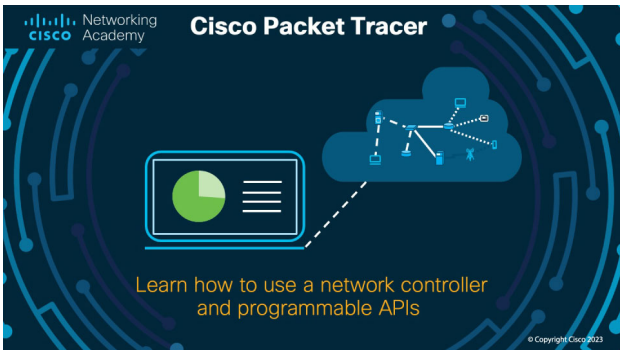
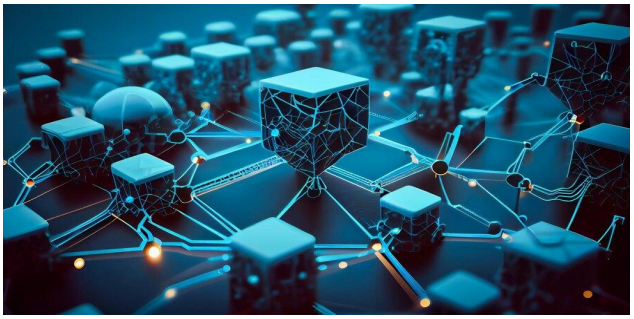
Job 1 :

Installation de *Cisco packet tracer*



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* ou des *services*. Ces dispositifs appelés nœuds sont capables de transmettre et de recevoir des données parmi eux les ordinateurs, les serveurs, les routeurs, des commutateurs et divers autres encore.**

➔ À quoi sert un réseau informatique ?

Un réseau informatique **permet de *connecter* des dispositifs pour *partager* des ressources, faciliter la communication, l'accès à l'information, la collaboration, la sécurité, la gestion de l'infrastructure, le commerce en ligne, le divertissement, le télétravail, l 'éducation en ligne et la télémédecine, jouant un rôle *essentiel* dans la société moderne.**

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

Clients Ordinateurs et Dispositifs : **Ce sont les *dispositifs* utilisateurs qui accèdent au réseau pour *envoyer*, recevoir et *traiter* des données. Ils peuvent être des ordinateurs de bureau, des ordinateurs portables, des smartphones, des tablettes, etc.**

Serveurs : **Les serveurs sont des ordinateurs *puissants* conçus pour *stocker* des données, exécuter des applications, gérer des *ressources* et répondre aux demandes des dispositifs clients.**

Routeurs : **Les routeurs sont des *dispositifs* qui dirigent le *trafic* réseau entre différents *réseaux*, tels que votre réseau local (LAN) et Internet. Ils prennent des décisions sur la manière de *transférer* les données entre les différents réseaux.**

Commutateurs (Interrupteurs) : **Les commutateurs permettent la *communication* au sein d'un *réseau* local en transférant les données qu'aux dispositifs destinataires *appropriés*,**

Boîtiers et armoires réseau : **Ils servent à *protéger* le matériel réseau, à organiser les câbles et à *maintenir* une disposition propre et sécurisée des composants.**

Imprimantes en réseau : **Les imprimantes en réseau permettent l'impression *partagée*, de sorte que plusieurs dispositifs peuvent *envoyer* des impressions vers une imprimante centrale.**

Câblage : **Le câblage structuré, tel que les câbles Ethernet, est *essentiel* pour relier les *dispositifs* au réseau. Il existe différents types de connexion, tels que le câble Cat 5e, Cat 6 et Cat 6a, qui influencent la *vitesse* et la *fiabilité* de la connexion.**

Onduleurs (UPS - Alimentation Sans Interruption) : **Les UPS fournissent une *alimentation* de *secours* en cas de panne électrique pour *éviter* la perte de données et *maintenir* le fonctionnement du réseau.**

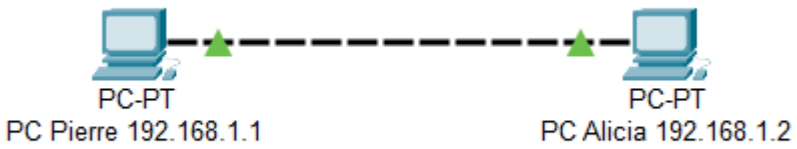
Pare-feu : **Les pare-feu sont des *dispositifs* de sécurité qui contrôlent et *filtrent* le trafic réseau pour *protéger* le réseau contre les menaces *extérieures*, telles que les intrusions et les virus.**

Points d'accès sans fil (AP - Access Points) : **Les AP permettent aux *dispositifs* sans fil tels que les ordinateurs portables et les smartphones de se connecter au réseau. Ils sont *essentiels* pour les réseaux**

Wi-Fi.Modems : **Les modems permettent la connexion à Internet en *traduisant* les signaux numériques du réseau en *signaux* analogiques compréhensibles par le fournisseur d'accès Internet (FAI)**

Systèmes de stockage en réseau (NAS - Network-Attached Storage) : **Les NAS sont des *dispositifs* de stockage qui permettent le stockage *centralisé* de données sur le réseau, facilitant ainsi le *partage* de fichiers et la *sauvegarde***

Job 3 :



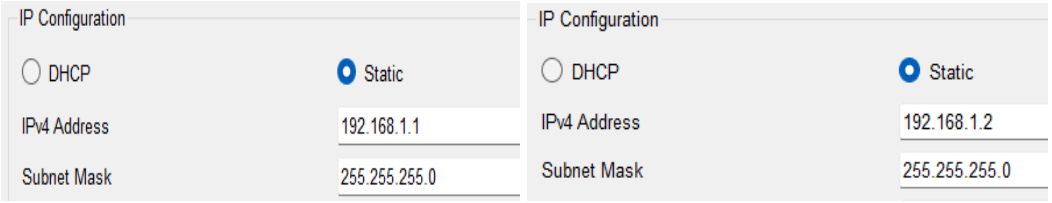
➔ Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

Le câble le plus couramment utilisé est le *Copper Cross-Over (Câble croisé en cuivre)*,car il permet *d'inverser* les broches des câbles pour établir une *communication directe entre* les deux appareils.

C'est un type de câble Ethernet pour connecter des périphériques réseau *homogène*, Cependant, de nombreux appareils *réseau modernes*, y compris les ordinateurs, sont équipés de ports *Ethernet auto-ajustables (auto-MDI/MDIX)* qui peuvent détecter *automatiquement* le type de câble et s'adapter en conséquence.

Cela signifie que dans de nombreux cas,le choix *d'un câble droit ou un câble croisé* dépendra de la *configuration* spécifique de l'appareil et de sa capacité *d'auto-détection.*

Job 4 :



➔ Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol Address) est une *série* de *numéros* qui identifient de manière unique un dispositif ou un nœud sur un réseau informatique utilisant le *protocole Internet (IP)*. Les adresses IP sont essentielles pour *diriger*, *router* et *acheminer* le trafic de données sur Internet et les réseaux locaux.

Il existe deux principales versions d'adresses IP :

IPv4 (Internet Protocol version 4)

IPv6 (Internet Protocol version 6)

➔ À quoi sert un IP ?

Une adresse IP (Internet Protocol) sert à plusieurs fonctions essentielles dans le domaine des réseaux informatiques :

***Acheminement des Données :* Les adresses IP sont utilisées pour *diriger* et acheminer *les paquets* de données à travers un réseau. Chaque paquet de données est *étiqueté* avec l'adresse IP de l'expéditeur et du destinataire, ce qui *permet* aux routeurs et aux commutateurs de déterminer comment *acheminer* les données vers leur destination.**

***Hébergement de Sites Web et de Services :* Les serveurs Web, les serveurs de *messagerie* et d'autres services en ligne ont des adresses IP *associées* à leur nom de domaine. Les visiteurs utilisent ces adresses pour accéder aux sites web et aux services**

Analyse : **Les adresses IP sont *utilisées* pour collecter des *informations* sur le trafic réseau, ce qui permet *d'analyser* les performances du réseau, de *diagnostiquer* les problèmes et de suivre l'utilisation**

Identification des Dispositifs : **Les adresses IP *identifient* de manière *unique* chaque *dispositif* (comme un ordinateur, un serveur, etc) connecté à un réseau. Cela permet de *distinguer* un dispositif d'un autre sur le réseau.**

Sécurité : **Les adresses IP peuvent être *utilisées* dans la détection d'intrusions et le réseau de sécurité pour identifier des activités suspectes ou des menaces.**

Contrôle d'accès : **Les adresses IP sont souvent *utilisées* pour définir des règles de contrôle d'accès, telles que les *listes* de contrôle d'accès (ACL) et les pare-feu. Cela permet de *contrôler* quelles adresses IP sont autorisées ou bloquées sur un réseau**

Connexion à Internet : **Les adresses IP sont attribuées aux *dispositifs* pour qu'ils puissent se connecter à Internet. L'adresse IP d'un dispositif est utilisée pour le *localiser* et le *relier* au réseau mondial.**

➔ *Qu'est-ce qu'une adresse MAC ?*

Une adresse MAC (Media Access Control Address) **est une adresse *matérielle* unique attribuée à une *carte réseau* ou à une *interface réseau d'un dispositif*, telle qu'une carte réseau Ethernet. Contrairement à une adresse IP, qui est utilisée pour identifier un dispositif sur un réseau logique (comme un réseau local ou Internet), une adresse MAC est *spécifique* à la couche de liaison de données du *modèle OSI* (couche 2) et *identifie* un dispositif au sein du réseau physique local. Possédant des caractéristiques clés comme *l'Unicité, le Format, Rôle etc.***

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

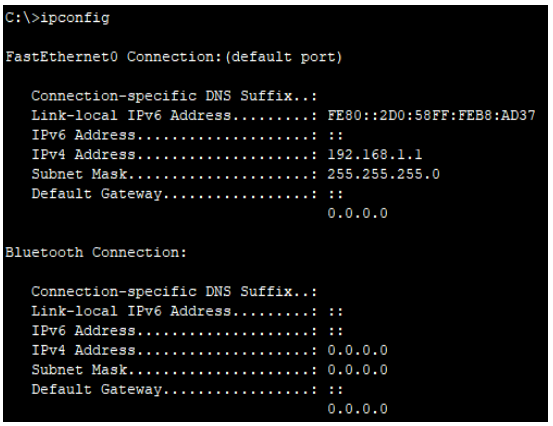
Une adresse IP publique **est une adresse *attribuée* à un *dispositif* ou à un *réseau* qui est directement accessible depuis Internet. Elle permet à ce dispositif ou à ce réseau de *communiquer* avec d'autres dispositifs et réseaux sur Internet. Les adresses IP publiques sont *uniques* à l'échelle mondiale, ce qui signifie qu'aucun autre dispositif sur Internet ne devrait avoir la même *adresse IP publique*. Les serveurs Web, les serveurs de messagerie, les sites Web, les routeurs et les pare-feu exposés sur Internet ont généralement des adresses IP publiques.**

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

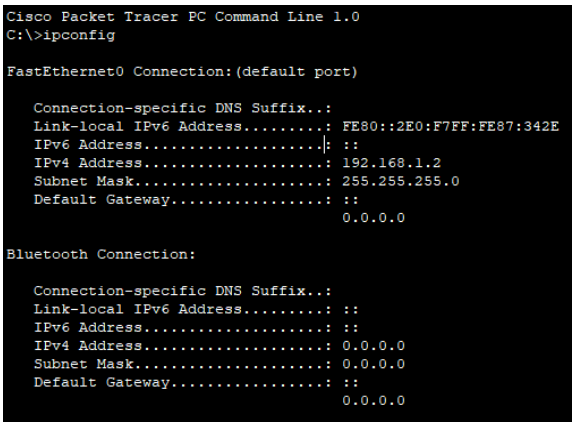
Les trois premiers octets (192.168.1) *indiquent* l'adresse du réseau, et le dernier octet est utilisé pour *identifier* les hôtes spécifiques dans ce réseau. Donc *l'adresse de ce réseau est 192.168.1.0.*

Job 5 :

Capture d'écran de l'ip de Pierre



Capture d'écran de l'ip d'Alicia

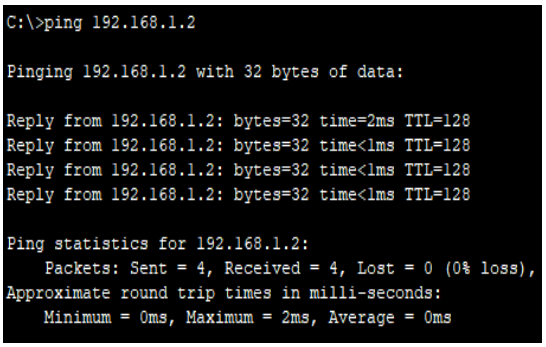


➔ *Quelle ligne de commande avez-vous utilisée pour vérifier l'id des machines ?*

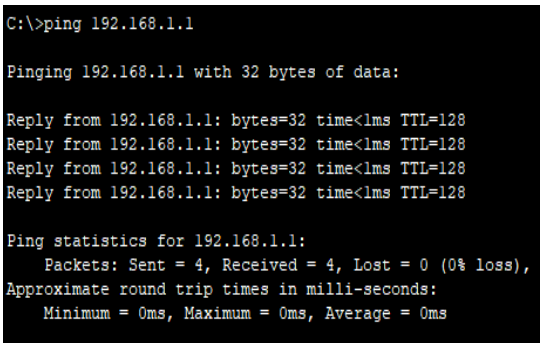
La ligne de commande utilisé est : *ipconfig*

Job 6 :

Capture d'écran du ping de Pierre



Capture d'écran du ping d'Alicia



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

La commande utilisé est : *ping "192.168.1.2 ou 192.168.1.1"*

Job 7 :

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

➔ Expliquez pourquoi.

Le PC de Pierre *n'a pas reçu de paquets* envoyés par Alicia.

L'extinction de l'ordinateur coupe sa connectivité réseau, ce qui signifie qu'il ne peut pas recevoir ni répondre aux paquets "ping" ou à toute autre communication réseau tant qu'il est éteint.

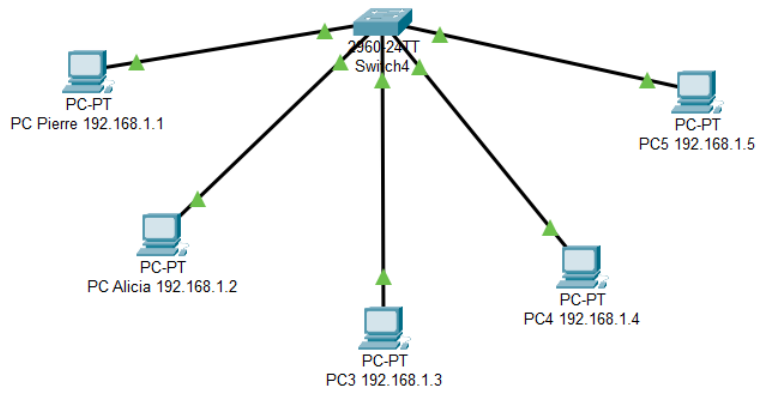
```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Job 8 :



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

Hub : **Un hub est un *dispositif* réseau de la couche *physique* qui *transmet* les données qu'il reçoit à tous les *appareils* connectés à lui. Cela signifie que tous les appareils connectés au hub reçoivent toutes les *données*, ce qui peut provoquer du *trafic inutile* et de la congestion sur le réseau.**

Switch : **Un switch est un *dispositif* de la couche de *liaison* de données qui *opère* au niveau des *adresses* MAC (Media Access Control). Il *examine* l'adresse MAC de chaque *trame* de données *entrante* et la *transmet* uniquement au *port* auquel l'appareil de destination est connecté. Cela réduit la collision et le trafic inutile, *améliorant* ainsi *l'efficacité* et les *performances* du réseau.**

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

Fonctionnement : **Un hub *répète* simplement les *données* reçues sur tous ses *ports*, sans aucune intelligence pour gérer le *trafic*. Il fonctionne en *broadcast*, envoyant les données à tous les appareils connectés.**

Avantages : **Les hubs sont généralement peu coûteux et *faciles* à configurer. Ils conviennent aux petits réseaux où la performance n'est pas critique.**

Inconvénients : **Les inconvénients d'un hub incluent une *mauvaise* efficacité et une *congestion* potentielle du réseau, car tous les appareils reçoivent toutes les données, même celles qui ne leur sont pas destinées. Ils sont obsolètes pour la plupart des applications modernes.**

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

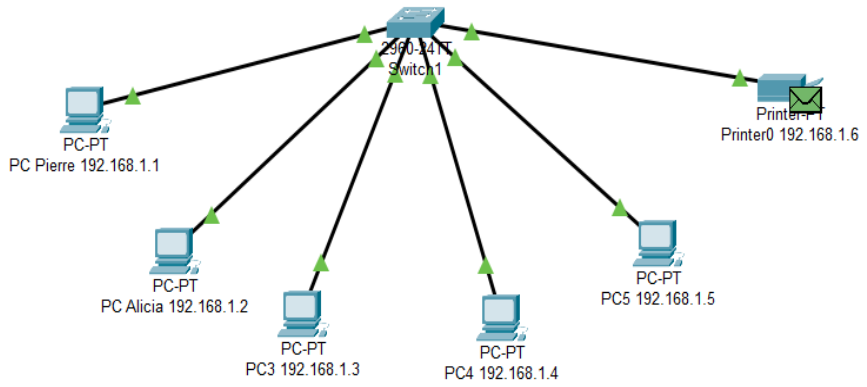
Avantages : **Les avantages d'un switch incluent une *meilleure performance*, une gestion efficace du trafic, la *réduction des collisions*, la segmentation du réseau en groupes logiques, et la *sécurité* accrue, car les données ne sont transmises qu'aux appareils destinataires. Ils sont *essentiels* pour les réseaux de taille moyenne à grande.**

Inconvénients : **Les inconvénients des switches comprennent un *coût plus élevé* que les hubs, une configuration et une maintenance plus *complexes*, ainsi que le besoin de gérer la table d'adresses MAC pour garantir une opération efficace.**

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

Un switch *utilise* une table d'adresses MAC pour *associer* des adresses MAC aux ports physiques du switch. Lorsqu'une trame de données entre dans le switch, il examine l'adresse MAC de destination de la trame, *consulte* sa table d'adresses pour déterminer à quel *port* cette adresse est associée, puis *transmet* la trame uniquement au port correspondant. Cela *limite* la diffusion de données non *nécessaires* et améliore *l'efficacité* du réseau. En conséquence, un switch permet de gérer le trafic réseau de manière beaucoup *plus efficace qu'un hu*

Job 9 :

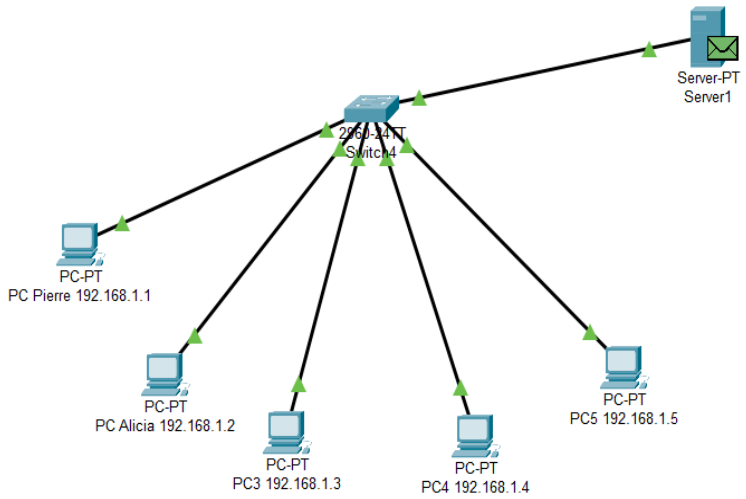


***Visualisation de la topologie du réseau :* Un schéma de réseau fournit une *représentation visuelle de la manière dont tous les composants du réseau sont interconnectés*. Cela permet aux administrateurs et aux équipes de support de *comprendre rapidement la structure du réseau*, y compris les routeurs, les commutateurs, etc. Cela *simplifie* la résolution de problèmes et l'identification des pannes.**

***Planification et évolution du réseau :* Il est plus *facile de planifier des modifications ou des mises à niveau du réseau*. Vous pouvez visualiser l'emplacement actuel des équipements, des câbles et des connexions, ce qui *facilite la planification de nouvelles installations ou de modifications de configuration*.**

***Documenter les informations clés :* Un schéma de réseau permet de *documenter des informations importantes* telles que les adresses IP, les noms d'hôtes, les numéros de port, les types de câbles, etc. Cela *crée une ressource de référence précieuse pour les membres de l'équipe informatique et aide à assurer la cohérence des configurations* et la conformité aux normes.**

Job 10 :



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

la différence se situe au niveau de la *configuration*, en effet Les adresses IP statiques se configure *manuellement* par un administrateur, restent stables et ne *changent pas automatiquement*, quant aux adresses attribuées par DHCP, elles sont configurées *automatiquement* par un serveur DHCP, elles sont *dynamiques* et par conséquent peuvent *changent* à chaque nouvelle connexion.

Job 11 :

Routeur 1 **(Interface 0 - 10.0.0.1 /28) :**

Sous-réseau 1 **(12 hôtes) :**

- **Masque de sous-réseau : 255.255.255.240 (/28)**
- **Plage d'adresses : 10.0.0.1 - 10.0.0.14**

Sous-réseau 2 **(30 hôtes) :**

- **Masque de sous-réseau : 255.255.255.224 (/27)**
- **Plage d'adresses : 10.0.0.17 - 10.0.0.46**

Sous-réseau 3 **(30 hôtes) :**

- **Masque de sous-réseau : 255.255.255.224 (/27)**
- **Plage d'adresses : 10.0.0.49 - 10.0.0.78**

Sous-réseau 4 **(30 hôtes) :**

- **Masque de sous-réseau : 255.255.255.224 (/27)**
- **Plage d'adresses : 10.0.0.81 - 10.0.0.110**

Sous-réseau 5 **(30 hôtes) :**

- **Masque de sous-réseau : 255.255.255.224 (/27)**
- **Plage d'adresses : 10.0.0.113 - 10.0.0.142**

Routeur 2 ***(Interface 1 - 10.0.0.49 /28) :***

Sous-réseau 6 **(30 hôtes) :**

- **Masque de sous-réseau : 255.255.255.224 (/27)**
- **Plage d'adresses : 10.0.0.145 - 10.0.0.174**

Sous-réseau 7 **(120 hôtes) :**

- **Masque de sous-réseau : 255.255.255.128 (/25)**
- **Plage d'adresses : 10.0.0.177 - 10.0.0.254**

Sous-réseau 8 **(120 hôtes) :**

- **Masque de sous-réseau : 255.255.255.128 (/25)**
- **Plage d'adresses : 10.0.0.257 - 10.0.0.384**

Sous-réseau 9 **(120 hôtes) :**

- **Masque de sous-réseau : 255.255.255.128 (/25)**
- **Plage d'adresses : 10.0.0.387 - 10.0.0.514**

Sous-réseau 10 **(120 hôtes) :**

- **Masque de sous-réseau : 255.255.255.128 (/25)**
- **Plage d'adresses : 10.0.0.517 - 10.0.0.644**

Sous-réseau 11 **(120 hôtes) :**

- **Masque de sous-réseau : 255.255.255.128 (/25)**
- **Plage d'adresses : 10.0.0.649 - 10.0.0.792**

Routeur 3 ***(Interface 2 - 10.0.0.97 /28) :***

Sous-réseau 12 **(160 hôtes) :**

- **Masque de sous-réseau : 255.255.255.192 (/26)**
- **Plage d'adresses : 10.0.0.801 - 10.0.0.944**

Sous-réseau 13 **(160 hôtes) :**

- **Masque de sous-réseau : 255.255.255.192 (/26)**
- **Plage d'adresses : 10.0.0.953 - 10.0.0.1096**

Sous-réseau 14 **(160 hôtes) :**

- **Masque de sous-réseau : 255.255.255.192 (/26)**
- **Plage d'adresses : 10.0.0.1105 - 10.0.0.1248**

Sous-réseau 15 **(160 hôtes) :**

- **Masque de sous-réseau : 255.255.255.192 (/26)**
- **Plage d'adresses : 10.0.0.1257 - 10.0.0.1400**

Sous-réseau 16 **(160 hôtes) :**

- **Masque de sous-réseau : 255.255.255.192 (/26)**

- **Plage d'adresses : 10.0.0.1401 - 10.0.0.1550**

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

L'utilisation de l'adresse de classe A 10.0.0.0 a été choisie car les adresses de classe A disposent *d'un octet de réseau de 8 bits*, ce qui permet une grande *flexibilité* pour *diviser* l'espace d'adressage en *sous-réseaux* de différentes tailles.

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

La différence entre les différents types d'adresses réside principalement dans la *taille* du réseau qu'elles peuvent contenir et le *nombre d'hôtes* qu'elles peuvent prendre en charge :

***Les adresses de classe A* sont conçues pour les *grands réseaux*, avec *un octet de réseau*. Elles peuvent prendre en charge un *très grand nombre d'hôtes*, mais elles sont souvent utilisées pour créer de nombreux *sous-réseaux de tailles différentes*.**

***Les adresses de classe B* ont *deux octets de réseau* et sont conçues pour les réseaux de *taille moyenne*. Elles peuvent prendre en charge un *nombre modéré d'hôtes* et sont également utilisées pour créer des *sous-réseaux*.**

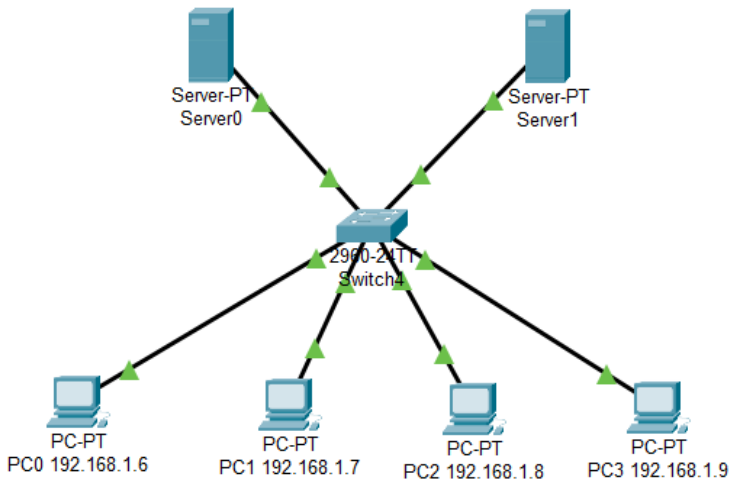
***Les adresses de classe C* ont *trois octets de réseau* et sont conçues pour les *petits réseaux*. Elles prennent en charge un *nombre limité d'hôtes*.**

Job 12 :

Couche OSI	Matériels Protocoles	Description des Rôles
Couche 7	HTML, FTP	La couche Application est en contact direct avec les utilisateurs et les applications. Elle fournit des services de réseau aux applications logicielles (par exemple, HTTP, FTP, HTML).
Couche 6	SSL/TLS	La couche Présentation est responsable de la conversion, de la compression, du cryptage et du formatage des données pour l'envoi. Elle s'occupe de la syntaxe des données échangées.
Couche 5	PPTP (Point-to-Point Tunneling Protocol)	La couche Session est responsable de l'établissement, de la gestion et de la fin des sessions de communication entre les applications (par exemple, SSL/TLS pour sécuriser les sessions).
Couche 4	TCP (Transmission Control Protocol), UDP (User Datagram Protocol)	La couche Transport assure la fiabilité de la communication en gérant le contrôle de flux, la correction d'erreurs et la segmentation des données. Les protocoles courants incluent TCP et UDP.
Couche 3	IPv4, IPv6, routeur	La couche Réseau traite le routage des paquets de données, l'acheminement et la détermination du

		meilleur chemin pour atteindre la destination. Les protocoles courants incluent *IPv4 et IPv6*.
Couche 2	***Ethernet, MAC (adresse MAC), Wi-Fi, câble RJ45***	La couche ***Liaison de données*** gère *la communication entre les nœuds directs et assure la détection d'erreurs et le contrôle d'accès au support* (par exemple, Ethernet, Wi-Fi, et les adresses MAC).
Couche 1	***Fibre optique***	La couche ***Physique*** se *concentre sur la transmission brute des données sur un support physique* (par exemple, câble RJ45, fibre optique, signaux électriques, etc.).

Job 13 :



Architecture du réseau : Ce réseau est configuré en utilisant *l'adresse IP 192.168.10.XXX, où XXX est compris entre 1 et 255*. Le masque de sous-réseau 255.255.255.0 indique que les *3 premiers octets (192.168.10) sont le réseau*, et le *dernier octet est utilisé pour l'identification des hôtes*.

Adresse IP du réseau : **L'adresse IP du réseau est *192.168.10.0*. Cela correspond à l'adresse de réseau de *la plage d'adresses IP* attribuée aux ordinateurs.**

Nombre de machines sur le réseau : **Avec un masque de sous-réseau de 255.255.255.0, vous avez *8 bits disponibles pour les adresses IP des hôtes* (car 32 bits au total moins les 24 bits utilisés par le masque de sous-réseau). Cela signifie qu'il y a *256 adresses IP possibles pour les hôtes*, mais *deux adresses* sont *réservées (l'adresse de réseau et l'adresse de diffusion)*, laissant *254 adresses IP* utilisables pour les ordinateurs sur ce réseau.**

Adresse de diffusion du réseau : **L'adresse de diffusion pour ce réseau est *192.168.10.255*. Cela signifie que si vous *envoyez un paquet à cette adresse*, il sera *diffusé à toutes les machines sur le réseau*.**

Job 14 :

145.32.59.24 en binaire :

145 en binaire :
10010001

32 en binaire :
00100000

59 en binaire :
00111011

24 en binaire :
00011000

Adresse IP en binaire :
10010001.00100000.00111011.00011000

200.42.129.16 en binaire :

200 en binaire :
11001000

42 en binaire :
00101010

129 en binaire :
10000001

16 en binaire :
00010000

Adresse IP en binaire :
11001000.00101010.10000001.00010000

14.82.19.54 en binaire :

14 en binaire :
00001110

82 en binaire :
01010010

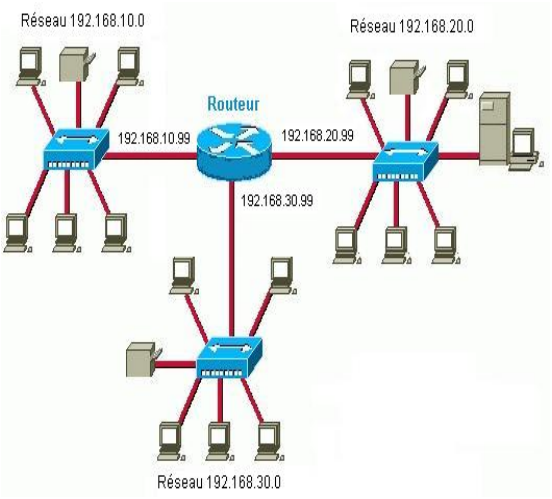
19 en binaire :
00010011

54 en binaire :
00110110

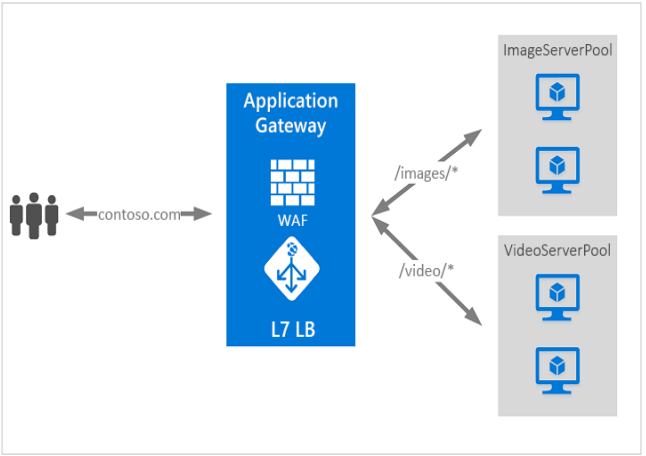
Adresse IP en binaire :
00001110.01010010.00010011.00110110

Job 15 :

Le routage : **Le routage est le processus de *transmission* de données entre différents réseaux informatiques. Il consiste à déterminer le *chemin* optimal pour les paquets de *données* à travers un réseau, en fonction des *adresses IP de destination*, pour assurer leur *acheminement* vers la destination correcte. Ils prennent des décisions de routage en fonction des informations de la table de routage.**



Une gateway : **Une gateway, ou passerelle, est un *périphérique* qui connecte différents réseaux informatiques. Elle sert de *point d'entrée et de sortie* entre un réseau local (LAN) et d'autres réseaux, tels qu'Internet. Les gateways sont souvent utilisés pour *relier* un *réseau interne à Internet*. Elles effectuent des tâches de routage et de translation d'adresses réseau (NAT) pour permettre la *communication* entre des réseaux de protocoles différents.**



Un VPN (Virtual Private Network) : **Un VPN est un *réseau privé virtuel* qui permet de sécuriser et *d'anonymiser* la communication sur un réseau public, comme *Internet*. Il crée un tunnel *crypté* entre l'ordinateur de l'utilisateur et un serveur VPN, *masquant* ainsi *l'adresse IP* de l'utilisateur et chiffrant les données. Les VPN sont couramment *utilisés pour la confidentialité en ligne*, l'accès à distance sécurisé à des réseaux privés.**

Un DNS (Domain Name System) : **Le DNS est un *système* de noms de domaine qui *traduit* les noms de domaine conviviaux pour les humains *en adresses IP* utilisées par les ordinateurs pour *localiser* des ressources en ligne. *Il associe des noms de domaine* (comme www.exemple.com) à des adresses IP correspondantes. Le DNS facilite la navigation sur le web en utilisant des *noms de domaine* au lieu de se souvenir d'adresses IP numérique**