Runtrack réseau

JOB 2

Qu’est ce qu’un réseau ?

Un réseau informatique est un ensemble d'appareils informatiques interconnectés qui communiquent entre eux pour partager des ressources, des informations et des services. Ces appareils peuvent inclure des ordinateurs, des serveurs, des routeurs, des commutateurs, des imprimantes, des téléphones, des tablettes, des appareils IoT (Internet des objets) et d'autres dispositifs compatibles réseau.

A quoi sert un réseau informatique ?

Un réseau informatique sert à diverses fins essentielles dans le monde moderne, permettant la connectivité, la communication et le partage des ressources. Voici quelques-unes des principales utilisations et fonctions d'un réseau informatique :
Partage de ressources , accès à distance , communication , accès à internet , stockage centralisé, collaboration, automatisation et contrôle, échange d’informations, sécurité et surveillance, réduction des couts.

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

Pour construire un réseau informatique nous avons besoin de divers composants matériels qui remplissent des fonctions spécifiques pour permettre la connectivité. Voici une liste des composants matériels couramment utilisés pour construire un réseau,

avec une description des fonctions de chacun :

Ordinateurs et appareils finaux : Ce sont les dispositifs utilisateurs finaux tels que des ordinateurs, des téléphones, des tablettes, des imprimantes, des serveurs, etc. Ils sont utilisés pour accéder aux ressources et aux services du réseau.

Câbles : Les câbles sont utilisés pour connecter les appareils au réseau. Les câbles Ethernet sont couramment utilisés pour les connexions filaires, tandis que des câbles coaxiaux, à fibre optique ou des connexions sans fil (Wi-Fi) peuvent également être utilisés.

Routeurs : Les routeurs interconnectent différents réseaux, gérant le trafic entre eux. Ils permettent également de partager une seule connexion Internet entre plusieurs appareils.

Commutateurs (Switches) : Les commutateurs permettent de connecter plusieurs appareils au sein d'un réseau local (LAN). Ils acheminent le trafic vers l'appareil approprié en fonction de l'adresse MAC (Media Access Control) de chaque appareil.

Firewalls : Les pare-feu sont des dispositifs de sécurité qui protègent le réseau en filtrant le trafic entrant et sortant, en appliquant des règles de sécurité et en prévenant les menaces potentielles.

Serveurs : Les serveurs stockent et gèrent des ressources et des services, tels que des fichiers, des applications, des bases de données, des sites Web, etc., que les utilisateurs du réseau peuvent accéder.

Points d'accès sans fil (WAP) : Les points d'accès sans fil permettent aux appareils d'accéder au réseau via Wi-Fi. Ils étendent la connectivité sans fil dans un réseau.

Modems : Les modems permettent de se connecter à Internet via une connexion haut débit, comme DSL, câble ou fibre optique. Ils transforment le signal numérique de l'ordinateur en signal analogique pour la transmission via le fournisseur de services Internet (FSI).

Serveurs de fichiers : Ces serveurs sont conçus pour stocker et gérer des fichiers, facilitant le partage de fichiers au sein du réseau.

Imprimantes réseau : Les imprimantes réseau peuvent être partagées entre plusieurs utilisateurs et permettent l'impression directe depuis le réseau.

Coffrets de câblage (Rack) : Les coffrets de câblage fournissent un espace organisé pour loger les commutateurs, les serveurs, les routeurs, les câbles, et d'autres équipements réseau.

Caméras IP : Les caméras IP sont utilisées pour la vidéosurveillance et la sécurité, et elles peuvent être intégrées dans le réseau.

Batteries de secours (UPS) : Les onduleurs (UPS) fournissent une alimentation de secours pour les équipements réseau en cas de panne de courant, garantissant que le réseau continue de fonctionner.

Équipements de refroidissement : Les dispositifs de refroidissement, comme les ventilateurs et les climatiseurs, assurent la régulation de la température des salles serveurs et des coffrets de câblage.

JOB 3

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

J’ai choisi les câbles croisés pour relier les deux ordinateurs car si nous avons deux ordinateurs connectés directement l'un à l'autre, et que les deux ordinateurs essaient de transmettre sur le câble TX, leurs signaux vont entrer en collision. En outre, rien ne sera envoyé sur le câble RX. Par conséquent, les ordinateurs ne pourront rien recevoir. À ce stade, le câble croisé est nécessaire pour établir des connexions entre deux ordinateurs. Puisque ce genre de câble est croisé, le signal envoyé sur le câble TX depuis l’ordinateur 1 peut être reçu sur le câble RX de l’ordinateur 2. C’est la raison pour laquelle les câbles croisés sont souvent utilisés pour connecter deux mêmes périphériques.

JOB 4

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.

À quoi sert un IP ?

Une adresse IP est un numéro d'identification attribué à un ordinateur connecté à un réseau Internet. Concrètement, ce matricule sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet

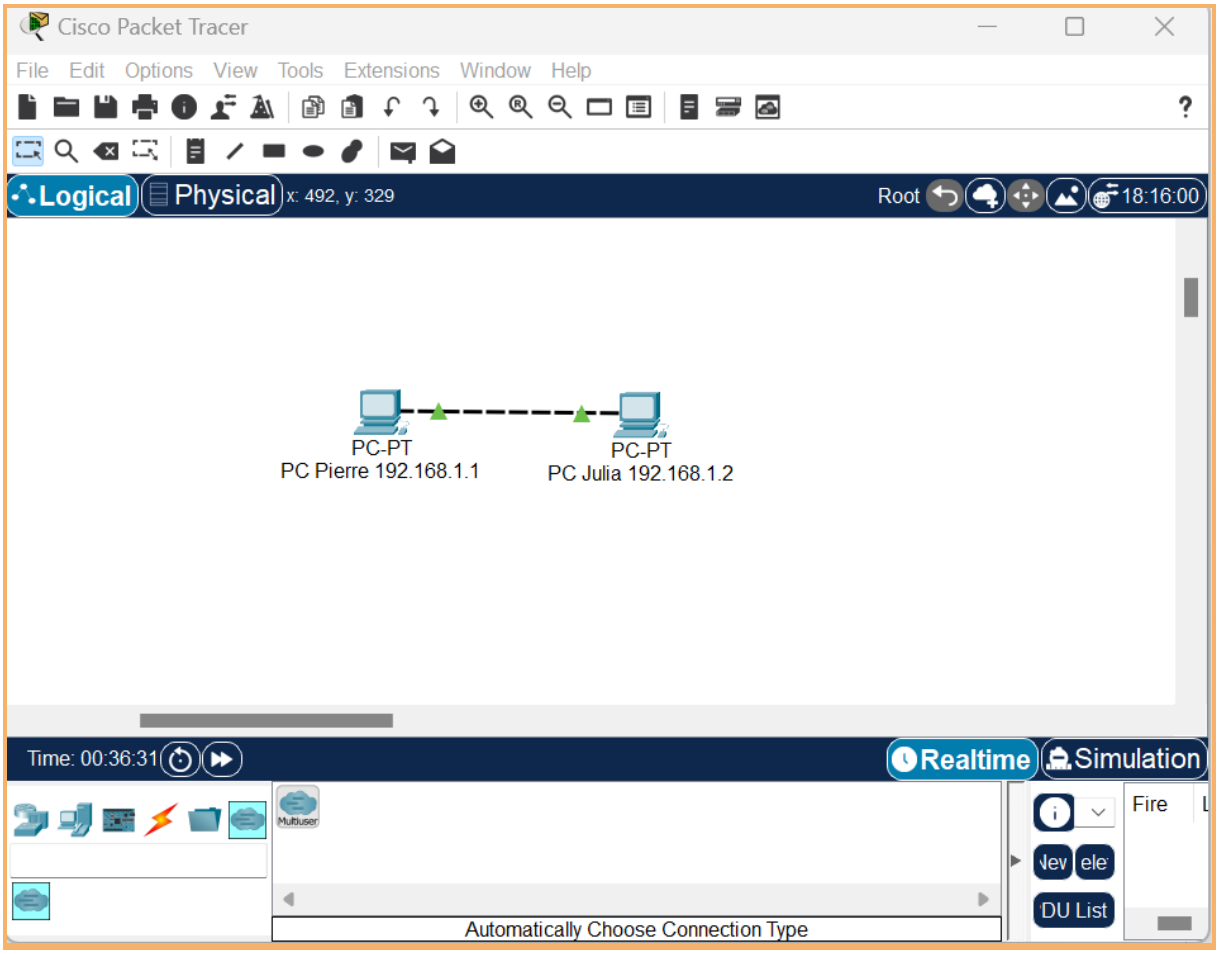
Qu’est-ce qu'une adresse MAC ?

MAC signifie "*Media Access Control*" et cette adresse correspond à l'adresse physique d'un équipement réseau. Cette adresse est un identifiant, normalement unique, permettant d'identifier un équipement réseau par rapport à un autre.

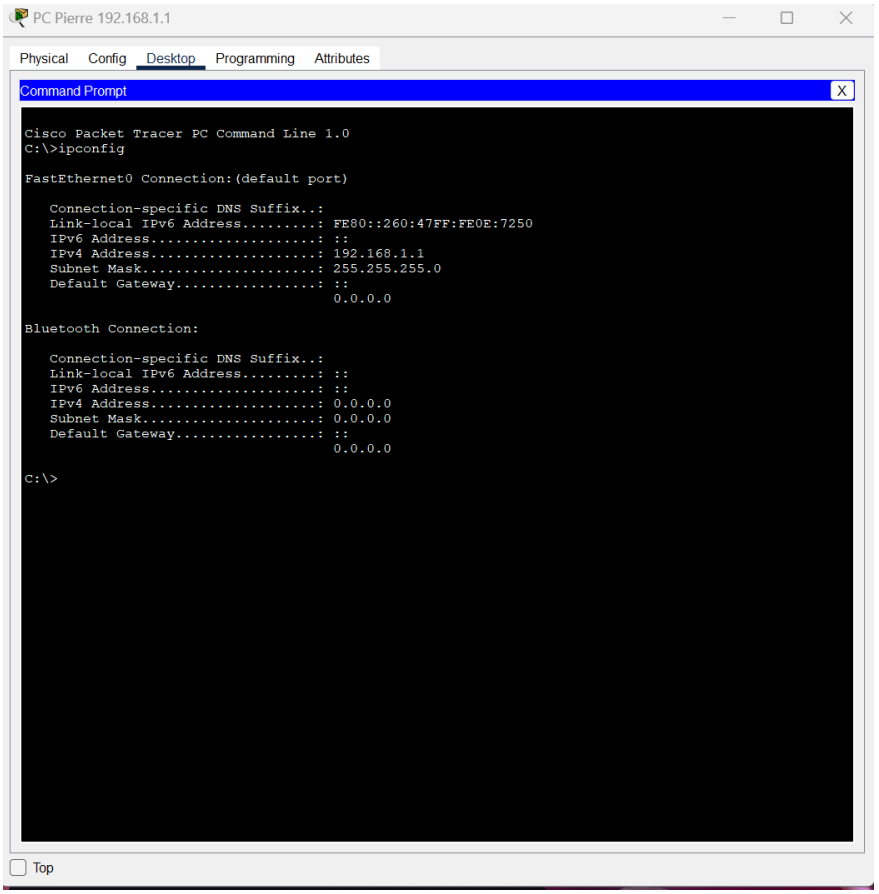
Qu’est-ce qu’une IP publique et privée ?

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.

Quelle est l’adresse de ce réseau ?



JOB 5



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

J'ai utilisé la commande ipconfig

JOB 6

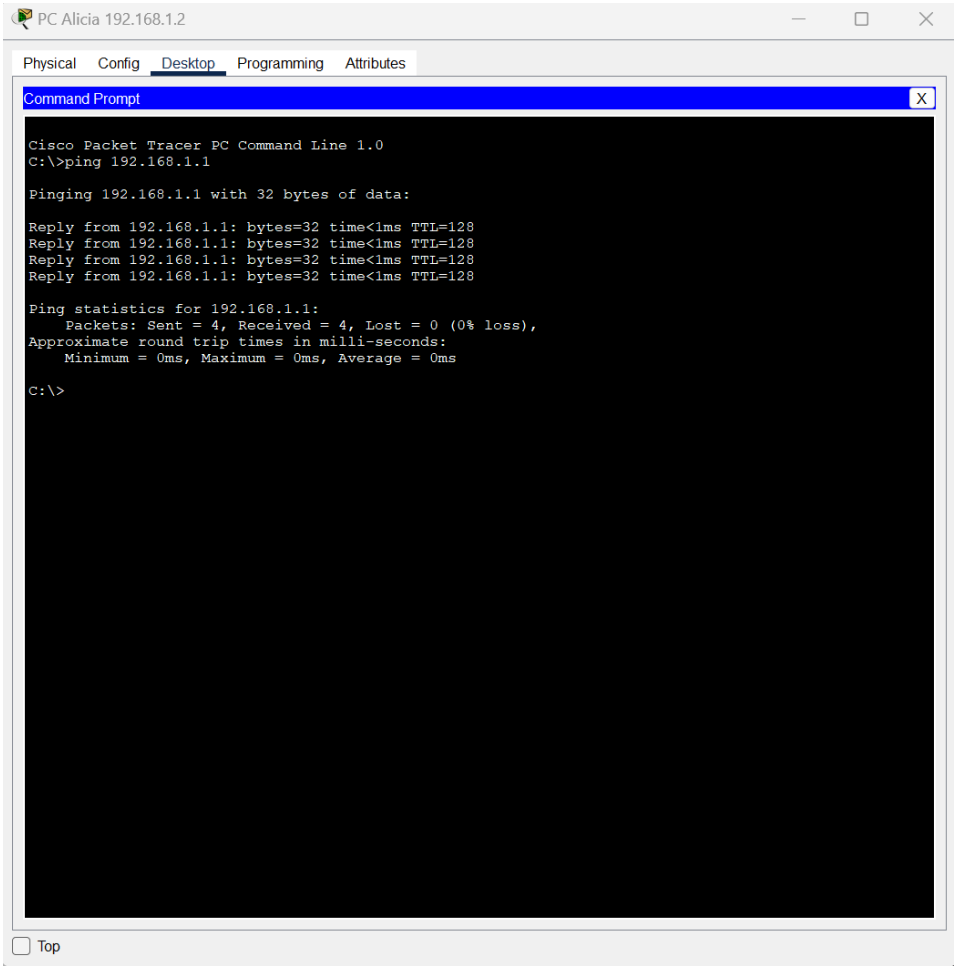
Quelle est la commande permettant de Ping entre des PC ?

La commande permettant le Ping entre les PC est
ping [adresse IP ou nom d'hôte]

JOB 7

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

Oui on peut le lire sur la ligne (Packets: Sent = 4 Received = 4 Lost = 0)



JOB 8

Quelle est la différence entre un hub et un switch ?

Un hub et un switch sont deux dispositifs couramment utilisés pour connecter plusieurs périphériques au sein d'un réseau local (LAN)
Un hub fonctionne au niveau de la couche physique du modèle OSI tandis que le switch fonctionne au niveau de la couche de liaison de données du modèle OSI.

Les switches sont généralement préférés aux hubs dans les réseaux modernes en raison de leurs performances supérieures, de leur efficacité de bande passante, de leur sécurité et de leur capacité à réduire le trafic inutile. Les hubs sont largement obsolètes et sont rarement utilisés dans les environnements réseau actuels.

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

Lorsque des données sont envoyées à un port, elles sont répliquées sur tous les autres ports, quel que soit le destinataire. Cela peut entraîner une utilisation inefficace de la bande passante.Les hubs sont moins performants car ils ne filtrent pas le trafic. Tous les appareils connectés au hub voient le trafic de tous les autres

appareils, ce qui peut entraîner des collisions de données et des goulots d'étranglement sur le réseau.

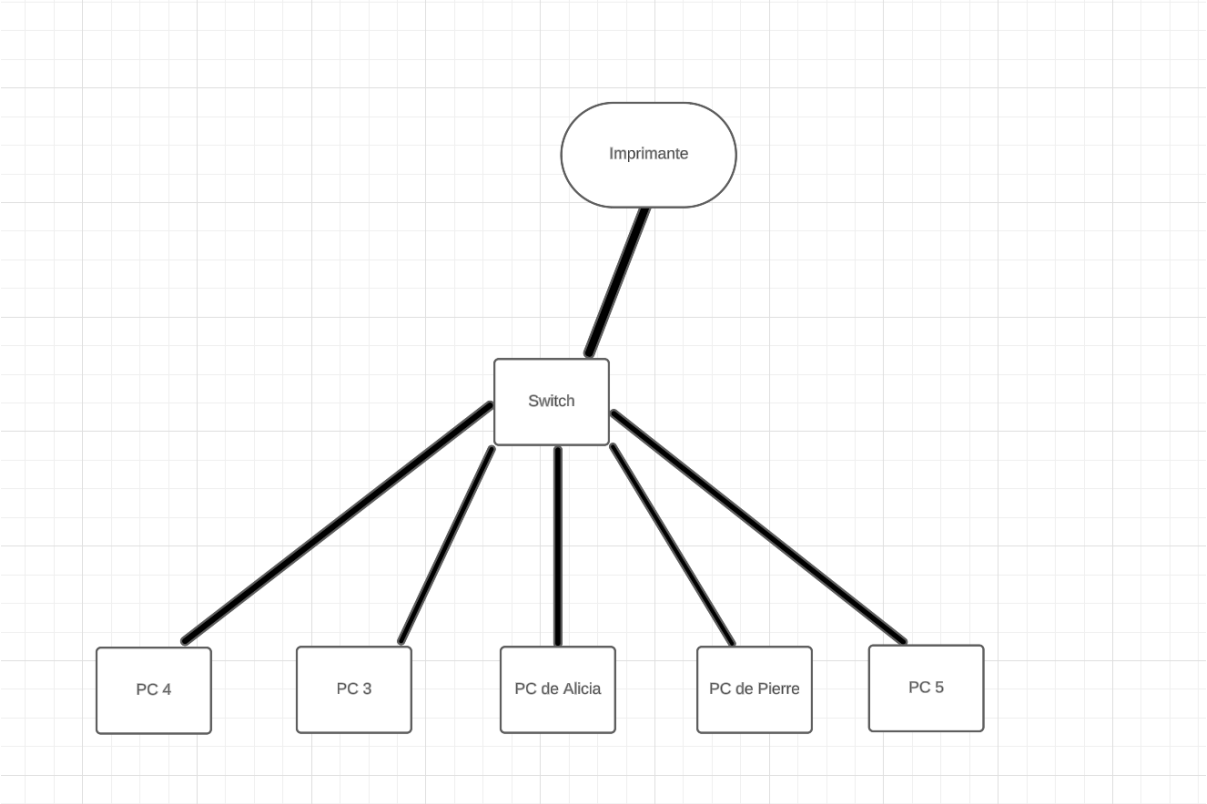
Quels sont les avantages et inconvénients d’un switch ?

Les switches sont plus performants car ils filtrent le trafic. Ils n'envoient que le trafic au port qui nécessite la donnée, réduisant ainsi le risque de collisions et optimisant la bande passante de plus , les switches offrent une meilleure sécurité car ils isolent le trafic entre les ports. Les appareils ne voient que le trafic qui leur est destiné.

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

Un switch fonctionne au niveau de la couche de liaison de données du modèle OSI. Il analyse l'adresse MAC (Media Access Control) des trames entrantes et ne transmet que la trame au port de destination. Cela réduit le trafic inutile et augmente l'efficacité du réseau.

JOB 9



Schématiser vos processus vous permettra d'obtenir une vue d'ensemble sur les étapes, les décisions à prendre au sein d'un paramètre donné et les relations entre les différentes étapes. Vous pourrez alors mieux les comprendre et les améliorer.

JOB 10

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

La principale différence entre les adresses IP statiques et les adresses IP attribuées par DHCP réside dans le mode d'attribution. Les adresses IP statiques sont configurées manuellement et ne changent pas, tandis que les adresses IP attribuées par DHCP sont attribuées automatiquement et peuvent changer. Le choix entre ces deux méthodes dépend des besoins spécifiques d'un réseau et de la complexité de sa gestion. Les adresses IP statiques sont souvent préférées pour les serveurs et les périphériques critiques, tandis que DHCP est plus courant pour les appareils clients.

JOB 11

1 sous-réseau de 12 hôtes : /28 (16 adresses, 14 utilisables)

- Plage d'adresses : 10.0.1.0/28
- Hôtes : 10.0.1.1 à 10.0.1.14
- Adresse réseau : 10.0.1.0
- Adresse de diffusion : 10.0.1.15

5 sous-réseaux de 30 hôtes : /27 (32 adresses, 30 utilisables)

- Plage d'adresses 1 : 10.0.2.0/27
- Plage d'adresses 2 : 10.0.2.32/27
- Plage d'adresses 3 : 10.0.2.64/27
- Plage d'adresses 4 : 10.0.2.96/27
- Plage d'adresses 5 : 10.0.2.128/27
- Hôtes (chaque sous-réseau) : 10.0.2.1 à 10.0.2.30, 10.0.2.33 à 10.0.2.62, etc.

5 sous-réseaux de 120 hôtes : /25(128 adresses, 126 utilisables)

- Plage d'adresses 1 : 10.0.3.0/25
- Plage d'adresses 2 : 10.0.3.128/25
- Plage d'adresses 3 : 10.0.4.0/25
- Plage d'adresses 4 : 10.0.4.128/25
- Plage d'adresses 5 : 10.0.5.0/25

- Hôtes (chaque sous-réseau) : 10.0.3.1 à 10.0.3.126, 10.0.3.129 à 10.0.3.254, etc.

  5 sous-réseaux de 160 hôtes : /26 (64 adresses , 62 utilisables)

- Plage d'adresses 1 : 10.0.6.0/26
- Plage d'adresses 2 : 10.0.6.64/26
- Plage d'adresses 3 : 10.0.6.128/26
- Plage d'adresses 4 : 10.0.6.192/26
- Plage d'adresses 5 : 10.0.7.0/26
- Hôtes (chaque sous-réseau) : 10.0.6.1 à 10.0.6.62, 10.0.6.65 à 10.0.6.126, etc.

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

L'adresse IP 10.0.0.0 fait partie de la plage d'adresses réservée pour les réseaux privés, et elle est généralement utilisée pour les réseaux locaux privés (LAN). Cela signifie que les adresses IP de cette plage ne sont pas routées sur Internet public, ce qui les rend appropriées pour un usage interne dans les réseaux d'entreprise, les réseaux domestiques, ou d'autres réseaux isolés.

Quelle est la différence entre les différents types d’adresses ?

Adresse de diffusion : Utilisée pour envoyer des données à tous les appareils d'un réseau. Par exemple, dans IPv4, l'adresse de diffusion pour le réseau 192.168.1.0/24 est 192.168.1.255.

Adresse de réseau : Identifie le réseau lui-même et est souvent utilisée comme première adresse IP d'un sous-réseau.

JOB 12

Modèle OSI

Différentes Couches	
Couche Physique (Physical LAyer)	fibre optique , Wi-Fi , routeur
Couche de liaison de données (Data Link Layer)	Ethernet , MAC , RJ45
Couche réseau (Network Layer)	PPTP , Ipv4 , Ipv6 , HTML
Couche transport (Transport Layer)	TCP
Couche session (Session Layer)	(Tcp) SSL/TLS
Couche présentation (Presentation Layer)	routeur
Couche application (Application Layer)	FTP

JOB 13

Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est basée sur un réseau local (LAN) composé de quatre ordinateurs (PC0, PC1, PC2, PC3) et deux serveurs (Serveur 1 et Serveur 2). Tous les appareils partagent la même plage d'adresses IP, ce qui suggère qu'ils sont tous sur le même sous-réseau.

Indiquer quelle est l'adresse IP du réseau ?

Adresse IP du réseau : 192.168.10.0

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

Le nombre d'hôtes que vous pouvez brancher sur ce réseau peut être calculé en fonction du nombre de bits disponibles pour les hôtes dans le masque sous-réseau. Dans ce cas , il y a 8 bits disponibles pour les hôtes, ce qui donne 2 x 8 = 256 combinaisons possibles. Cependant, deux adresses sont réservées : l'adresse

réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255). Par conséquent, le nombre total de machines que l'on peut brancher sur ce réseau est de 256 - 2 = 254.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion de ce réseau est 192.168.10.255. Elle est utilisée pour envoyer des paquets à toutes les machines du réseau simultanément.

JOB 14

145.32.59.24 en binaire : 10010001.00100000.00111011.00011000

200.42.129.16 en binaire : 11001000.00101010.10000001.00010000

14.82.19.54 en binaire : 00001110.01010010.00010011.00110110

JOB 15

Qu'est-ce que le routage ?

Le routage est le processus de transmission de données entre différents réseaux informatiques. Il consiste à déterminer le meilleur chemin pour acheminer des données d'un point de départ (source) vers un point d'arrivée (destination) à travers un réseau ou entre plusieurs réseaux. Le routeur, un périphérique réseau spécialisé, joue un rôle clé dans le processus de routage.

Qu'est-ce qu'un gateway ?

Une passerelle (gateway en anglais) est un périphérique ou un logiciel qui relie deux réseaux informatiques différents, leur permettant de communiquer et de transférer des données entre eux. Les passerelles jouent un rôle essentiel dans la connectivité entre des réseaux hétérogènes, qu'il s'agisse de réseaux locaux (LAN), de réseaux étendus (WAN), d'Internet, ou de tout autre type de réseau.

Qu'est-ce qu'un VPN ?

Un VPN, ou Virtual Private Network (Réseau Privé Virtuel en français), est une technologie qui permet de créer un réseau sécurisé et privé, généralement sur Internet, pour permettre la transmission sécurisée de données entre des appareils ou des réseaux distants. Un VPN crée un tunnel crypté qui protège les données en transit, garantissant ainsi la confidentialité, l'intégrité et l'authenticité de la communication.

Qu’est-ce qu’un DNS ?

Le DNS, ou Domain Name System (Système de Noms de Domaines en français), est un système de gestion de noms de domaine qui permet de traduire des noms de domaine conviviaux en adresses IP numériques, facilitant ainsi la navigation sur Internet. En d'autres termes, le DNS joue le rôle d'un "annuaire" pour le Web en associant des noms de domaine (par exemple, www.google.com) à des adresses IP (par exemple, 172.217.3.238) utilisées pour localiser des serveurs et des ressources sur Internet.