurations manuelles, elle peut créer des problèmes de réseau en cas d'utilisation sans une bonne maîtrise du protocole TCP/IP. DHCP est un protocole permettant d'automatiser la tâche d'attribution des adresses IP.

Job 11 :

J'ai définis ci-dessous le plan d'adressage :

Hôtes	Adresse IP
12	10.0.0.2 à 10.0.0.13
30	10.1.0.1 à 10.1.0.30
30	10.2.0.1 à 10.2.0.30
30	10.3.0.1 à 10.3.0.30
30	10.4.0.1 à 10.4.0.30
30	10.5.0.1 à 10.5.0.30
120	10.6.0.1 à 10.6.0.120
120	10.7.0.1 à 10.7.0.120
120	10.8.0.1 à 10.8.0.120
120	10.9.0.1 à 10.9.0.120
120	10.10.0.1 à 10.10.0.120
160	10.11.0.160 à 10.11.0.160
160	10.12.0.160 à 10.12.0.160
160	10.13.0.160 à 10.13.0.160
160	10.14.0.160 à 10.14.0.160
160	10.15.0.160 à 10.15.0.160

Q.1 Pourquoi a-t-on choisi une adresse 10.0.0.0 de classe A ?

La raison principale pour laquelle on utilise l'adresse 10.0.0.0 de classe A dans les réseaux privés est sa disponibilité d'adresses IP. Avec une classe A, il y a une énorme quantité d'adresses IP disponibles pour l'attribution aux dispositifs du réseau, ce qui est généralement bien plus que suffisant pour la plupart des réseaux privés. En outre, l'utilisation d'une adresse de classe A permet une grande flexibilité dans la subdivision des réseaux privés en sous-réseaux plus petits en utilisant des masques de sous-réseau appropriés.

Q.2 Quelle est la différence entre les différents types d'adresses ?

Pour commencer, il existe plusieurs types d'adresses IP, chacun ayant une fonction et une portée spécifiques dans le contexte du protocole Internet (IP). Voici les principales catégories d'adresses IP et leurs différences :

Adresse IP version 4 (IPv4) :

IPv4 est le protocole IP original et le plus largement utilisé.

Les adresses IPv4 sont des séquences de 32 bits, généralement représentées sous forme de quatre nombres décimaux séparés par des points (par exemple, 192.168.1.1).

Les adresses IPv4 sont divisées en classes (A, B, C, D, E), mais la notation CIDR (Classless Inter-Domain Routing) est couramment utilisée pour permettre une allocation plus flexible des adresses.

Les adresses IPv4 sont largement épuisées, car il n'y a qu'un nombre limité d'adresses disponibles (environ 4 milliards).

Adresse IP version 6 (IPv6) :

IPv6 est le protocole IP de nouvelle génération conçu pour remplacer IPv4.

Les adresses IPv6 sont composées de 128 bits.

Les adresses IPv6 sont généralement représentées sous forme hexadécimale, séparées par des deux-points.

IPv6 a été développé pour faire face à l'épuisement imminent des adresses IPv4 et pour répondre aux besoins croissants de l'Internet des objets (IoT).

Adresse IP publique :

Une adresse IP publique est une adresse utilisée pour identifier un dispositif ou un réseau sur Internet.

Elle est routable sur Internet et peut être utilisée pour communiquer directement avec des ressources sur le réseau mondial.

Les fournisseurs d'accès Internet (FAI) attribuent des adresses IP publiques aux utilisateurs, mais le nombre d'adresses IPv4 publiques disponibles est limité.

Adresse IP privée : Les adresses IP privées sont utilisées à l'intérieur de réseaux privés, comme les réseaux domestiques ou d'entreprise.

Elles ne sont pas routables sur Internet et sont généralement utilisées pour le trafic interne d'un réseau.

Adresse IP réservée : Certaines adresses IP sont réservées à des fins spécifiques. 127.0.0.1 est réservée pour la boucle locale (localhost) dans IPv4, tandis que des

plages d'adresses sont réservées pour des usages spécifiques, comme les adresses multicast dans IPv4 (classe D) et IPv6.

Adresse IP statique vs dynamique : Une adresse IP statique est une adresse fixe attribuée manuellement à un dispositif. Elle ne change pas.

Une adresse IP dynamique est attribuée par un serveur DHCP (Dynamic Host Configuration Protocol) et peut changer périodiquement.

Job 12 :

Qu'est ce qu'un modèle OSI ?

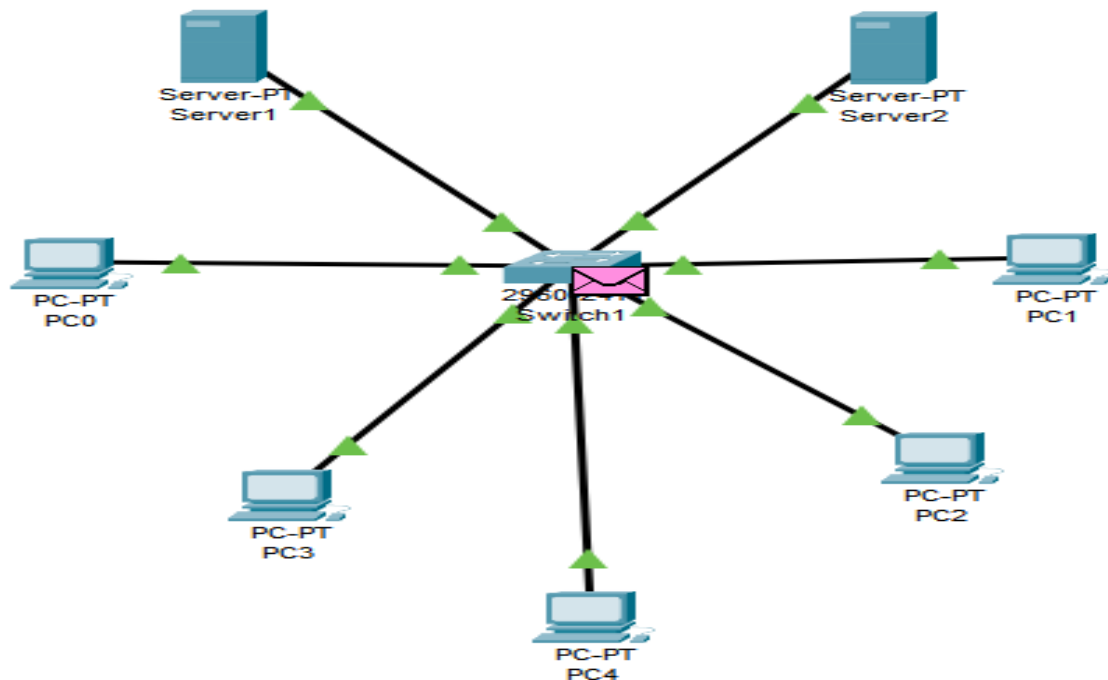
Le modèle OSI est une norme de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

Réalisation du tableau des sept couches du modèle OSI correspondant à leurs rôles ainsi qu'à leurs matériaux correspondants :

Couche OSI	Rôles	Matériels/Protocoles
Couche 1 - Physique	Transmission de bits sur un support physique	Fibre optique, câble RJ45
Couche 2 - Liaison de données	Gestion des trames, contrôle d'accès au support	Ethernet, MAC, Wi-Fi, câble RJ45
Couche 3 - Réseau	Routage des données, adressage logique	IPv4, IPv6, routeur
Couche 4 - Transport	Gestion de la communication point à point, contrôle d'erreur	TCP, UDP
Couche 5 - Session	Gestion de sessions et de connexions	SSL/TLS, PPTP
Couche 6 - Présentation	Translation des données, cryptage, compression	SSL/TLS, HTML
Couche 7 - Application	Interface utilisateur, communication avec les applications	HTTP, FTP, PPTP, SSL/TLS, HTML

Job 13 :

Q.1 Quel est l'architecture de ce réseau ?



Cet architecture réseau correspond à une architecture d'étoile :

Dans une architecture en étoile, tous les dispositifs du réseau sont connectés à un concentrateur central (communément appelé commutateur ou routeur). Les dispositifs ne sont pas directement connectés les uns aux autres. C'est une architecture courante pour les réseaux locaux (LAN) et les réseaux domestiques.

Q.2 Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est de **192.168.10.0**.

Q.3 Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?

Nous pouvons brancher 256 machines sur ce réseaux car le masque de sous-réseaux comme l'indique la consigne est définit à 255.255.255.0 et étant donné que pour le masque de sous-réseau que nous utilisons détermine la taille du sous-réseau et le nombre d'adresses IP disponibles. Par exemple, un masque de sous-réseau de 255.255.255.0 permet 256 adresses IP.

Q.4 Quelle est l'adresse de diffusion de ce réseau ?

Pour calculer l'adresse de diffusion du réseau 192.168.10.0, nous avons besoin de connaître le masque de sous-réseau associé. Les adresses de diffusion dépendent du masque de sous-réseau car elles sont calculées en fonction de ce masque. Supposons que le masque de sous-réseau soit 255.255.255.0, ce qui est courant pour un réseau de classe C.

Ensuite, nous effectuons une opération XOR entre l'adresse IP du réseau (192.168.10.0) et l'inverse du masque de sous-réseau (0.0.0.255) pour trouver l'adresse de diffusion. Voici le calcul :

Adresse de diffusion = 192.168.10.0 + 0.0.0.255

En binaire, cela donne :

192.168.10.0 : 11000000.10101000.00001010.00000000 0.0.0.255 :
00000000.00000000.00000000.11111111

Effectuons l'opération en additionnant octet par octet :

Pour le premier octet : 11000000 + 00000000 = 11000000

Pour le deuxième octet : 10101000 + 00000000 = 10101000

Pour le troisième octet : 00001010 + 00000000 = 00001010

Pour le quatrième octet : 00000000 + 11111111 = 11111111

L'adresse de diffusion est donc **192.168.10.255** pour ce réseau spécifique avec un masque de sous-réseau de **255.255.255.0**.

Job 14 :

Q.1 Convertir cette adresse IP en nombre binaires : **145.32.59.24** :

10010001.00100000.00111011.00011000.

Q.2 Convertir cette adresse IP en nombre binaires : **200.42.129.16** :

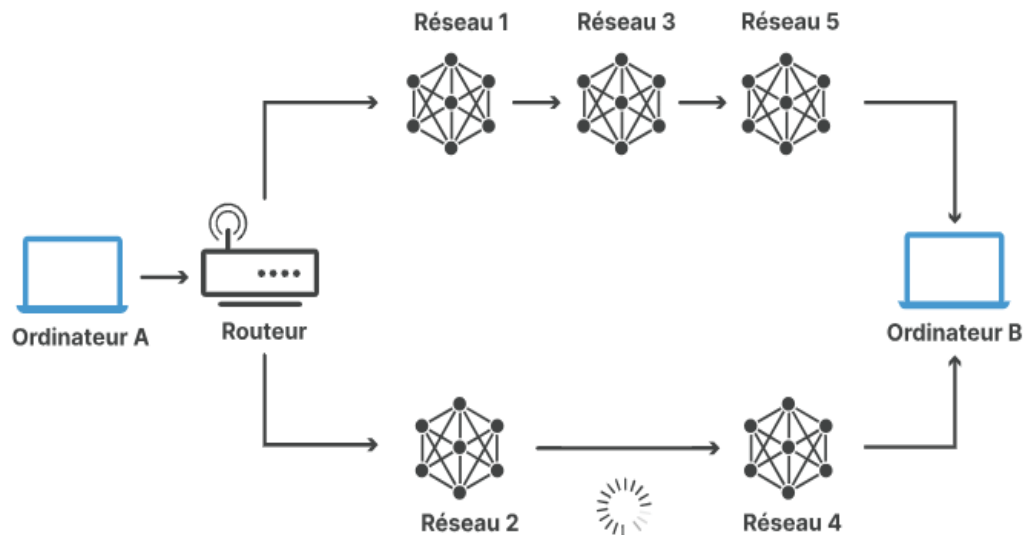
11001000.00101010.1000001.00010000.

Q.3 Convertir cette adresse IP en nombre binaires : **14.82.19.54** :

00001110.01010010.00010011.00110110.

Job 15 :

Q.1 Qu'est-ce que le routage ?



Le routage réseau est le processus de sélection d'un chemin à travers un ou plusieurs réseaux. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP pour se rendre de leur origine à leur destination. Ces décisions de routage Internet sont prises par des périphériques réseau spécialisés appelés routeurs.

Pour qu'un paquet de données puisse se rendre de l'ordinateur A à l'ordinateur B, doit-il passer par les réseaux 1, 3 et 5 ou les réseaux 2 et 4 ? Le paquet empruntera un chemin plus court via les réseaux 2 et 4, mais les réseaux 1, 3 et 5 pourraient s'avérer plus rapides pour acheminer les paquets. C'est là le genre de choix que les routeurs réseau effectuent en permanence.

Q.2 Qu'est-ce qu'un gateway ?

Une gateway désigne en informatique un dispositif matériel et logiciel qui permet de relier deux réseaux informatiques, ou deux réseaux de télécommunications, aux caractéristiques différentes. La plupart du temps, la passerelle applicative a pour mission de relier un réseau local à Internet. La gateway la plus connue est ainsi la box Internet.

Comment fonctionne une gateway ?

Lorsque l'utilisateur d'un réseau souhaite accéder à un réseau utilisant un protocole différent, la gateway examine la légitimité de sa demande. Si celle-ci respecte les conditions fixées par l'administrateur du réseau visé, alors la gateway établit une liaison entre les deux réseaux. La passerelle joue ainsi un rôle de pare-feu et participe à la sécurisation des échanges via des protocoles réseau différents.

Sur le plan technique, il existe diverses formes de passerelles : un répéteur est considéré comme une passerelle de niveau 1, un pont comme une passerelle de niveau 2 et un routeur comme une passerelle de niveau 3.

Q.3 Qu'est-ce qu'un VPN ?



Un réseau privé virtuel (VPN) est un moyen de se connecter à internet d'une manière plus sûre ou plus privée. Lorsque vous vous connectez à internet, c'est votre fournisseur d'accès (Orange, Free, SFR, Bouygues, etc.) qui vous met en relation avec un site web. En une fraction de seconde les serveurs des fournisseurs trouvent où se situe le site web sur la toile (son adresse IP) et guident votre navigateur pour afficher le site sur votre ordinateur ou smartphone.

Lorsque vous vous connectez avec un service VPN, votre fournisseur vous met en relation avec un ordinateur distant, un serveur, détenu par le service VPN que vous avez choisi. Il chiffre (brouille) les informations échangées entre vous et le reste d'internet. Lors de la connexion à un site web, c'est le serveur VPN qui relaie la demande, votre fournisseur d'accès internet n'a plus accès à cette information.

Q.4 Qu'est-ce qu'un DNS ?

Pour faciliter la recherche d'un site donné sur Internet, le système de noms de domaine (DNS) a été inventé. Le DNS permet d'associer un nom compréhensible, à une adresse IP. On associe donc une adresse logique, le nom de domaine, à une adresse physique l'adresse IP.

Le nom de domaine et l'adresse IP sont uniques. Le DNS permet à notre message d'atteindre son destinataire et non quelqu'un d'autre possédant un nom de domaine similaire. Il nous permet également de taper «www.nameshield.com» sans avoir à saisir une longue adresse IP et d'accéder au site web approprié.

Pour ces opérations ce sont principalement deux types de serveurs qui sont utilisés :

Le Serveur faisant autorité : Serveur DNS qui connaît le contenu d'un domaine. (Les serveurs de l'AFNIC connaissent ce qu'il y a dans .Fr et peuvent répondre).

Résolveur ou serveur récursif : serveur DNS qui ne connaît pas le contenu d'un domaine mais pose des questions aux serveurs faisant autorité et mémorise les réponses. (Chez le FAI, ou sur le réseau local).

