Run Track Réseau :

Job 2 :

➔ Qu'est-ce qu'un réseau ?

Un réseau est une structure interconnectée facilitant la transmission d'informations, de ressources ou d'énergie entre des entités distinctes. En informatique, un réseau peut être local *(LAN)* ou étendu *(WAN)*, reliant des ordinateurs pour partager des données.

Sur les médias sociaux, un réseau désigne une plateforme en ligne permettant aux individus de se connecter et d'échanger. Dans le contexte électrique, un réseau distribue l'électricité via des connexions complexes. Les réseaux peuvent également se manifester dans le transport, la biologie, et d'autres domaines, représentant des connexions interdépendantes entre différents éléments pour favoriser la communication, la distribution ou la coopération.

➔ À quoi sert un réseau informatique ?

Un réseau informatique sert à faciliter la communication et le partage de ressources entre des ordinateurs et périphériques connectés.
Il permet le partage de fichiers, l'accès à des bases de données, la collaboration en ligne, la gestion des ressources, l'accès à distance, la sauvegarde centralisée, et offre une connectivité à Internet.
Ces fonctionnalités améliorent l'efficacité, la productivité et la flexibilité au sein d'organisations et facilitent la vie quotidienne des utilisateurs en simplifiant l'accès à l'information et aux services.

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

La construction d'un réseau informatique nécessite plusieurs composants matériels. Voici une liste des éléments essentiels et leurs fonctions :

Switch (commutateur) :

- **Fonction :** Permet de connecter plusieurs appareils au sein d'un réseau local **(LAN).** Les switchs dirigent le trafic réseau en fonction des adresses *MAC* des dispositifs, facilitant ainsi la communication entre eux.

Routeur :

- **Fonction :** Connecte différents réseaux, tels que votre réseau local à Internet. Les routeurs dirigent le trafic entre ces réseaux en utilisant des adresses IP. Ils offrent également des fonctionnalités de sécurité et peuvent attribuer des adresses IP aux dispositifs connectés.

Modem :

- **Fonction :** Convertit les signaux numériques des ordinateurs en signaux analogiques ou numériques adaptés à la connexion Internet. Il permet l'accès à Internet en se connectant au fournisseur de services Internet **(FSI)**.

Points d'accès Wi-Fi :

- **Fonction :** Permettent aux dispositifs sans fil de se connecter au réseau. Ils étendent la portée du réseau, offrant une connectivité sans fil dans une zone donnée.

Câbles Ethernet :

- **Fonction :** Utilisés pour connecter les périphériques au réseau à l'aide de prises Ethernet. Les câbles peuvent être de

catégories différentes **(par exemple, Cat5e, Cat6)** en fonction des besoins de vitesse et de performance.

Cartes réseau :

- Fonction : Intégrées aux ordinateurs ou ajoutées en tant que carte d'extension, les cartes réseau permettent à un dispositif de se connecter physiquement au réseau.

Serveurs :

- Fonction : Fournissent des services tels que le stockage de fichiers, la gestion des utilisateurs, les bases de données, les applications, etc. Ils jouent un rôle central dans la fourniture de ressources et de services aux utilisateurs du réseau.

Firewall :

- Fonction : Protège le réseau en filtrant le trafic, en bloquant les accès non autorisés et en surveillant les communications pour prévenir les menaces de sécurité.

Câblage structuré :

- Fonction : Ensemble organisé de câbles et de connecteurs qui forment l'infrastructure physique du réseau. Le câblage structuré inclut les câbles Ethernet, les connecteurs et les panneaux de brassage.

L'assemblage de ces composants crée une infrastructure réseau qui permet la communication, le partage de ressources et l'accès à Internet au sein d'une organisation ou d'une maison.

Job 3 :

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

Pour relier les 2 ordinateurs j'ai choisi le cable *"Cropper cross over"* qui est un câble croisé je l'ai choisi car le cordon croisé est utilisé pour les connexions entre homologues **(peer-to-peer)** ce qui veut dire qu'il est utile pour relier nos 2 ordinateurs.

Job 4 :

Questions :

➔ Qu'est-ce qu'une adresse IP ?

Une adresse IP, ou Protocole Internet, est une étiquette numérique attribuée à chaque appareil connecté à un réseau informatique, lui permettant d'être identifié et de communiquer.
Ces adresses uniques, sous la forme de séquences de chiffres ou alphanumériques, facilitent le routage des données sur Internet.

Il existe deux types principaux d'adresses IP, IPv4 et IPv6. Les adresses IP sont essentielles pour la navigation en ligne, car elles aident à diriger les informations entre les appareils. Elles peuvent être statiques (fixes) ou dynamiques (temporaires), et leur utilisation s'étend de la navigation Web aux connexions réseau locales.

➔ À quoi sert un IP ?

Une adresse IP *(Internet Protocol)* sert principalement à identifier et à localiser de manière unique un appareil sur un réseau, notamment sur Internet. Cela permet le routage des données, assurant qu'elles atteignent leur destination correcte. Les principales utilisations d'une adresse IP incluent :

Identification : Chaque appareil connecté à un réseau, qu'il s'agisse d'un ordinateur, d'un smartphone, d'un routeur, ou d'autres périphériques, est attribué une adresse IP unique pour l'identifier de manière distincte.

Communication : L'adresse IP est utilisée pour acheminer les données d'un appareil à un autre à travers le réseau. Elle est intégrée à la communication sur Internet, permettant l'échange d'informations entre les utilisateurs, les serveurs, et d'autres dispositifs connectés.

Routage : Les adresses IP sont cruciales pour le routage des paquets de données à travers les réseaux, en assurant que l'information atteigne sa destination correcte de manière efficace. Hébergement de services : Les serveurs sur Internet, tels que les sites web, les services de messagerie, et les applications, sont également identifiés par des adresses IP, permettant aux utilisateurs d'accéder à ces services en utilisant leur navigateur ou d'autres applications.

Gestion du réseau : Les adresses IP sont utilisées dans la configuration et la gestion des réseaux. Les administrateurs réseau peuvent attribuer des adresses IP de manière statique ou dynamique, et utiliser des protocoles spécifiques pour organiser et surveiller le trafic réseau.

En résumé, l'adresse IP joue un rôle fondamental dans la connectivité et la communication au sein des réseaux, en particulier sur Internet, en permettant l'identification, le routage, et la transmission d'informations entre les appareils connectés.

➔ Qu'est-ce qu'une adresse MAC ?

Une adresse *MAC* **(Media Access Control)** est une étiquette unique assignée à l'interface réseau de chaque appareil, comme une carte réseau sur un ordinateur ou un adaptateur sans fil sur un smartphone. Composée de chiffres hexadécimaux, elle sert d'identifiant physique fixe, attribué par le fabricant. L'adresse *MAC* facilite le routage des données au sein d'un réseau local **(LAN)** en assurant l'acheminement précis vers la bonne interface.

Elle est utilisée dans la résolution d'adresses **ARP**, le contrôle d'accès réseau, et demeure stable même si l'appareil se déplace, bien qu'elle ne soit généralement pas routable à l'échelle d'Internet.

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

Les adresses IP publiques et privées sont deux concepts clés dans la gestion des réseaux, en particulier dans le contexte des réseaux locaux *(LAN)* et d'Internet.

Adresse IP publique :

- Définition : Une adresse IP publique est une adresse unique attribuée à un appareil sur Internet. C'est l'adresse qui est visible sur le réseau mondial, permettant à cet appareil de communiquer avec d'autres appareils à l'échelle mondiale

- **Utilisation :** Les adresses IP publiques sont utilisées pour identifier les routeurs et les serveurs directement connectés à Internet, permettant à ces dispositifs d'être accessibles depuis n'importe où sur le réseau mondial.

Adresse IP privée :

- Définition : Une adresse IP privée est une adresse attribuée à un appareil au sein d'un réseau local *(LAN)*, tel qu'un réseau domestique ou d'entreprise. Ces adresses ne sont pas directement accessibles depuis Internet.

- Utilisation : Les adresses IP privées sont utilisées pour permettre la communication au sein du réseau local, mais elles ne sont pas routables sur Internet. Les routeurs utilisent des mécanismes de traduction d'adresse réseau *(NAT)* pour permettre aux appareils avec des adresses IP privées d'accéder à Internet en utilisant l'adresse IP publique du routeur.

En résumé, les adresses IP publiques sont utilisées pour l'identification sur Internet, tandis que les adresses IP privées sont utilisées pour la communication à l'intérieur des réseaux locaux. La combinaison de ces deux types d'adresses et l'utilisation du *NAT* permettent à plusieurs appareils dans un réseau local d'accéder à Internet en partageant une seule adresse IP publique.

➔ Quelle est l'adresse de ce réseau ?

```
Carte réseau sans fil Wi-Fi 3 :

   Suffixe DNS propre à la connexion. . . : laplateforme.io
   Adresse IPv6 de liaison locale. . . . .: fe80::dfd9:3f47:760b:3a6%7
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.3.33
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.10.0.1
```

Job 5 :

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

La ligne de commande que j'ai utilisé pour vérifier l'id des machines est **"ipconfig"**.

```
C:\Users\pc>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

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

Carte Ethernet Ethernet 2 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::fcfa:113a:abd8:f9f5%19
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.56.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :

Carte réseau sans fil Connexion au réseau local* 1 :

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

Carte réseau sans fil Connexion au réseau local* 2 :

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

Carte Ethernet Ethernet 3 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::d90f:cb63:3987:695%11
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.137.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

Job 6 :

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

La commande permettant de ping entre des pc est *"ping + adresse ip du pc"*.

```
C:\>ping 198.168.1.1

Pinging 198.168.1.1 with 32 bytes of data:

Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 198.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>ping 198.168.1.2

Pinging 198.168.1.2 with 32 bytes of data:

Reply from 198.168.1.2: bytes=32 time=11ms TTL=128
Reply from 198.168.1.2: bytes=32 time=4ms TTL=128
Reply from 198.168.1.2: bytes=32 time<1ms TTL=128
Reply from 198.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 198.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 4ms
```

Job 7 :

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

Non, le PC de pierre n'a pas reçu les paquets envoyés par Alicia.

Expliquer pourquoi.

Tout simplement car le PC de pierre est éteint donc le délai de de la demande à été dépassé.

```
C:\Users\pc>ping 192.168.1.1

Envoi d'une requête 'Ping'  192.168.1.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Job 8 :

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

Un switch est semblable à un hub, mais avec des fonctionnalités supplémentaires.
Les commutateurs réseau peuvent identifier et filtrer les données à des fins de sécurité, et leur permettent également de segmenter le réseau local en plusieurs sous-réseaux.
Les routeurs utilisent le modèle *OSI* pour transmettre des données entre différents réseaux.
La principale différence entre un switch et un routeur est que le premier est utilisé pour connecter des périphériques sur un réseau local, tandis que le second est utilisé pour relier des réseaux entre eux.

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

Un hub fonctionne en diffusant les données reçues à tous les appareils connectés, agissant comme un répétiteur.
Ses avantages incluent un coût moindre et une simplicité d'installation. Cependant, les inconvénients sont significatifs : il partage la bande passante entre tous les appareils, entraînant des collisions, une performance réduite, et une sécurité limitée, car toutes les données sont diffusées à tous les ports.
Son manque d'intelligence pour diriger spécifiquement les données vers un destinataire les rend inefficaces pour les réseaux modernes, et les switches sont généralement préférés pour une gestion plus efficace du trafic et une sécurité améliorée.

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

Avantages d'un Switch :

Efficacité : Un switch fonctionne au niveau de la couche de liaison de données, transmettant sélectivement les données uniquement au port destinataire, améliorant l'efficacité du réseau.

Bande passante dédiée : Chaque port sur un switch dispose de sa propre bande passante, évitant le partage global comme c'est le cas avec un hub.

Performance : Les switches réduisent les collisions et offrent des performances supérieures en dirigeant intelligemment le trafic vers les ports appropriés.
Isolation du trafic : Ils isolent le trafic, améliorant la sécurité en empêchant la diffusion inutile de données à tous les ports.
Adaptabilité : Les switches sont adaptatifs, ajustant dynamiquement la bande passante selon les besoins du réseau.

Isolation du trafic : Ils isolent le trafic, améliorant la sécurité en empêchant la diffusion inutile de données à tous les ports.

Adaptabilité : Les switches sont adaptatifs, ajustant dynamiquement la bande passante selon les besoins du réseau.

Inconvénients d'un Switch :

Coût : Les switches sont généralement plus coûteux que les hubs, ce qui peut être un facteur limitant pour les petits réseaux ou les installations temporaires.

Complexité : La configuration et la gestion des switches peuvent être plus complexes que celles des hubs, nécessitant parfois des compétences spécifiques.

Évolutivité limitée : Dans de grands réseaux, la multiplication des ports peut nécessiter des switches plus puissants, augmentant les coûts.

En résumé, les switches offrent une meilleure performance, une gestion du trafic plus intelligente et une sécurité améliorée par rapport aux hubs, mais ils peuvent être plus coûteux et nécessiter une configuration plus avancée. Ils sont cependant essentiels dans les réseaux modernes pour garantir une communication efficace et sécurisée.

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

Un switch gère le trafic réseau de manière intelligente en fonctionnant au niveau de la couche de liaison de données du modèle *OSI* **(Open Systems Interconnection)**. Voici comment il gère le trafic :

Inspection des adresses MAC : Lorsqu'un switch reçoit des trames *(frames)* de données, il examine l'adresse *MAC* **(Media Access Control)** de la trame pour identifier l'appareil source et destination.

Table de commutation (MAC Address Table) : Le switch utilise une table de commutation pour enregistrer les adresses *MAC* des appareils connectés à chaque port. Cette table est mise à jour dynamiquement à mesure que le switch apprend quel appareil est connecté à chaque port.

Transmission sélective : Contrairement à un hub qui diffuse les données à tous les ports, un switch transmet sélectivement les données uniquement au port associé à l'adresse *MAC* de destination, minimisant ainsi la congestion et les collisions sur le réseau.

Élimination des collisions : En transmettant sélectivement, le switch évite les collisions, car chaque port a une bande passante dédiée.

Détection automatique : Les switches détectent automatiquement les nouvelles connexions et ajustent la table de commutation en conséquence.

Optimisation de la bande passante : En fournissant une bande passante dédiée à chaque port, le switch optimise l'utilisation de la bande passante, offrant des performances supérieures par rapport à un hub.

Sécurité améliorée : En transmettant sélectivement, le switch isole le trafic, améliorant la sécurité en évitant la diffusion inutile de données à tous les ports.

En résumé, le switch gère le trafic en utilisant des adresses *MAC* pour diriger sélectivement les données vers le port approprié, offrant ainsi une performance, une sécurité et une efficacité accrues par rapport aux dispositifs de réseau moins avancés tels que les hubs.

Job 9 :

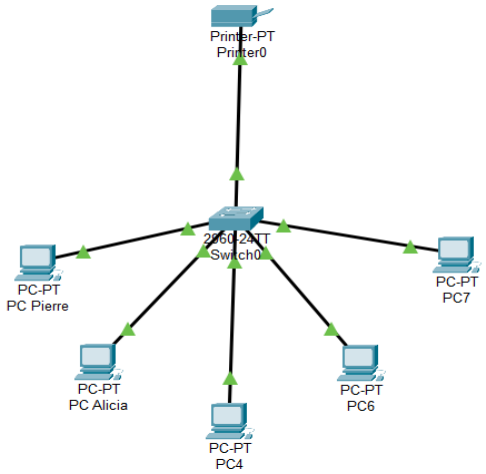
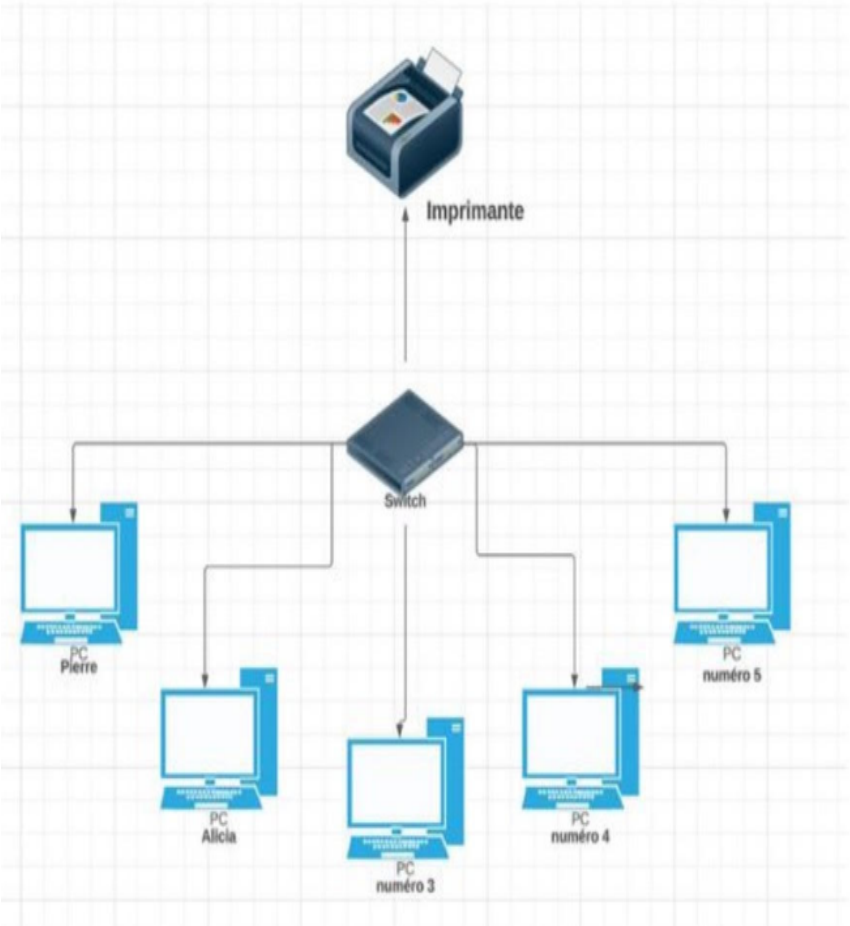


Schéma de mon réseau ci dessous :



Les 3 avantages d'avoir un schéma sont :

Compréhension Visuelle :

- Un schéma offre une représentation visuelle claire de la structure et de la topologie d'un système ou d'un processus. Cela facilite la compréhension rapide et complète, même pour ceux qui ne sont pas experts dans le domaine.

Communication Efficace :

- Il facilite la communication entre les membres de l'équipe et les parties prenantes en fournissant un moyen visuel de présenter des informations complexes. Cela réduit les malentendus et favorise une communication plus efficace.

Planification et Gestion :

- Un schéma sert de base pour la planification et la gestion d'un système. Il permet d'identifier les composants clés, les connexions et les relations, ce qui facilite la prise de décision

stratégique, la gestion des ressources et la résolution de problèmes potentiels.

Job 10 :

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

Adresse IP statique :

- **Définition :** Une adresse IP statique est une adresse IP qui est manuellement configurée pour un appareil et reste fixe. Elle ne change pas, sauf si elle est modifiée manuellement.
- **Configuration :** L'utilisateur ou l'administrateur réseau doit spécifier manuellement l'adresse IP, ainsi que d'autres paramètres tels que la passerelle par défaut et les serveurs DNS.
- Stabilité : L'adresse IP statique reste constante, ce qui peut être pratique dans certaines situations où la stabilité de l'adresse est importante.
- **Utilisation :** Souvent utilisée pour des serveurs, imprimantes réseau et autres dispositifs nécessitant une adresse IP constante et prévisible.

Adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) :

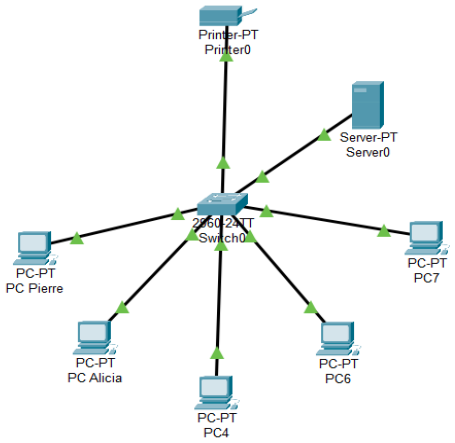
- **Définition :** Une adresse IP attribuée par DHCP est une adresse IP qui est automatiquement assignée à un appareil par un serveur DHCP sur le réseau.
- **Configuration :** Le serveur DHCP configuré dynamiquement l'adresse IP, la passerelle par défaut, les serveurs DNS, etc., au moment de la connexion de l'appareil au réseau.
- **Dynamisme :** L'adresse IP peut changer à chaque nouvelle connexion au réseau, ce qui permet une gestion dynamique des adresses au sein du réseau.
- **Utilisation :** Principalement utilisée pour les ordinateurs de bureau, les ordinateurs portables et les appareils mobiles, offrant une gestion facile et une utilisation efficace des adresses IP.

Différences :

Configuration : L'adresse IP statique est configurée manuellement, tandis que l'adresse IP attribuée par DHCP est automatiquement assignée par un serveur DHCP.

Stabilité : Une adresse IP statique reste constante, alors qu'une adresse IP attribuée par DHCP peut changer à chaque connexion.
Gestion : Les adresses IP statiques nécessitent une gestion manuelle, tandis que DHCP simplifie la gestion des adresses IP en les attribuant dynamiquement.

Utilisation : Les adresses IP statiques sont souvent utilisées pour des dispositifs nécessitant une stabilité, tandis que DHCP est couramment utilisé pour les appareils quotidiens dans un réseau, offrant une gestion plus flexible.



Job 11 :

sous-réseau 1	10.0.0.1	10.0.0.13	255.0.0.0
sous-réseau 2	10.0.0.14	10.0.0.44	255.0.0.0
sous-réseau 3	10.0.0.45	10.0.0.106	255.0.0.0
sous-réseau 4	10.0.0.76	10.0.0.137	255.0.0.0
sous-réseau 5	10.0.0.107	10.0.0.137	255.0.0.0
sous-réseau 6	10.0.0.138	10.0.0.168	255.0.0.0
sous-réseau 7	10.0.0.169	10.0.1.34	255.0.0.0
sous-réseau 8	10.0.1.35	10.0.1.155	255.0.0.0
sous-réseau 9	10.0.1.156	10.0.2.21	255.0.0.0
sous-réseau 10	10.0.2.22	10.0.2.142	255.0.0.0
sous-réseau 11	10.0.2.143	10.0.3.8	255.0.0.0
sous-réseau 12	10.0.3.9	10.0.3.169	255.0.0.0
sous-réseau 13	10.0.3.170	10.0.4.75	255.0.0.0
sous-réseau 14	10.0.4.76	10.0.4.236	255.0.0.0
sous-réseau 15	10.0.5..143	10.0.5.142	255.0.0.0
sous-réseau 16	10.0.5.143	10.0.6.48	255.0.0.0

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

On à choisi d'utliser l'adresse 10.0.0.0 de classe A pour les réseaux car elle privilégie flexibilités en termes de gestions des adresses ip répondant notamment au besoins de nombreux réseau locaux ce qui en fait un choix de taille 🙂.

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

Adresse IP : Identifie de manière unique un périphérique sur un réseau IP (par exemple, 192.168.1.1 pour IPv4, ou 2001:0db8:85a3:0000:0000:8a2e:0370:7334 pour IPv6).

Adresse MAC (Media Access Control) : Identifie de manière unique une carte réseau sur un réseau local (par exemple, 00:1A:2B:3C:4D:5E).

Adresse de Diffusion (Broadcast) : Permet d'envoyer un message à tous les périphériques sur un réseau (par exemple, 255.255.255.255 en IPv4).

Adresse de Boucle Locale (Loopback) : Utilisée pour tester la pile réseau d'un périphérique (par exemple, 127.0.0.1 en IPv4).

Adresse Privée et Publique (IPv4) : Les adresses privées sont utilisées à l'intérieur d'un réseau local, tandis que les adresses publiques sont routables sur Internet (par exemple, 192.168.1.1 en privé, assignée par le FAI en public).

URL (Uniform Resource Locator) : Utilisée pour localiser des ressources sur le web (par exemple, http://www.example.com).
Chaque type d'adresse a une fonction spécifique, que ce soit pour l'identification des périphériques, la communication sur le réseau, la gestion du trafic ou la localisation de ressources sur Internet.

Job 12 :

Couche OSI	Descriptions de rôles	Matériels
Couche application	Cette couche est responsable de l'interface entre l'application utilisateur et le reste du modèle OSI. Elle gère les protocoles de haut niveau utilisés pour des applications telles que la messagerie électronique, la navigation web, etc.	HTTP (HTML), FTP, SSL/TLS
Couche 1 (Physique)	La couche physique s'occupe du transfert de bits bruts sur un support de transmission. Elle gère les caractéristiques matérielles, telles que le type de câble, la fibre optique, etc.	Fibre optique, câble RJ45
Couche 2 (Liaison de données)	Cette couche gère la communication entre des nœuds directement connectés. Elle divise les données en trames et gère les adresses MAC pour la livraison des trames.	Ethernet, Wi-Fi, cable RJ45
Couche 3 (Réseau)	La couche réseau est responsable du routage des données entre différents réseaux. Elle utilise des adresses IP pour diriger les paquets vers leur destination.	IPv4, IPv6, routeur
Couche 4 (Transport)	Cette couche assure la fiabilité et le contrôle du flux de bout en bout de la communication. Elle gère également la segmentation et le réassemblage des données.	TCP, UDP
Couche 5 (Session)	La couche de session établit, gère et termine les sessions de communication entre deux applications. Elle gère également la synchronisation entre les applications.	PPTP
Couche 6 (Présentation)	La couche de présentation gère la traduction, la compression et le chiffrement des données pour assurer que les applications des couches supérieures puissent interpréter correctement les informations. SSL/TLS, HTML (pour la présentation)	SSL/TLS, HTML

Job 13 :

➔ Quelle est l'architecture de ce réseau ?

L'architecture est une architecture de classe C masque de sous-réseau par défaut de
255.255.255.0 et leur premier octet est compris entre 192 et 223.

➔ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est 192.168.10 car le masque de sous réseau 255.255.255.0 (les 3 premiers octets de l'adresse IP sont réservés pour le réseau, et le dernier pour les hôtes).

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

Le nombre de machines possibles de brancher est au nombre de 253 sur ce réseau.

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

L'adresse de diffusion de ce réseau est 192.168.10.255, car tous les bits d'hôtes sont définis à 1 dans le dernier octet (255 en décimal), ce qui signifie que c'est l'adresse de diffusion pour le réseau 192.168.10.0/24.

Job 14 :

Convertissez les adresses IP suivantes en binaires :

- **145.32.59.24**

145 en binaire : 10010001
32 en binaire : 00100000
59 en binaire : 00111011
24 en binaire : 00011000

En conclusion.
145.32.59.24 en binaire est : 10010001.00100000.00111011.00011000

- **200.42.129.16**

200 en binaire : 11001000
42 en binaire : 00101010
129 en binaire : 10000001
16 en binaire : 00010000

En conclusion.
200.42.129.16 en binaire est :11001000.00101010.10000001.00010000

- **14.82.19.54**

14 en binaire : 00001110
82 en binaire : 01010010
19 en binaire : 00010011
54 en binaire : 00110110

Et enfin pour conclure 14.82.19.54 en binaire est :
00001110.01010010.00010011.00110110

Job 15 :

➔ Qu'est-ce que le routage ?

Le routage est le processus de transmission efficace des données entre réseaux informatiques. Il implique la sélection du meilleur chemin pour acheminer des paquets de données d'une source vers une destination à travers des dispositifs appelés routeurs.
Ces derniers utilisent des tables de routage et des protocoles spécifiques pour prendre des décisions basées sur les adresses IP.
Le routage permet la connectivité Internet, l'acheminement optimal des données, et joue un rôle crucial dans la communication inter-réseaux. Il facilite la gestion des réseaux complexes en dirigeant intelligemment le trafic pour garantir une transmission efficace et sécurisée.

➔ Qu'est-ce qu'un gateway ?

Un gateway désigne 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 la box Internet.

➔ Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network) est un réseau privé virtuel qui crée une connexion sécurisée sur Internet.
Il permet à un utilisateur d'accéder à des ressources réseau à distance de manière confidentielle et sécurisée.
Le VPN utilise un processus de chiffrement pour protéger les données transitant entre l'utilisateur et le serveur VPN, assurant ainsi la confidentialité et la sécurité des informations. Les VPN sont utilisés pour plusieurs raisons, notamment la protection de la vie privée en masquant l'adresse IP, la contournant des restrictions géographiques, l'accès sécurisé aux réseaux d'entreprise depuis des emplacements distants, et la sécurisation des communications sur les réseaux Wi-Fi publics.

➔ Qu’est-ce qu’un DNS ?

Le DNS (Domain Name System) est un système qui permet de traduire les noms de domaine conviviaux en adresses IP numériques compréhensibles par les ordinateurs. Il s'agit d'un service fondamental sur Internet. Lorsqu'un utilisateur entre un nom de domaine dans son navigateur, le DNS prend en charge la résolution de ce nom en une adresse IP correspondante. Cela facilite la navigation sur le web, car les utilisateurs n'ont pas besoin de mémoriser des adresses IP complexes. Le DNS fonctionne comme un annuaire distribué, avec des serveurs DNS qui se chargent de la conversion des noms de domaine en adresses IP, et vice versa.

Voila la documentation sur runtrack réseau s’achève merci d’avoir pris le temps de le lire

Cordialement Bendassi Imrane.