JOB2 :

1- Qu’est-ce qu’un réseau ?

Un réseau est un ensemble de dispositifs interconnectés qui communiquent les uns avec les autres. Ces dispositifs peuvent être des ordinateurs, des serveurs, des périphériques, des routeurs, des commutateurs, des concentrateurs, des téléphones, des caméras, etc. Les réseaux permettent à ces dispositifs de partager des informations, des ressources et des services.

1- À quoi sert un réseau informatique ?

Un réseau informatique sert à connecter différents dispositifs informatiques (ordinateurs, serveurs, imprimantes, routeurs, etc.) afin de leur permettre de communiquer et de partager des ressources et des informations.

2- Quel matériel avons-nous besoin pour construire un réseau ? Détaillez les fonctions de chaque pièce.La construction d'un réseau informatique implique l'utilisation de divers composants matériels, chacun ayant un rôle spécifique dans le fonctionnement du réseau. Voici une liste de certains des composants matériels clés nécessaires pour construire un réseau, ainsi que leurs fonctions :

1. Ordinateurs : Les ordinateurs sont les dispositifs clients sur le réseau. Ils communiquent avec d'autres ordinateurs, accèdent aux ressources partagées et exécutent des applications réseau.

2. Serveurs : Les serveurs sont des ordinateurs spécialisés qui fournissent des services aux clients sur le réseau. Ils peuvent être des serveurs de fichiers, des serveurs web, des serveurs de messagerie, etc.

3. Routeurs : Les routeurs sont des dispositifs de réseau qui acheminent le trafic entre différents réseaux. Ils déterminent la meilleure route pour envoyer des données entre les réseaux.

4. Commutateurs (Switches) : Les commutateurs sont des dispositifs qui relient des dispositifs au sein d'un réseau local (LAN). Ils dirigent le trafic uniquement vers le dispositif de destination approprié, ce qui améliore l'efficacité du réseau.

5. Points d'accès sans fil (WAP) : Les WAP permettent aux dispositifs sans fil de se connecter à un réseau câblé. Ils sont couramment utilisés pour les réseaux Wi-Fi.

6. Câblage : Le câblage est essentiel pour connecter les dispositifs d'un réseau. Il peut s'agir de câbles Ethernet, de câbles de fibre optique, de câbles coaxiaux, etc.

7. Cartes réseau (NIC): Les cartes réseau sont installées dans les ordinateurs et les serveurs pour leur permettre de se connecter au réseau. Ils sont dotés d'adresses MAC uniques pour l'identification.

8. Firewalls : Les pare-feu sont des dispositifs ou des logiciels qui protègent le réseau en filtrant le trafic entrant et sortant, en bloquant les menaces et en maintenant la sécurité.

9. Modems : Les modems sont utilisés pour établir des connexions réseau, en particulier pour l'accès à Internet. Ils convertissent les signaux numériques en signaux analogiques (pour le DSL, le câble, etc.) et vice versa.

10. Imprimantes réseau : Les imprimantes réseau permettent aux utilisateurs d'imprimer des documents directement depuis le réseau.

11. Sauvegarde et stockage en réseau : Les dispositifs de stockage en réseau (NAS) sont utilisés pour stocker des données de manière centralisée et les rendre accessibles à plusieurs utilisateurs.

12. Caméras de sécurité IP Les caméras de sécurité IP sont utilisées pour surveiller et enregistrer des vidéos sur un réseau, offrant une sécurité et une surveillance.

13. Alimentations électriques et onduleurs : Ces dispositifs assurent une alimentation électrique stable aux composants du réseau et protègent contre les pannes de courant.

14. Accessoires réseau: Cela inclut des câbles, des connecteurs, des supports de fixation, des étagères, des ventilateurs de refroidissement, etc.

Chaque composant joue un rôle crucial dans le fonctionnement global du réseau. Les ordinateurs, les serveurs, les routeurs et les commutateurs sont souvent au cœur du réseau, tandis que d'autres composants facilitent la connectivité, la sécurité, le stockage et la gestion du réseau. Le choix des composants dépend des besoins spécifiques du réseau, de sa taille et de sa complexité.

JOB 3 :

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

j’ai utilisé le câbles Automatically Choose Connection Type parce que c’est le plus adéquat pour relier deux ordinateurs et faire passer la connexion.

JOB 4:

1-Qu’est-ce qu’une adresse IP ?

Une adresse IP, ou adresse de protocole Internet, est une étiquette numérique attribuée à chaque dispositif (par exemple, ordinateur, imprimante, routeur, smartphone) connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Les adresses IP sont essentielles pour identifier et localiser chaque dispositif sur un réseau, leur permettant de communiquer et d'échanger des données.

2-À quoi sert un IP ?

Une adresse IP (Internet Protocol) est un identifiant numérique attribué à chaque appareil connecté à Internet. Elle sert à plusieurs choses :

_ Identification de l’appareil

_ Localisation de la connexion

_ Communication entre appareils

_ Sécurité

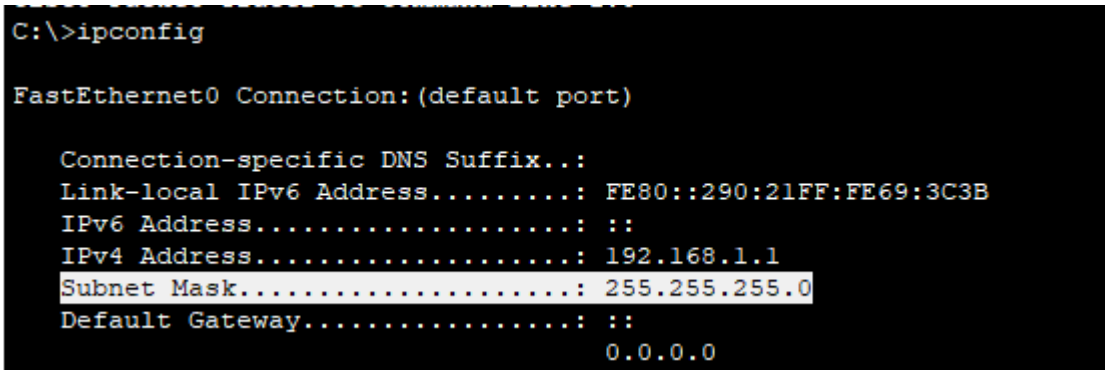
3- Qu’est-ce qu'une adresse MAC ?

Une adresse MAC, ou adresse de contrôle d'accès au support (Media Access Control), est une adresse unique attribuée à chaque interface réseau d'un dispositif. Contrairement à une adresse IP, qui est utilisée pour identifier un dispositif au sein d'un réseau, une adresse MAC identifie de manière unique une carte réseau (carte Ethernet, carte Wi-Fi, etc.) au niveau matériel.

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.

JOB 5: Quelle est l’adresse de ce réseau ?



2- **Quelle ligne de commande avez-vous utilisée pour vérifier l’ip des machines ?**

La commande que j’ai utiliser pour vérifier l’ip des machines est: **ipconfig**

JOB 6 : La connectivité entre le pc de Pierre et celui de Alicia

pc de Pierre:

```
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 = 1ms, Average = 0ms
```

pc Alicia :

```
Cisco Packet Tracer PC Command Line 1.0
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=3ms 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=7ms 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 = 7ms, Average = 2ms
```

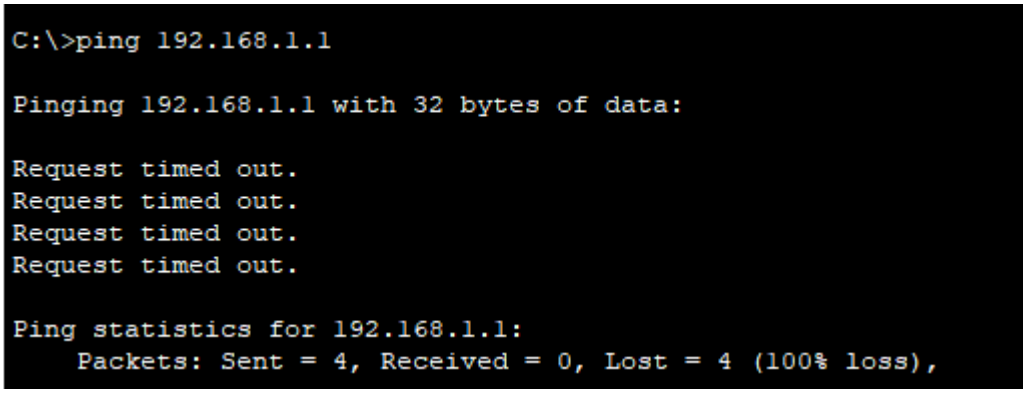
2- **Quelle est la commande permettant de Ping entre des PC ?**

La commande qui m'a permis de de Ping entre des PC est : **ping 192.168.1.**

JOB 7 :

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

Oui Pierre a reçu les paquets envoyés par Alicia



2- **Expliquez pourquoi.**

Après avoir utilisé la commande suivante **ping 192.168.1.1** sur le terminal du PC de Alicia ça nous affiche directement si Pierre a reçu le paquets ou pas . En observant le capture d'écran on voit que le paquets a bien été reçu.

JOB 8 :

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

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.

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

Tous les raccordements (ou ports) d'un hub fonctionnent à la même vitesse et se trouvent dans un même domaine de collision (regroupant tous les appareils connectés en réseau). Contrairement à d'autres périphériques réseau, un hub ne permet pas de cibler ou d'exclure uniquement certains de ces récepteurs.

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

Un commutateur (switch) est un dispositif de réseau qui opère au niveau de la couche 2 (liaison de données) du modèle OSI et est couramment utilisé pour connecter des dispositifs au sein d'un réseau local (LAN). Les commutateurs ont leurs avantages et inconvénients :

Avantages d'un switch :

1. Efficacité de la bande passante : Les commutateurs sont plus efficaces que les hubs, car ils acheminent le trafic uniquement vers le port de destination approprié, plutôt que de diffuser le trafic à tous les ports du réseau. Cela évite la congestion du réseau.

2. Meilleure sécurité: Les commutateurs isolent le trafic entre les ports, ce qui signifie que les données ne sont pas accessibles à tous les dispositifs connectés au switch. Cela améliore la sécurité du réseau.

3. Haute performance : Les commutateurs offrent de bonnes performances, car ils sont conçus pour traiter efficacement le trafic réseau, y compris les transferts de données volumineux et les communications en temps réel.

4. Configuration avancée : Les commutateurs offrent des fonctionnalités de configuration avancée, telles que la surveillance du trafic, le VLAN (Virtual LAN), la qualité de service (QoS) et d'autres options de personnalisation pour optimiser le réseau.

5. Isolation de collision : Les commutateurs évitent les collisions de données, ce qui améliore la stabilité du réseau.

6. Évolutivité: Les commutateurs sont extensibles et permettent de connecter un grand nombre de dispositifs au sein d'un réseau.

Inconvénients d'un switch :

1. Coût: Les commutateurs sont généralement plus chers que les hubs, ce qui peut être un inconvénient pour les réseaux avec un budget limité.

2. Complexité de gestion : Les commutateurs offrent de nombreuses options de configuration avancée, ce qui peut rendre la gestion plus complexe pour les administrateurs réseau inexpérimentés.

3. Éventuelle saturation du réseau : Si mal configurés, les commutateurs peuvent également provoquer une saturation du réseau en raison d'une mauvaise gestion du trafic.

4. Nécessité de surveillance et de maintenance : Les commutateurs nécessitent une surveillance et une maintenance régulières pour s'assurer qu'ils fonctionnent correctement.

5. Risques de sécurité : Bien que les commutateurs offrent une sécurité améliorée, ils ne sont pas immunisés contre toutes les menaces de sécurité, et des vulnérabilités peuvent être exploitées si la sécurité n'est pas correctement configurée.

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

Un switch (commutateur) gère le trafic réseau en utilisant des adresses MAC (Media Access Control) pour déterminer où acheminer les trames de données. Voici comment un switch gère le trafic réseau :

1. Apprentissage des adresses MAC : Lorsqu'un dispositif est connecté à un port du switch, le switch enregistre l'adresse MAC du dispositif associé à ce port dans sa table d'adresses MAC, également appelée table CAM (Content Addressable Memory). Cette table contient des entrées qui associent des adresses MAC à des ports spécifiques du switch.

2. Filtrage et acheminement des trames : Lorsqu'une trame de données arrive sur un port du switch, le switch consulte sa table d'adresses MAC pour déterminer à quel port il doit acheminer la trame. Le switch recherche l'adresse MAC de destination dans la table d'adresse MAC. Si l'adresse MAC est répertoriée dans la table, le switch envoie la trame uniquement au port associé à cette adresse. Cela réduit le trafic inutile sur le réseau.

3. Diffusion (broadcast) : Si le switch ne trouve pas l'adresse MAC de destination dans sa table, il diffuse la trame à tous les ports, sauf le port d'origine. Cela permet de gérer les trames de diffusion, qui sont destinées à tous les dispositifs du réseau local.

4. Routage des trames : Les switches sont conçus pour acheminer efficacement les trames vers leur destination. Cela signifie que chaque trame est acheminée uniquement vers le port du switch où se trouve le dispositif de destination, évitant ainsi les collisions de données et la congestion du réseau.

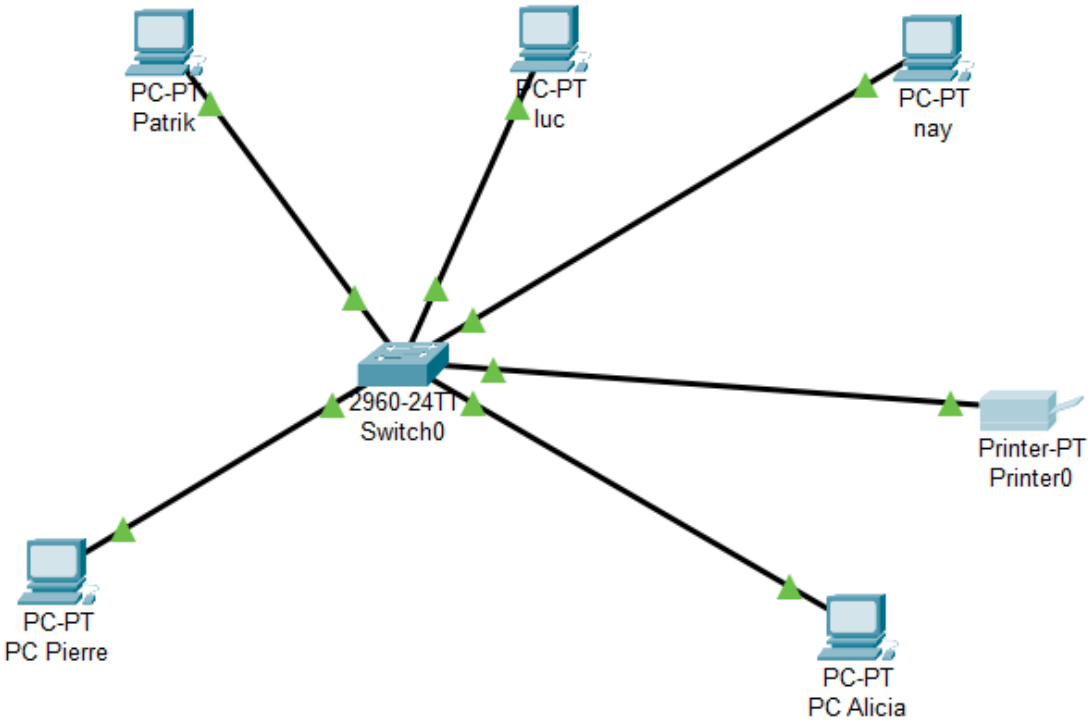
5. Filtrage de trames indésirables : Les switches peuvent également être configurés pour filtrer certaines trames en fonction de critères spécifiques, tels que des listes d'adresses MAC autorisées ou des critères de qualité de service (QoS).

6. Gestion de la qualité de service (QoS) : Certains switches prennent en charge des fonctionnalités de QoS qui permettent de prioriser certaines trames en fonction de leurs besoins, par exemple, en donnant la priorité aux trames vocales sur les trames de données.

7. Mise à jour de la table d'adresses MAC : La table d'adresses MAC du switch est mise à jour en permanence à mesure que de nouveaux dispositifs sont connectés ou que des dispositifs existants sont déconnectés. Cela permet au switch de maintenir une liste à jour des adresses MAC connues.

JOB 9 :

le schéma



Créer un schéma de votre réseau présente plusieurs avantages importants. Voici trois avantages principaux :

1. Visualisation de la topologie : Un schéma de réseau vous permet de visualiser clairement la topologie de votre réseau, c'est-à-dire comment les appareils, les commutateurs, les routeurs, les serveurs, etc., sont connectés les uns aux autres. Cela facilite la compréhension de la structure de votre réseau.

2. Dépannage facilité: En cas de problème ou de panne sur le réseau, un schéma bien documenté peut être un outil précieux pour le dépannage. Vous pouvez rapidement

identifier les connexions, les composants ou les chemins potentiellement problématiques.

3. Planification et amélioration du réseau : Un schéma de réseau vous permet de planifier des améliorations ou des mises à niveau en identifiant les zones de congestion, les points faibles et les opportunités d'optimisation. Cela vous aide à

prendre des décisions éclairées pour améliorer les performances et la sécurité du réseau.

Maintenant, vous pouvez ajouter ces avantages à votre documentation, accompagnés du schéma de votre réseau pour illustrer ces concepts. Assurez-vous d'utiliser un logiciel de dessin ou de conception graphique pour créer un schéma clair et informatif de votre réseau. Les logiciels courants pour cela incluent Microsoft Visio, Lucidchart, Draw.io, ou même des outils de dessin gratuits comme draw.io. Une fois que vous avez créé votre schéma, insérez-le dans votre documentation et ajoutez des explications pour mettre en évidence les avantages que j'ai énumérés.

JOB 10 :

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

La principale différence entre une adresse IP statique et une adresse IP attribuée par DHCP réside dans le mode d'attribution : l'une est configurée manuellement par un administrateur, tandis que l'autre est attribuée automatiquement par un serveur DHCP. Le choix entre les deux méthodes dépend des besoins spécifiques du réseau et de la gestion prévue des adresses IP.

JOB 11 :

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

L'adresse de classe A a une grande plage d'adresses disponibles, ce qui est nécessaire pour créer de nombreux sous-réseaux. Dans ce cas, une adresse de

classe A est suffisante pour répondre à vos besoins en termes de sous-réseaux et d'hôtes.

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

Les classes d'adresses (A, B, C, D, E) déterminent la plage d'adresses disponibles dans un réseau. Les adresses de classe A ont un préfixe de réseau de 8 bits, ce qui signifie qu'elles peuvent être utilisées pour un grand nombre de sous-réseaux avec un grand nombre d'hôtes. Les autres classes ont des préfixes de réseau de différentes tailles, ce qui limite le nombre d'adresses de réseau et d'hôtes possibles. Les sous-réseaux sont créés en empruntant des bits d'adresse d'hôte pour les répartir en sous-réseaux plus petits. La taille des sous-réseaux et le nombre d'hôtes possibles varient en fonction de la classe de l'adresse et du nombre de bits empruntés pour l'adressage du sous-réseau.

JOB 12 :

1- **voilà le tableau dans lequel se trouvent les sept couches du modèle OSI, avec chaque couche une description des rôles.**

COUCHE OSI	DESCRIPTION DES RÔLES	Matériels/Protocoles associés
7. Application	Fournit des interfaces pour les services réseau aux applications	HTTP, FTP, HTML, SSL/TLS
6. Présentation	Convertit, chiffre et comprime les données pour l'échange entre systèmes	SSL/TLS, HTML
5. Session	Établit, gère et termine les sessions entre les applications	SSL/TLS, PPTP
4. Transport	Assure le transfert de bout en bout fiable des données	TCP, UDP
3. Réseau	Gère les adresses logiques et le routage des données	IPv4, IPv6, routeur
2. Liaison de données	Gère les communications entre les entités réseau sur le même lien physique	Ethernet, Wi-Fi, MAC, câble RJ45
1. Physique	Gère les signaux électriques ou optiques pour le transport de données	Fibre optique, câble RJ45

JOB 13 :

1- **Quelle est l'architecture de ce réseau ?**

L'architecture d'un réseau est la structure organisationnelle qui définit comment les composants d'un réseau informatique sont disposés, interconnectés et gérés.

2- **Indiquer quelle est l'adresse IP du réseau ?**

L'adresse IP du réseau, également appelée adresse réseau, est l'adresse IP utilisée pour identifier le réseau dans son ensemble. Elle ne peut pas être attribuée à un dispositif individuel. Dans le contexte de l'adresse IP de classe A 10.0.0.0 que vous avez mentionnée précédemment, l'adresse IP du réseau est 10.0.0.0.

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

le nombre de machines que l'on peut connecter à chaque sous-réseau dépend du masque de sous-réseau spécifié. Les masques de sous-réseau plus petits permettent d'héberger plus d'hôtes, tandis que les masques plus grands limitent le nombre d'hôtes. Pour l'ensemble du réseau, la capacité totale dépend du nombre de sous-réseaux et de la capacité de chacun.

4- **Quelle est l'adresse de diffusion de ce réseau ?**

L'adresse de diffusion d'un réseau est une adresse spéciale utilisée pour envoyer des données à tous les dispositifs du réseau en même temps. Pour déterminer l'adresse de diffusion d'un réseau, vous devez connaître l'adresse IP du réseau et le masque de sous-réseau.

JOB 14 :

1- **Convertissez les adresses IP suivantes en binaires :**

Voici les adresses IP converties en binaire :

1. 145.32.59.24 :
   - Adresse IP binaire : 10010001.00100000.00111011.00011000

2. 200.42.129.16 :
   - Adresse IP binaire : 11001000.00101010.10000001.00010000

3. 14.82.19.54 :
   - Adresse IP binaire : 00001110.01010010.00010011.00110110

Ces adresses IP ont été converties en binaire en représentant chaque octet (chiffre entre deux points) sous forme binaire, où chaque chiffre décimal est remplacé par sa représentation binaire à 8 bits.

JOB 15 :

1- Qu'est-ce que le routage ?

Le routage est le processus de sélection du chemin dans un réseau. Un réseau informatique est composé de nombreuses machines, appelées *nœuds*, et de chemins ou de liaisons qui relient ces nœuds. La communication entre deux nœuds d'un réseau interconnecté peut s'effectuer par de nombreux chemins différents. Le routage est le processus qui consiste à sélectionner le meilleur chemin à l'aide de certaines règles prédéterminées.

2- Qu'est-ce qu'une 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 loca à Internet.

3- **Qu'est-ce qu'un VPN ?**

VPN signifie Virtual **Private Network** et décrit la possibilité d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Les VPN chiffrent votre trafic Internet et camouflent votre identité en ligne. Il est ainsi plus difficile pour des tiers de suivre vos activités en ligne et de voler des données. Le chiffrement est effectué en **temps réel**.

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

Le DNS (Domain Name System, système de nom de domaine) est en quelque sorte le répertoire téléphonique d'Internet. Les internautes accèdent aux informations en ligne via des noms de domaine (par exemple, nytimes.com ou

espn.com), tandis que les navigateurs interagissent par le biais d'adresses IP (Internet Protocol, protocole Internet). Le DNS traduit les noms de domaine en adresses IP afin que les navigateurs puissent charger les ressources web.