JOB 02 :

Qu’est-ce qu’un réseau ?

Un réseau informatique est un ensemble de dispositifs électroniques interconnectés qui permettent le partage de ressources, de données et de services entre des ordinateurs, des serveurs, des périphériques et d'autres composants informatiques. Ces dispositifs sont reliés entre eux par des câbles physiques, des liaisons sans fil ou d'autres technologies de communication.

À quoi sert un réseau informatique ?

Les réseaux informatiques sont essentiels pour permettre la communication et la collaboration entre les appareils et les utilisateurs. Ils peuvent avoir différentes échelles, allant de petits réseaux locaux (LAN) dans un bureau ou une maison, à des réseaux étendus (WAN) qui relient des sites distants à travers de vastes distances géographiques.

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

Pour établir un réseau informatique, il est nécessaire d'avoir les composants matériels de base, notamment une infrastructure physique qui comprend des éléments tels que les cartes réseau (Ethernet, Wi-Fi, fibre optique), les commutateurs (switches), les points d'accès sans fil (Access Point), des routeurs, ainsi que les câbles de connexion.

JOB 03 :

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

J’ai choisi un cable ethernet crossover (copper crossover) car ils sont designé pour connecter deux appareils du même types grâce a leur cablage inversé

JOB 04 :

Qu’est-ce qu’une adresse IP ?

Une adresse IP (Internet Protocol Address) est une étiquette numérique attribuée à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet Protocol pour l'acheminement des données. Les adresses IP sont essentielles pour l'identification et la communication entre les appareils sur un réseau, en particulier sur Internet.

À quoi sert un IP ?

Une adresse IP permet d'identifier de manière distinctive un composant du réseau.

Qu’est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control), également appelée adresse matérielle, est une adresse unique attribuée à chaque carte réseau ou adaptateur réseau (comme une carte Ethernet ou une carte Wi-Fi) présente dans un appareil, tel qu'un ordinateur, un téléphone, une imprimante ou un routeur. Contrairement à l'adresse IP, l'adresse MAC est une valeur physique, généralement inscrite sur la puce de la carte réseau par le fabricant et qui ne change pas, sauf en cas de remplacement de la carte réseau.

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

Une adresse IP publique est délivrée par le fournisseur d'accès à Internet au routeur, qui agit comme une passerelle entre un réseau privé local et Internet. Elle est accessible et identifiable par tous les appareils connectés à Internet.

D'un autre côté, une adresse IP privée est une adresse attribuée à un appareil au sein d'un réseau local, et elle n'est accessible qu'à partir des appareils appartenant à ce réseau local spécifique.

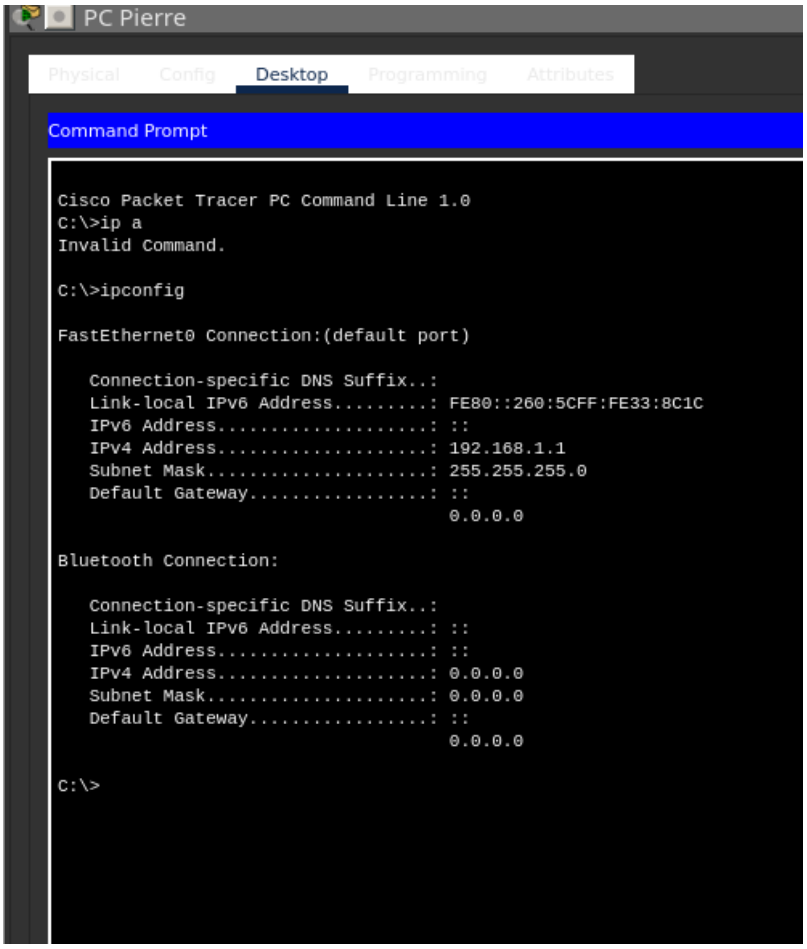
Quelle est l’adresse de ce réseau ?

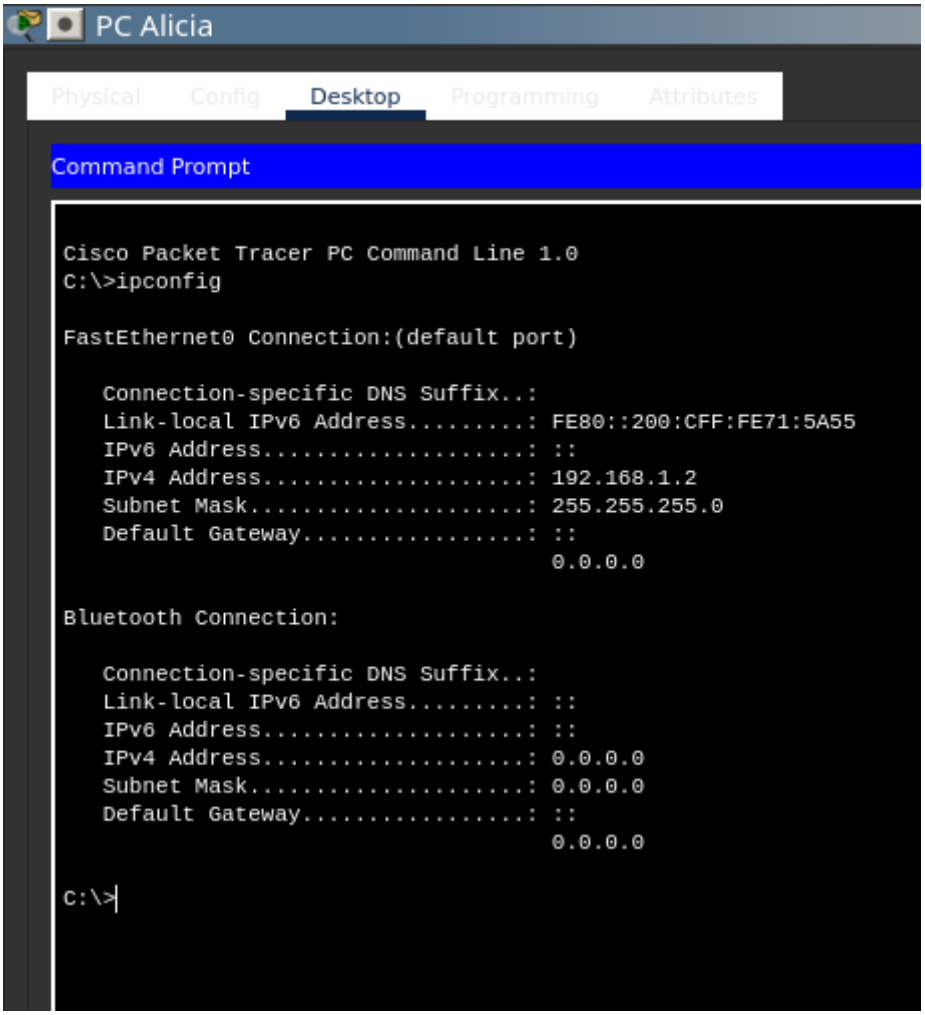
192.168.1.0/24
(je suis pas sûr de la réponse car je ne pense pas avoir bien compris la question)

JOB 05 :

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

La commande *ipconfig* (on peut également ajouter */all* a la fin pour toutes les informations réseau mais pour ce cas ce n’est pas nécéssaire)

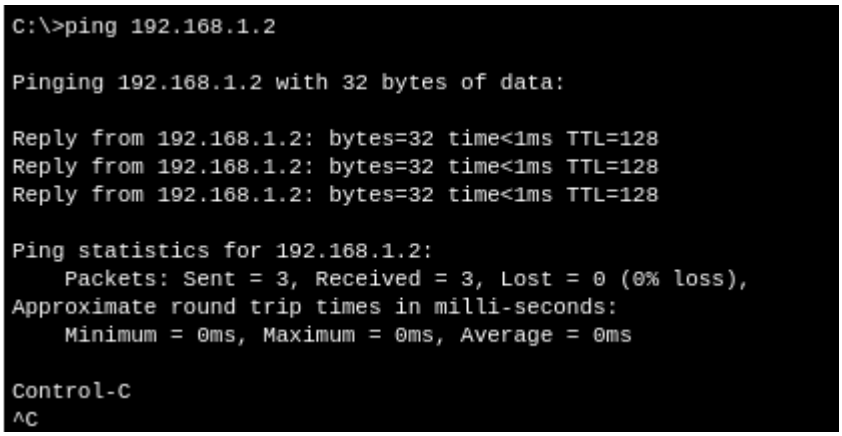

PC Pierre
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ip a
Invalid Command.
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::260:5CFF:FE33:8C1C
IPv6 Address.....: ::
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:\>

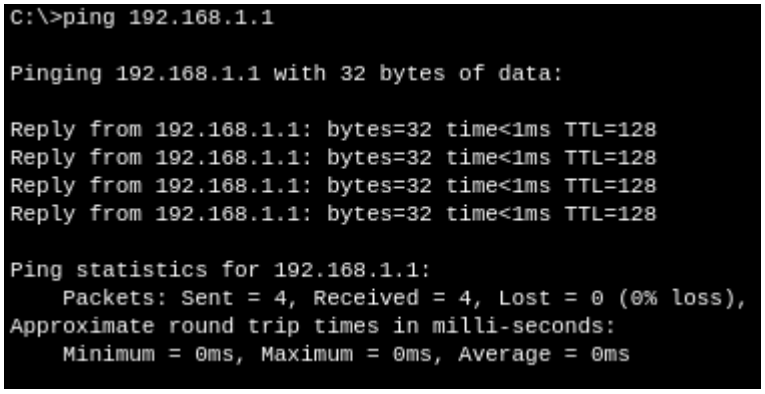

PC Alicia
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Link-local IPv6 Address.....: FE80::200:CFF:FE71:5A55
IPv6 Address.....: ::
IPv4 Address.....: 192.168.1.2
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:\>

Job 06

Quelle est la commande permettant de Ping entre des PC ?

ping [ADDRESSE IP]





JOB 07

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

Non, bien que les paquets ai été envoyés il est nécéssaire que le receveur soit allumé pour qu'il puissent traiter les paquets et y répondre.

JOB 08

Quelle est la différence entre un hub et un switch ?
Comment fonctionne un hub et quels sont ses avantages et ses inconvénients ?
Quels sont les avantages et inconvénients d'un switch ?
Comment un switch gère-t-il le trafic réseau ?

La principale différence entre un hub et un switch réside dans leur manière de gérer le trafic sur un réseau. Un hub fonctionne en diffusant simplement les données reçues à tous les appareils connectés à ses ports, sans tenir compte de la destination des données. Cela signifie que tous les appareils reçoivent l'ensemble du trafic, même si les données ne leur sont pas destinées, ce qui peut entraîner des collisions de données et des inefficacités sur le réseau. En revanche, un switch opère à

un niveau plus élevé en examinant l'adresse MAC de destination dans les trames de données. Il achemine ensuite ces trames uniquement vers le port auquel l'appareil de destination est connecté, réduisant ainsi le trafic inutile et évitant les collisions, ce qui améliore considérablement l'efficacité et les performances du réseau. De plus, le switch offre une certaine isolation entre les appareils, améliorant ainsi la sécurité en limitant la visibilité des données.

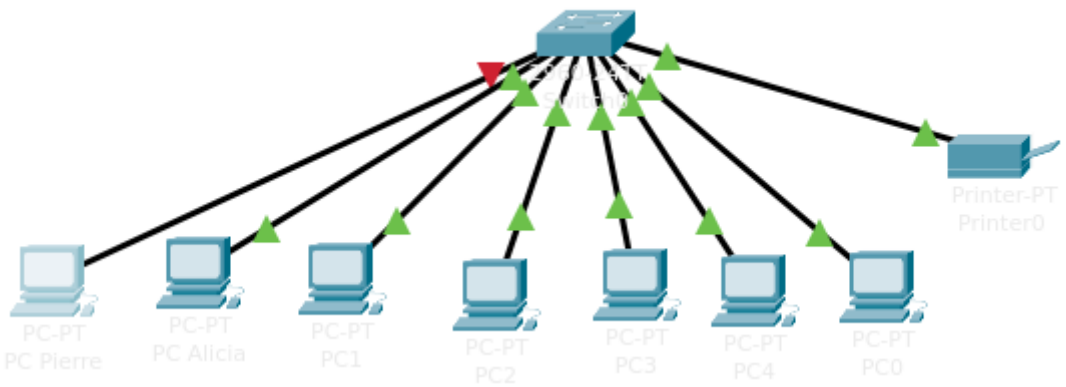
En termes de coût, les hubs sont généralement moins chers, ce qui peut en faire une option économique pour de petites configurations de réseau. Les switches sont plus coûteux, mais leur capacité à offrir des performances supérieures et une gestion de trafic plus efficace les rend adaptés aux réseaux de plus grande envergure et aux environnements où la sécurité et la performance sont essentielles. Ainsi, la différence entre un hub et un switch réside dans leur efficacité, leur sécurité et leur coût, ce qui influence le choix de l'un ou l'autre en fonction des besoins spécifiques du réseau.

JOB 09

Un schéma de réseau informatique, également appelé plan ou diagramme de réseau, offre de nombreux avantages importants pour la gestion, la planification et la compréhension de l'infrastructure réseau. Voici trois avantages majeurs de disposer d'un schéma de réseau :

1. **Clarté et Compréhension** : Un schéma de réseau fournit une vue visuelle de l'ensemble de l'infrastructure, montrant la manière dont les appareils, les routeurs, les commutateurs et les autres composants sont interconnectés. Cela améliore la compréhension du réseau, ce qui est essentiel pour les administrateurs réseau et le dépannage. En identifiant rapidement la configuration du réseau, il est plus facile de diagnostiquer et de résoudre les problèmes.
2. **Planification et Évolutivité** : Un schéma de réseau facilite la planification de la croissance du réseau. En visualisant l'infrastructure actuelle, les administrateurs peuvent déterminer où et comment ajouter de nouveaux appareils ou composants. Cela permet une évolutivité plus efficace du réseau, en évitant les goulets d'étranglement potentiels et les conflits d'adressage.
3. **Sécurité et Gestion** : Un schéma de réseau aide à renforcer la sécurité en identifiant les points d'entrée potentiels pour les menaces. En connaissant l'emplacement des pare-feu, des points d'accès sans fil, des serveurs, etc., les administrateurs peuvent élaborer des stratégies de sécurité plus ciblées. De plus, un schéma de réseau simplifie la gestion en fournissant un aperçu de l'emplacement des ressources, ce qui facilite la gestion des adresses IP, la surveillance du trafic et l'administration globale du réseau.

Le logiciel Packet Tracer étant déjà un outil utilisé pour faire des schémas de réseaux voici la topologie de mon réseau :



JOB 10

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 assignées : une adresse IP statique est configurée manuellement par un administrateur réseau, restant fixe jusqu'à une modification manuelle, tandis qu'une adresse IP attribuée par DHCP est allouée automatiquement par un serveur DHCP à l'appareil lors de sa connexion au réseau, offrant une flexibilité d'attribution dynamique. Les adresses statiques sont utilisées pour des appareils nécessitant des adresses permanentes, comme les serveurs, tandis que le DHCP est couramment employé pour les appareils temporaires ou sur des réseaux de grande envergure, simplifiant la gestion des adresses.

JOB 11

Nombres d'hôtes	Masque de réseau	IP réseau	IP DHCP	IP disponibles	IP diffusion
12	255.255.255.240/28	10.0.0.0	10.0.0.1	10.0.0.2 a 10.0.0.13	10.0.0.14
30	255.255.255.192/26	10.0.1.0	10.0.1.1	10.0.1.2 a 10.0.1.31	10.0.1.32
30	255.255.255.192/26	10.0.2.0	10.0.2.1	10.0.2.2 a 10.0.2.31	10.0.2.32
30	255.255.255.192/26	10.0.3.0	10.0.3.1	10.0.3.2 a 10.0.2.31	10.0.3.32
30	255.255.255.192/26	10.0.4.0	10.0.4.1	10.0.4.2 a 10.0.4.31	10.0.4.32
30	255.255.255.192/26	10.0.5.0	10.0.5.1	10.0.5.2 a 10.0.5.31	10.0.5.32
120	255.255.255.128/25	10.0.6.0	10.0.6.1	10.0.6.2 a 10.0.6.121	10.0.6.122
120	255.255.255.128/25	10.0.7.0	10.0.7.1	10.0.7.2 a 10.0.7.121	10.0.7.122
120	255.255.255.128/25	10.0.8.0	10.0.8.1	10.0.8.2 a 10.0.8.121	10.0.8.122
120	255.255.255.128/25	10.0.9.0	10.0.9.1	10.0.9.2 a 10.0.9.121	10.0.9.122
120	255.255.255.128/25	10.0.10.0	10.0.10.1	10.0.10.2 a 10.0.10.121	10.0.10.122
160	255.255.255.0/24	10.0.11.0	10.0.11.1	10.0.11.2 a 10.0.11.161	10.0.11.162
160	255.255.255.0/24	10.0.12.0	10.0.12.1	10.0.12.2 a 10.0.12.161	10.0.12.162
160	255.255.255.0/24	10.0.13.0	10.0.13.1	10.0.13.2 a 10.0.13.161	10.0.13.162
160	255.255.255.0/24	10.0.14.0	10.0.14.1	10.0.14.2 a 10.0.14.161	10.0.14.162
160	255.255.255.0/24	10.0.15.0	10.0.15.1	10.0.15.2 a 10.0.15.161	10.0.15.162

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

L'adresse 10.0.0.0 de classe A a été choisie en raison de sa capacité d'adressage élevée, offrant plus de 16 millions d'adresses IP potentielles, ce qui garantit une marge de manœuvre pour l'expansion future du réseau. Elle simplifie également la gestion du réseau en évitant la nécessité de gérer de multiples sous-réseaux, et elle offre une grande flexibilité pour la création de sous-réseaux internes tout en maintenant une adresse de base bien établie. De plus, l'adresse 10.0.0.0 est couramment utilisée et reconnue, ce qui facilite l'interopérabilité avec d'autres réseaux et appareils.

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

Les adresses IP IPv4 sont divisées en cinq classes principales : A, B, C, D et E. Chacune de ces classes diffère par la taille de la portion de l'adresse réservée pour le réseau et pour l'hôte, ce qui a un impact sur le nombre d'adresses disponibles. Voici les principales différences entre ces classes :

1. **Classe A** :
    - Plage d'adresses : 1.0.0.0 à 126.0.0.0
    - Portion réseau : 8 bits (1.0.0.0)
    - Portion hôte : 24 bits (jusqu'à 16 777 214 hôtes)
    - Utilisation : Principalement pour les réseaux très grands, comme les grandes entreprises et les fournisseurs de services Internet.
2. **Classe B** :
    - Plage d'adresses : 128.0.0.0 à 191.255.0.0
    - Portion réseau : 16 bits (128.0.0.0)
    - Portion hôte : 16 bits (jusqu'à 65 534 hôtes)
    - Utilisation : Adaptée aux réseaux de taille moyenne, telles que les universités et les grandes organisations.
3. **Classe C** :
    - Plage d'adresses : 192.0.0.0 à 223.255.255.0
    - Portion réseau : 24 bits (192.0.0.0)
    - Portion hôte : 8 bits (jusqu'à 254 hôtes)
    - Utilisation : Appropriée pour les réseaux de petite à moyenne taille, tels que les réseaux locaux d'entreprise.
4. **Classe D** :
    - Plage d'adresses : 224.0.0.0 à 239.255.255.255
    - Portion réseau : N/A
    - Portion hôte : N/A
    - Utilisation : Réservée aux adresses multicast utilisées pour la diffusion de données à plusieurs destinataires.
5. **Classe E** :
    - Plage d'adresses : 240.0.0.0 à 255.255.255.255
    - Portion réseau : N/A
    - Portion hôte : N/A
    - Utilisation : Réservée à des fins expérimentales et de recherche.

En résumé, les classes d'adresses IP diffèrent par le nombre d'adresses disponibles et par leur utilisation. Les classes A, B et C sont les plus couramment utilisées pour les réseaux, tandis que les classes D et E ont des utilisations spécifiques pour la diffusion de données et des expériences de recherche, respectivement.

JOB 12

Couche OSI	Description des rôles
Couche 7 : Application	Gère l'interaction entre les applications et les services réseau.
Couche 6 : Présentation	S'occupe de la conversion, du chiffrement et de la compression des données.
Couche 5 : Session	Établit, gère et termine les sessions de communication.
Couche 4 : Transport	Assure la fiabilité et le contrôle du flux de données entre les appareils.
Couche 3 : Réseau	Gère la routage des paquets de données à travers le réseau.
Couche 2 : Liaison de données	Gère la communication entre des nœuds locaux, détecte et corrige les erreurs.
Couche 1 : Physique	Gère la transmission des bits bruts sur le support de communication.

Ethernet : Couche 1
MAC : Couche 2
fibre optique : Couche 1
PPTP : Couche 2
IPv4 : Couche 3
SSL/TLS : Couche 6
TCP : Couche 4/5
Wi-Fi : Couche 1
IPv6 : Couche 3
UDP : Couche 4/5
FTP : Couche 6/7
Routeur : Couche 3
HTML : Couche 7
Cable RJ45 : Couche 1

JOB 13

Quelle est l’architecture de ce réseau ?

C’est une topologie en étoile.

Indiquer quelle est l’adresse IP du réseau ?

192.168.10.0/24

Quelle est l'adresse de diffusion de ce réseau?

192.168.10.255

JOB 14

Convertissez les adresses IP suivantes en binaires :
- 145.32.59.24
- 200.42.129.16
- 14.82.19.54

145.32.59.24 deviens 10010001 00100000 00111011 00011000

200.42.129.16 deviens 11001000 00101010 10000001 00010000

14.82.19.54 deviens 00001110 01010010 00010011 00110110

JOB 15

Qu'est-ce que le routage?

Le routage est un processus essentiel dans les réseaux informatiques qui consiste à diriger le trafic de données d'un point à un autre à travers un réseau. Cela se fait en déterminant le chemin optimal pour les données, en tenant compte de divers facteurs tels que la distance, la charge du réseau, la priorité des données et les préférences de l'administrateur du réseau. Le routage permet de garantir que les données atteignent leur destination de manière efficace et fiable, que ce soit à l'intérieur d'un réseau local (LAN) ou sur Internet. Il repose sur des protocoles et des algorithmes spécifiques, comme le protocole IP (Internet Protocol) pour les réseaux IP, qui sont utilisés pour prendre des décisions de routage en fonction des adresses IP des appareils et des routes disponibles.

Dans un environnement informatique, le routage est essentiel pour assurer la connectivité entre les appareils, la transmission des données et le bon fonctionnement des réseaux, qu'il s'agisse de simples réseaux locaux domestiques ou de vastes réseaux mondiaux comme Internet. En résumé, le routage consiste à déterminer le chemin optimal pour les données à travers un réseau, ce qui permet de garantir une communication fluide et efficace entre les appareils connectés.

Qu’est-ce qu’un gateway ?

Une passerelle (gateway en anglais) est un dispositif matériel ou logiciel utilisé dans les réseaux informatiques pour connecter deux réseaux distincts et permettre la communication entre eux. Les passerelles agissent comme des points d'entrée et de sortie qui traduisent les données entre différents protocoles, normes ou topologies de réseau. Elles jouent un rôle crucial en permettant aux réseaux hétérogènes de coopérer en relayant des paquets de données d'un réseau à un autre. Par exemple, une passerelle peut permettre la communication entre un réseau local (LAN) basé sur Ethernet et Internet en traduisant les données de manière à ce qu'elles puissent être comprises et transmises efficacement entre ces deux environnements distincts.

Qu’est-ce qu’un VPN ?

Un VPN, ou Réseau Privé Virtuel, est un service ou une technologie qui permet de créer un tunnel sécurisé et chiffré entre un appareil (comme un ordinateur, un smartphone) et un serveur distant. Son principal objectif est de garantir la confidentialité, la sécurité et l'anonymat des données

lorsqu'elles transitent sur Internet. Les VPN sont couramment utilisés pour protéger la vie privée en ligne, contourner la censure, accéder à des contenus géo-restreints et sécuriser les connexions sur des réseaux Wi-Fi publics non sécurisés. Lorsque vous vous connectez à un VPN, tout le trafic Internet entre votre appareil et le serveur distant est crypté, masquant ainsi votre adresse IP et rendant plus difficile pour les tiers de surveiller ou d'intercepter vos activités en ligne.

Qu’est-ce qu’un DNS ?

Un DNS, ou Système de Noms de Domaine, est un composant essentiel de l'infrastructure d'Internet qui sert à traduire les noms de domaine, tels que www.example.com, en adresses IP numériques compréhensibles par les ordinateurs. Il agit comme un annuaire qui permet aux utilisateurs d'accéder aux sites Web et aux services en ligne en utilisant des noms faciles à retenir au lieu de se souvenir des longues séquences de chiffres qui constituent les adresses IP. Lorsque vous saisissez une URL dans votre navigateur, le DNS localise l'adresse IP correspondante associée au nom de domaine spécifié, ce qui permet d'acheminer efficacement le trafic Internet vers la destination souhaitée. En résumé, le DNS est un élément fondamental de l'architecture d'Internet qui simplifie la façon dont les utilisateurs accèdent aux ressources en ligne en traduisant les noms de domaine en adresses IP.