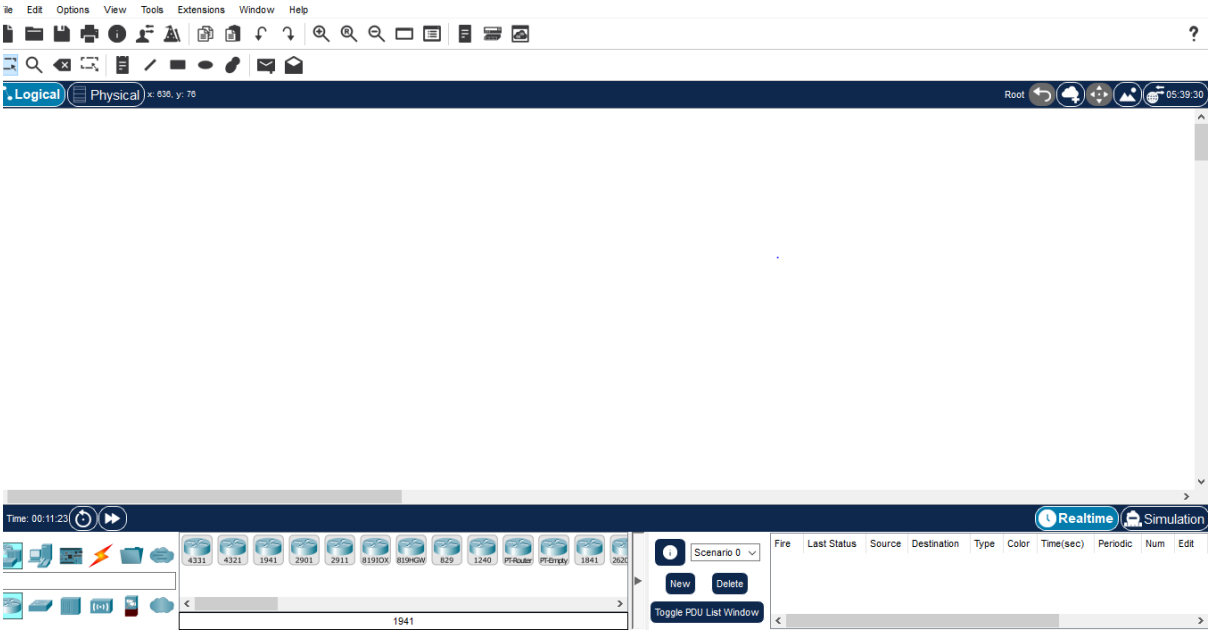
RunTrack réseau

job 1



job 2

- **Qu'est-ce qu'un réseau ?**

Un réseau est un ensemble de dispositifs interconnectés qui communiquent entre eux pour partager des informations, des ressources et des services. Ces dispositifs peuvent être des ordinateurs, des serveurs, des routeurs, des commutateurs, des smartphones, des tablettes, des objets connectés, et bien d'autres.

- **À quoi sert un réseau informatique ?**

Un réseau informatique sert à connecter et à interconnecter des ordinateurs et d'autres dispositifs pour permettre la communication, le partage de ressources et la distribution d'informations. Les réseaux informatiques sont essentiels dans le monde moderne pour de nombreuses raisons, notamment :**Communication,Partage de ressources ,Accès à Internet,etc**

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

  Pour construire un réseau informatique, vous aurez besoin de divers composants matériels qui remplissent des fonctions spécifiques pour permettre la connectivité, la communication et le partage de ressources. Voici une liste des principaux composants et leurs fonctions :

  Ordinateurs et Dispositifs Clients : Les ordinateurs et autres dispositifs, tels que des smartphones et des tablettes, sont les utilisateurs finaux du réseau. Ils accèdent aux ressources partagées, communiquent entre eux et utilisent les services du réseau.

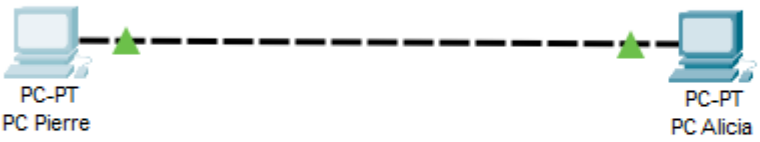
Serveurs : Les serveurs sont des ordinateurs spécialement configurés pour offrir des services, comme le stockage de fichiers, les sites web, les applications, la messagerie électronique, etc. Ils répondent aux demandes des clients sur le réseau.
Routeurs : Les routeurs dirigent le trafic entre différentes parties du réseau. Ils décident la meilleure route pour les données en fonction des adresses IP et d'autres facteurs. Les routeurs interconnectent des réseaux locaux (LAN) et des réseaux étendus (WAN).

Commutateurs (Switches) : Les commutateurs connectent les dispositifs dans un réseau local (LAN). Ils prennent en charge la commutation de paquets au niveau de la couche de liaison (couche 2) et sont utilisés pour créer un réseau local fiable et efficace.

Point d'accès sans fil (Access Point - AP) : Les points d'accès sans fil permettent la connexion sans fil des dispositifs au réseau. Ils fournissent un réseau Wi-Fi pour que les ordinateurs portables, les smartphones et d'autres dispositifs se connectent.

Câbles et Connexions : Les câbles Ethernet, les câbles à fibre optique, et d'autres types de câbles sont utilisés pour connecter physiquement les dispositifs au réseau. Les câbles doivent être correctement installés et entretenus pour garantir un bon fonctionnement du réseau. etc

job 3



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

j’ai choisi le cable automatically choose connection type parce qu’il relie directement le connexion des deux PC.

job 4

- **Qu’est-ce qu’une adresse IP ?**

Une adresse IP, ou adresse de protocole Internet, est un identifiant unique attribué à chaque dispositif connecté à un réseau informatique qui utilise le protocole Internet pour la communication.

- **À quoi sert un IP ?**
  Un "IP" peut se référer à deux choses différentes en informatique : une "adresse IP" ou "Intellectual Property" (propriété intellectuelle). Voici ce que signifie chacun de ces termes :

Adresse IP (Internet Protocol) : Une adresse IP (Internet Protocol) est un identifiant unique attribué à chaque dispositif connecté à un réseau informatique qui utilise le protocole Internet. Les adresses IP sont essentielles pour l'acheminement des données sur Internet et au sein de réseaux locaux (LAN) et étendus (WAN). Elles servent à identifier de manière univoque chaque dispositif sur un réseau, ce qui permet le routage des données vers la destination appropriée. Les adresses IP sont utilisées pour diverses applications, telles que la navigation sur le Web, l'envoi de courrier électronique, le partage de fichiers et la communication sur Internet.

Intellectual Property (Propriété Intellectuelle) : L'acronyme "IP" peut également faire référence à la "propriété intellectuelle", qui englobe les droits légaux accordés aux créateurs et propriétaires d'œuvres intellectuelles, telles que les brevets, les droits d'auteur, les marques commerciales et les secrets commerciaux. La propriété intellectuelle protège les idées, les inventions, les créations artistiques, les marques et d'autres formes de propriété immatérielle. Les lois sur la propriété intellectuelle visent à protéger les droits des créateurs et à encourager l'innovation et la création.

- **Qu’est-ce qu'une adresse MAC ?**

Une adresse MAC, ou adresse de contrôle d'accès au support, est un identifiant unique attribué à chaque carte réseau et adaptateur réseau connecté à un réseau informatique.
Qu’est-ce qu’une IP publique et privée ?

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

Une adresse IP publique et une adresse IP privée sont deux types d'adresses IP utilisés dans les réseaux informatiques, et elles jouent des rôles différents en fonction de la portée et de la visibilité du réseau.

Adresse IP Publique : Une adresse IP publique est une adresse unique et globalement routable attribuée à un dispositif ou à un réseau qui est directement accessible depuis Internet. Les adresses IP publiques sont utilisées pour identifier des dispositifs sur Internet, permettre la communication entre eux et accéder à des services en ligne, tels que des sites web ou des serveurs de messagerie.

Adresse IP Privée : Une adresse IP privée est une adresse utilisée au sein d'un réseau local (LAN) pour identifier des dispositifs au sein de ce réseau, mais qui n'est pas routable sur Internet. Les adresses IP privées sont réservées pour une utilisation dans des réseaux privés, tels que les réseaux locaux domestiques ou d'entreprise. Elles permettent aux dispositifs au sein du réseau local de communiquer entre eux, mais elles ne sont pas directement accessibles depuis Internet.

- **Quelle est l’adresse de ce réseau ?**

l'adresse de ce réseau est :

```
Adresse IP de la passerelle :  192.168.1.1

Masque de sous-réseau       :  255.255.255.0

-------------------------------------

Adresse de réseau           :  192.168.1.0
```

Donc, dans cet exemple, l'adresse de réseau serait "192.168.1.0".

job 5

vérification des IP

Pierre:

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::207:ECFF:FEA9:5B9C
   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
```

Alicia:

```
C:\>
ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20A:41FF:FE08:C753
   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
```

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

  on a utilisé le ligne de commande(ping l'adresse IP) pour vérifier si les IP des machines sont correctes.

job 6

vérification de connectivité

Pierre:

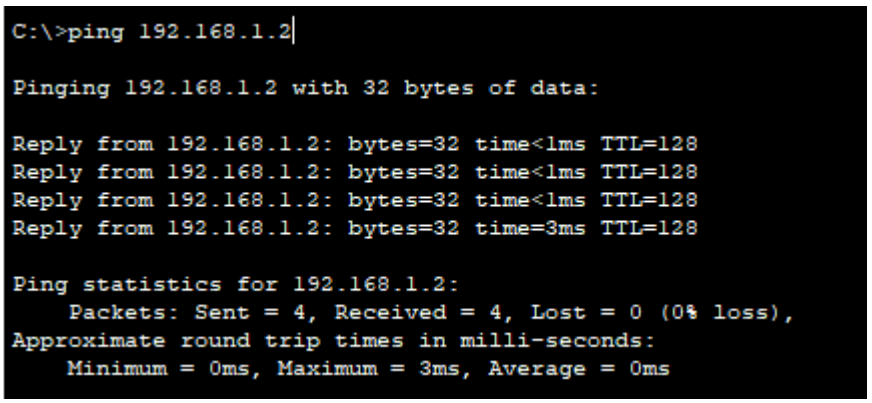
```
C:\>ping 192.168.1.1

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=22ms TTL=128
Reply from 192.168.1.1: bytes=32 time=19ms TTL=128
Reply from 192.168.1.1: bytes=32 time=24ms 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 = 24ms, Average = 16ms
```

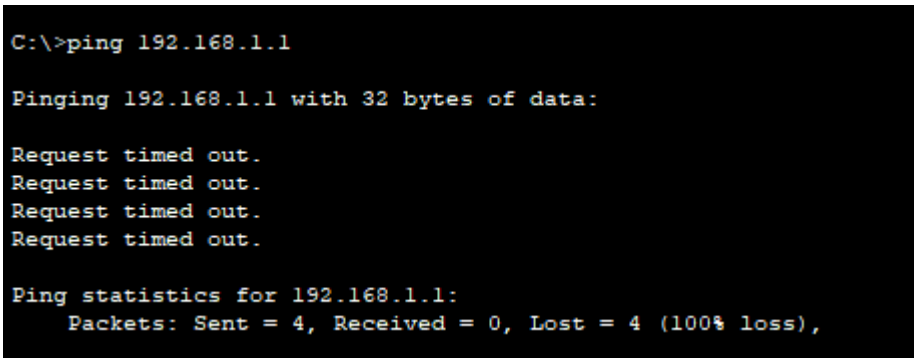
Alicia:



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

  la commande qui permet de ping entre des 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.**

  Non ,le PC de pierre ne reçoit pas les paquets envoyés par Alicia car le PC de Pierre est éteint.

job 8

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

  Un hub (concentrateur) et un switch sont deux types de dispositifs utilisés dans les réseaux informatiques pour connecter plusieurs appareils entre eux. Cependant, ils fonctionnent de manière très différente et ont des caractéristiques distinctes. Voici les principales différences entre un hub et un switch :

Hub : Un hub est un dispositif réseau de couche 1 (physique) qui agit simplement en tant que répéteur passif. Il reçoit des données sur un port et les transmet à tous les autres ports, sans intelligence pour déterminer où envoyer les données.

Switch : Un switch est un dispositif de couche 2 (liaison de données) ou de couche 3 (réseau) qui examine l'adresse MAC (Media Access Control) des paquets et prend des décisions intelligentes pour acheminer les données uniquement vers le port de destination approprié. Il crée une table de correspondance entre les adresses MAC des appareils connectés.

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

  Un hub fonctionne en répétant simplement les données qu'il reçoit sur un port à tous les autres ports. Lorsqu'il reçoit un paquet de données sur un port, il le transmet à tous les autres ports, indépendamment de la destination réelle des données. Il n'a aucune intelligence pour déterminer où envoyer les données en fonction de l'adresse MAC (Media Access Control) des appareils connectés. Il agit essentiellement comme un amplificateur, renvoyant les signaux à tous les périphériques connectés.

Avantages d'un hub :

1. **Coût :** Les hubs sont généralement moins chers que les commutateurs (switches) et peuvent être une option économique pour connecter plusieurs appareils sur un petit réseau.
2. **Simplicité :** Les hubs sont simples à utiliser et à configurer. Il n'y a généralement pas besoin de configuration complexe…

Inconvénients d'un hub :

1. **Efficacité :** L'un des principaux inconvénients d'un hub est qu'il transmet les données à tous les ports, même si seuls un ou quelques appareils ont réellement besoin des données. Cela peut entraîner une congestion du réseau et une utilisation inefficace de la bande passante.
2. **Sécurité :** Les données transmises via un hub sont visibles par tous les appareils connectés au hub. Il n'offre aucune isolation ou sécurité des données, ce qui pose des risques en matière de sécurité et de confidentialité…

- **Quels sont les avantages et inconvénients d'une switch ?**

Avantages d'un switch :

1. **Efficacité :** Les switches acheminent sélectivement les données uniquement vers le port de destination approprié, ce qui optimise l'utilisation de la bande passante et réduit la congestion du réseau.
2. **Sécurité :** Les données sont isolées, ce qui signifie que seuls les appareils concernés reçoivent les données. Cela renforce la sécurité en limitant la visibilité des données.

3. **Latence réduite :** Les switches offrent des temps de latence plus bas par rapport aux hubs, car ils acheminent directement les données vers le port de destination, minimisant ainsi les retards…

Inconvénients d'un switch :

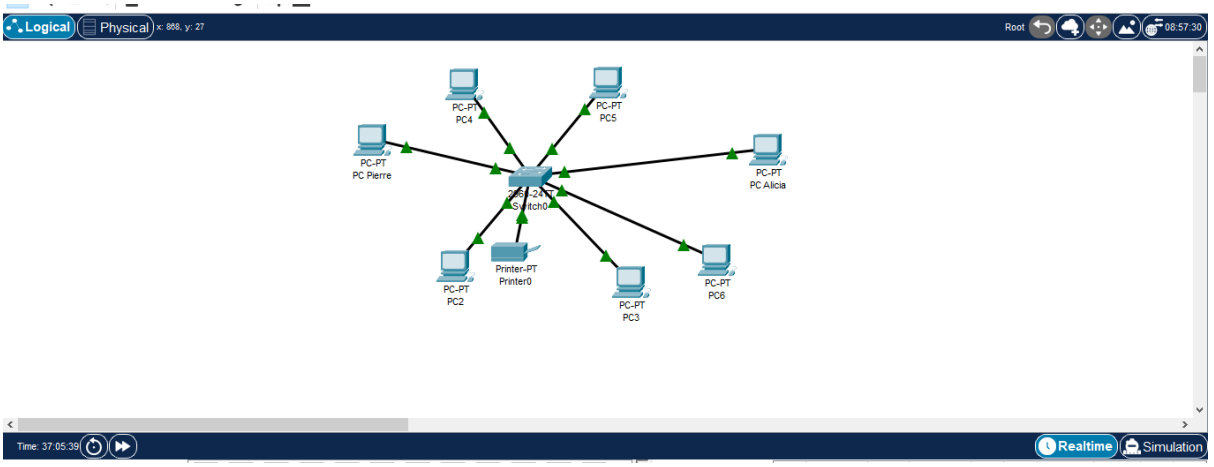
1. **Coût :** Les switches sont généralement plus coûteux que les hubs en raison de leurs fonctionnalités avancées, ce qui peut représenter un investissement plus important.
2. **Complexité :** Les switches sont plus complexes à configurer et à gérer que les hubs. Ils peuvent nécessiter une expertise technique pour une configuration optimale.
3. **Taille :** Les switches physiques sont généralement plus volumineux que les hubs ou les dispositifs de réseau plus simples…
    - **Comment un switch gère-t-il le trafic réseau** ?

Un switch gère le trafic réseau en utilisant des adresses MAC (Media Access Control) pour acheminer sélectivement les données vers les ports appropriés. Voici comment un switch gère le trafic réseau de manière plus détaillée :

1. **Apprentissage des adresses MAC :** Lorsqu'un périphérique est connecté à un switch, le switch "apprend" l'adresse MAC de ce périphérique. Il stocke ces informations dans une table de correspondance des adresses MAC. Cette table est également appelée "table CAM" (Content Addressable Memory).
2. **Filtrage et acheminement :** Lorsqu'un périphérique connecté à un switch envoie un paquet de données, le switch examine l'adresse MAC de destination du paquet. Il consulte sa table CAM pour déterminer sur quel port se trouve l'appareil correspondant à cette adresse MAC. Le switch achemine ensuite le paquet uniquement vers le port où se trouve l'appareil de destination, réduisant ainsi la congestion du réseau.
3. **Diffusion (Broadcast) :** Lorsqu'un paquet de diffusion (broadcast) est envoyé, le switch le transmet à tous les ports, car il est destiné à être reçu par tous les appareils sur le réseau. Cependant, le switch maintient une liste des adresses MAC déjà apprises, de sorte que les paquets de diffusion ne sont pas renvoyés sur le port d'origine…

job 9

Réalisez un schéma de votre réseau.



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

Avoir un schéma de réseau présente plusieurs avantages importants pour la gestion et la maintenance de votre infrastructure informatique. Voici trois des avantages les plus importants :

1. **Clarté et compréhension du réseau :** Un schéma de réseau permet une visualisation claire de la structure de votre réseau, y compris la disposition physique des composants, les connexions entre les appareils, et les flux de données.
2. **Dépannage plus efficace :** Lorsque des problèmes surviennent sur le réseau, un schéma bien documenté peut être un outil précieux pour le dépannage. Il permet aux administrateurs de suivre les connexions, de localiser les points de défaillance éventuels et d'isoler rapidement les problèmes.
3. **Planification et expansion du réseau :** Un schéma de réseau est essentiel pour la planification de la croissance et de l'évolution du réseau. Il permet d'identifier les domaines où des améliorations sont nécessaires, que ce soit en termes de capacité, de sécurité ou de performance. Il facilite également la mise en place de nouvelles connexions ou de nouveaux appareils, en indiquant où et comment ils peuvent être intégrés dans l'infrastructure existante.

JOB 10

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

Une adresse IP statique et une adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) sont deux méthodes de configuration des adresses IP sur un périphérique réseau. Voici les principales différences entre les deux :

1. **Adresse IP Statique :**
   - Une adresse IP statique est configurée manuellement par un administrateur réseau ou l'utilisateur sur un périphérique.

- L'adresse IP statique reste inchangée, sauf si elle est modifiée manuellement par l'administrateur.
- Elle est généralement utilisée pour des périphériques qui doivent avoir une adresse IP constante, comme un serveur ou un routeur, afin que d'autres appareils puissent toujours les atteindre à la même adresse.
- L'administrateur doit s'assurer qu'il n'y a pas de conflits d'adresses IP sur le réseau.

2. **Adresse IP attribuée par DHCP :**
   - Une adresse IP attribuée par DHCP est obtenue automatiquement à partir d'un serveur DHCP sur le réseau.
   - Le serveur DHCP attribue dynamiquement une adresse IP à un périphérique lorsque celui-ci se connecte au réseau.
   - L'adresse IP peut changer à chaque nouvelle connexion, en fonction de la configuration du serveur DHCP.
   - Elle est couramment utilisée pour les appareils clients, tels que les ordinateurs, les téléphones, et d'autres périphériques, car elle simplifie la gestion des adresses IP en évitant les conflits d'adresses.

     En résumé, la principale différence réside dans la manière dont l'adresse IP est attribuée. Une adresse IP statique est configurée manuellement et reste la même, tandis qu'une adresse IP attribuée par DHCP est obtenue automatiquement et peut changer à chaque connexion.

job 11

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

Lorsque vous avez mentionné l'adresse réseau 10.0.0.0, cela a été interprété comme une adresse IP de classe A. Cependant, il est important de noter que le concept de "classes" d'adresses IP a été obsolète depuis la mise en place de la notation CIDR (Classless Inter-Domain Routing). Les adresses IP sont maintenant généralement classées en fonction de la longueur de leur masque de sous-réseau plutôt que de leur classe d'origine.

Cela signifie que vous pouvez utiliser une adresse IP de classe A (comme 10.0.0.0) et la diviser en sous-réseaux plus petits en utilisant la notation CIDR en fonction de vos besoins. Dans le cas que vous avez décrit, vous avez choisi de diviser l'adresse de classe A 10.0.0.0 en sous-réseaux plus petits pour répondre à vos exigences spécifiques.

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

Il existe plusieurs types d'adresses IP, chacun ayant une fonction et une plage d'utilisation spécifiques. Voici une brève explication des principales catégories d'adresses IP :

1. Adresses IP Publiques et Privées :
   - Adresses IP Publiques : Ce sont des adresses IP routables sur l'Internet public. Elles sont uniques dans le monde entier et sont utilisées pour identifier des dispositifs ou des réseaux sur Internet.

    - Adresses IP Privées : Ce sont des adresses IP réservées à une utilisation interne dans des réseaux privés, comme les réseaux locaux d'entreprise ou domestiques. Elles ne sont pas routées sur Internet. Les adresses IP privées permettent de connecter de nombreux dispositifs dans un réseau privé sans épuiser les adresses IP publiques.
2. Adresses IPv4 et IPv6 :
    - IPv4 (Internet Protocol version 4) : C'est la version la plus répandue d'Internet Protocol. Les adresses IPv4 sont représentées sous la forme de quatre groupes de chiffres décimaux, par exemple, 192.168.1.1.
    - IPv6 (Internet Protocol version 6) : Conçu pour remédier à la pénurie d'adresses IPv4, IPv6 utilise une notation hexadécimale et est capable de prendre en charge un nombre colossal d'adresses IP. Par exemple, une adresse IPv6 ressemble à ceci : 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
3. Adresses Unicast, Broadcast et Multicast :
    - Unicast : Une adresse unicast est attribuée à un seul dispositif. Lorsque vous envoyez des données à une adresse unicast, elles parviennent uniquement à ce dispositif spécifique.
    - Broadcast : Une adresse de diffusion (broadcast) est utilisée pour envoyer des données à tous les dispositifs d'un réseau donné. Cependant, les réseaux modernes, en particulier sur Internet, limitent ou éliminent l'utilisation du broadcast pour des raisons de sécurité et d'efficacité.
    - Multicast : Une adresse multicast est utilisée pour envoyer des données à un groupe de dispositifs spécifiques. Les dispositifs qui souhaitent recevoir des données multicast se joignent au groupe…

JOB 12

job 13

JOB 14

JOB 15

Qu’est-ce que le routage ?

Le routage est le processus par lequel des données sont dirigées d'un point à un autre à travers un réseau, en choisissant le chemin le plus approprié pour les faire passer. Le routage est une fonction fondamentale dans les réseaux informatiques, qu'il s'agisse d'Internet, de réseaux locaux d'entreprise, ou d'autres types de réseaux.

Qu’est-ce qu’un gateway ?

Une gateway (ou passerelle en français) est un dispositif ou un logiciel qui agit en tant qu'interface entre deux réseaux informatiques distincts, permettant ainsi la communication et le transfert de données entre eux. Les gateways sont utilisées

pour relier des réseaux qui utilisent différents protocoles, architectures, ou technologies. Elles jouent un rôle crucial dans la transmission des données entre des réseaux hétérogènes.

Qu’est-ce qu’un VPN ?

Un VPN (Virtual Private Network, en français, Réseau Privé Virtuel) est un service ou une technologie qui permet de créer un réseau sécurisé et privé, même lors de la transmission de données sur des réseaux publics comme Internet.

Qu’est-ce qu’un DNS ?

DNS est l'acronyme de “Domain Name System”, ce qui signifie "Système de Noms de Domaine" en français. Le DNS est un protocole et un système de hiérarchie utilisé sur Internet pour convertir les noms de domaine conviviaux en adresses IP numériques, qui sont nécessaires pour acheminer le trafic sur le réseau.