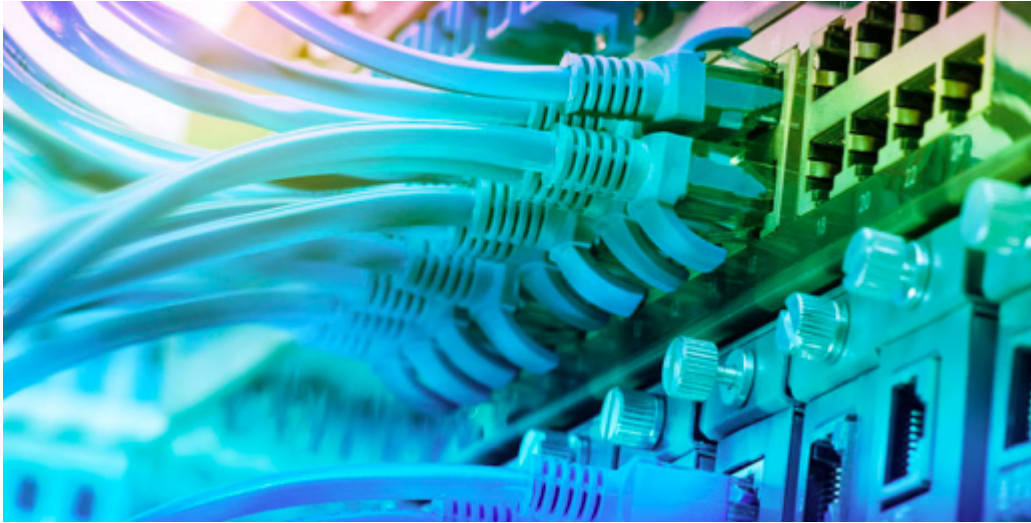


Runtrack Réseau



JOB 2

→ Qu'est-ce qu'un réseau ?

-Un réseau est une structure composée d'entités interconnectées qui échangent des informations, des ressources ou des services. Les entités dans un réseau peuvent être des ordinateurs, des personnes, des appareils, des organisations, des points d'accès sans fil, etc. Les réseaux sont utilisés pour faciliter la communication, le partage de données, l'accès à des ressources ou des services, et bien d'autres applications.

→ À quoi sert un réseau informatique ?

Un réseau informatique sert à connecter des ordinateurs et des appareils pour partager des ressources, des informations et faciliter la communication. Il permet également l'accès à Internet, la gestion des données, la sécurité, l'automatisation et bien d'autres fonctions essentielles.

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

Pour construire un réseau informatique, on aura besoin de divers composants matériels chacun ayant des fonctions spécifiques

Ordinateurs

et appareils clients

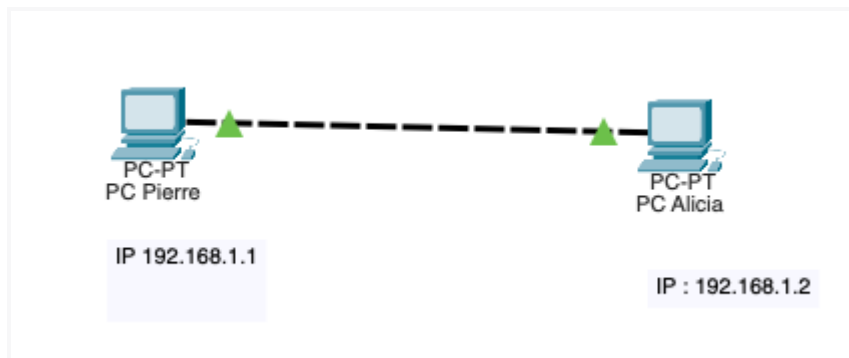
Serveurs Routeurs Câbles Points d'accès Wi-Fi Serveurs DHCP Firewalls ect a
revoir détaillée

JOB 3

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

j'ai choisie le câbles copper cross over pour relier les deux ordinateurs car il permet aux signaux de transmission de données d'être échangés correctement entre les deux dispositifs. Cela permet une communication directe d'un appareil à l'autre, ce qui est utile pour certaines configurations réseau.

JOB 4



→ Qu'est-ce qu'une adresse IP ?

Une adresse IP est un numéro d'identification permettant d'identifier et localiser un appareil sur un réseau et acheminer des données sur internet. Elle est composée de quatre nombres décimaux séparés par des points.

→ À quoi sert un IP ?

Les adresse ip sont indispensables pour l'acheminement des données et la communication sur les réseaux, pour surveiller le trafic et diagnostiquer des problèmes de réseaux , pour la sécurité (pare feu) pour identifier un appareil de façon unique et gérer les appareils et leurs communications sur un réseau. Et enfin acheminer les données.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC est un identifiant unique attribué à chaque carte réseau d'un appareil informatique? elles sont spécifiques à la couche de liaison de données dans le système OS

Elles sont essentielles pour le fonctionnement des réseaux locaux.

les adresses mac sont exprimées en Hexadécimales et sont composées en 12 caractères alphanumériques

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

1- Une adresse ip privée est utilisée à l'intérieur d'un réseau local généralement utilisé pour une utilisation en interne. les appareils dans un réseau local partagent en général une adresse ip privée pour communiquer entre eux.

2- Une adresse IP publique est utilisée pour identifier un appareil ou un réseau sur internet. c'est l'adresse ip que les appareils utilisent pour communiquer avec d'autres situés en dehors du réseau

→ Quel est l'adresse de ce réseau ?

ladresse de ce reseau est 255.255.255.0

JOB 5

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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::20C:CFFF:FE32:6D1A
    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
```

```

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:63FF:FE8C:BAAD
    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

```

j'utilise la commande ipconfig

JOB 6

→ Quelle est la commande permettant de Ping entre des PC ?
ping (adresse IP du PC cible)

```

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<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 = 3ms, Average = 0ms

C:\>

```

```

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<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=18ms 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 = 18ms, Average = 4ms

C:\>

```

JOB 7

```

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),

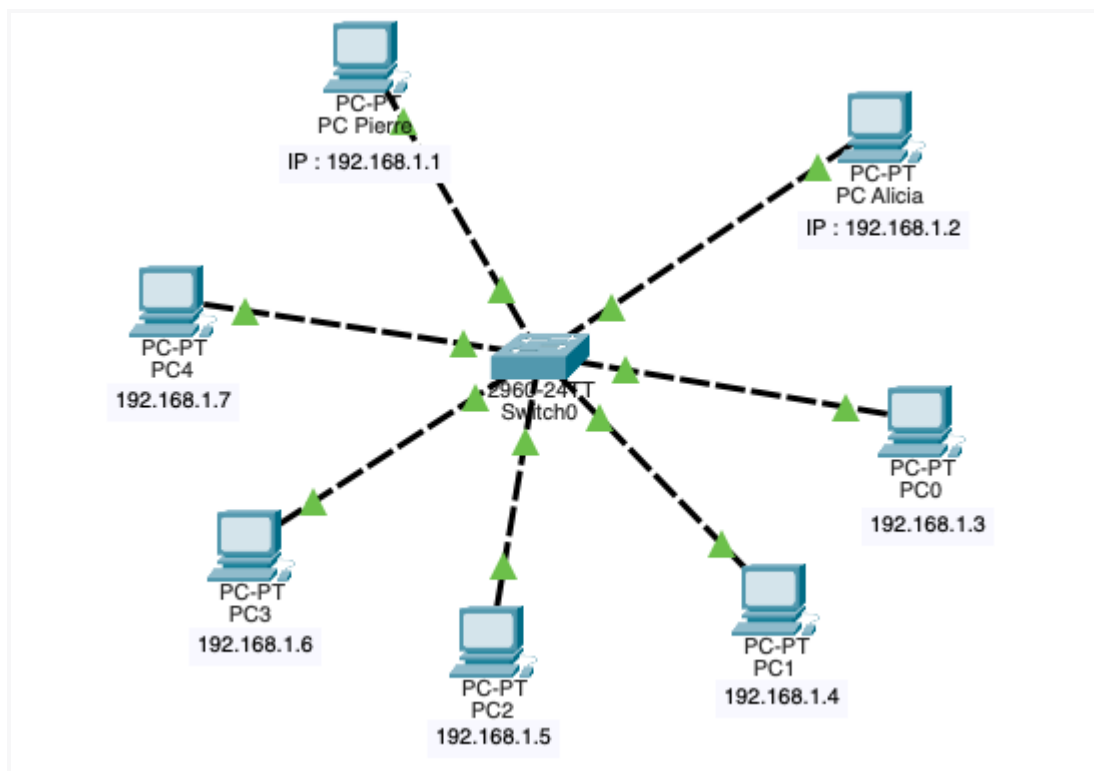
```

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

→ Expliquez pourquoi.

le pc de Pierre n'a pas reçu les paquets envoyés par Alicia car lorsque l'ordinateur est éteint, sa carte réseau est également éteinte. Par conséquent, il ne peut pas détecter ou traiter les paquets entrants.

JOB 8



```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=22ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 22ms, Average = 5ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=2ms TTL=128
Reply from 192.168.1.3: bytes=32 time=22ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 22ms, Average = 6ms

C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=23ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 23ms, Average = 6ms

C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.7

Pinging 192.168.1.7 with 32 bytes of data:

Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128
Reply from 192.168.1.7: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

→ 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.

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

Un hub fonctionne en rediffusant les données qu'il reçoit sur un port à tous les autres ports du hub, sans égard à leur destination. Lorsqu'un appareil connecté à un port du hub envoie des données, le hub les réplique sur tous les autres ports. Par conséquent, tous les appareils connectés au hub reçoivent les données, mais seuls ceux dont l'adresse MAC correspond à la destination réelle traitent ces données

Avantages :

- Simplicité : Les hubs sont simples à configurer et à utiliser, ce qui les rend adaptés aux réseaux de base.
- Coût abordable : Les hubs sont généralement moins chers que d'autres dispositifs de réseau.

Inconvénients :

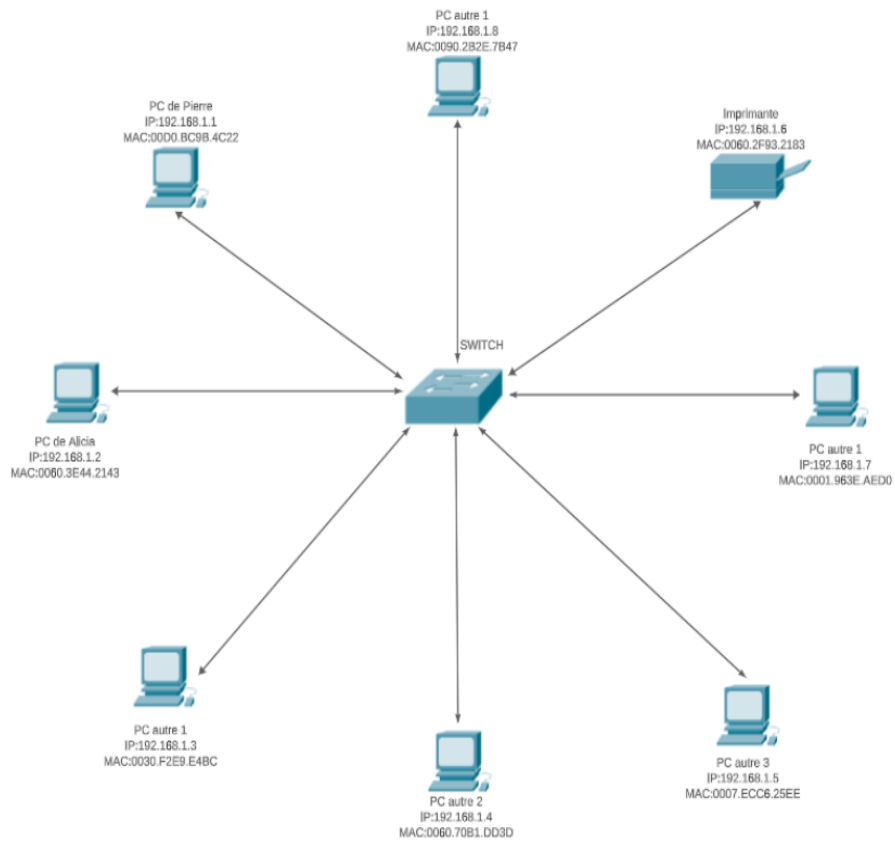
- Diffusion excessive : La rediffusion des données à tous les ports entraîne une diffusion excessive, ce qui peut engorger le réseau.
- Sécurité : Les données sont accessibles à tous les appareils connectés, ce qui les rend vulnérables à l'interception.
- Performance limitée : Les hubs ne sont pas adaptés aux réseaux modernes à haut débit, car ils peuvent provoquer des collisions de données et ralentir les performances.

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

avantages

- Rendement
- Performance élevée
- Isolation
- Sécurité
- Évolutivité

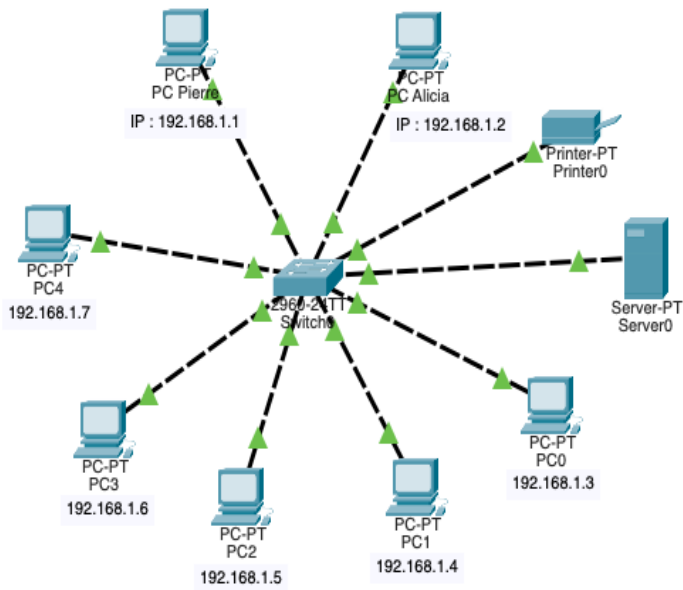
JOB 9



Les avantages de faire un schéma pour son réseau sont les suivants :

- Clarté visuelle
- Planification préalable
- Identification des problèmes potentiels
- Sécurité renforcé
- Optimisation de performance

JOB 10



Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☐ On ☒ Off

Pool Name: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 169 254 0 0

Subnet Mask: 255 255 0 0

Maximum Number of Users: 512

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	169.254...	255.255...	512	0.0.0.0	0.0.0.0

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

Une adresse IP statique est configurée manuellement sur un appareil, tandis qu'une adresse IP

attribuée par DHCP est automatiquement assignée par un serveur DHCP. Les adresses statiques sont permanentes, tandis que les adresses DHCP sont temporaires et gérées centralement.

JOB 11

Adresse réseau	Masque sous-réseau	Ci dr	Adresse sous-réseau	Nombr e hôtes	Plage d'adresse	Adresse Broadcast
10.0.0.0	255.255.255.240	28	10.1.0.0	14	10.1.0.1 à 10.1.0.14	10.1.0.15
10.0.0.1	255.255.255.224	27	10.2.0.0	30	10.2.0.1 à 10.2.0.30	10.2.0.31
10.0.0.0	255.255.255.224	27	10.3.0.0	30	10.3.0.1 à 10.3.0.30	10.3.0.31
10.0.0.0	255.255.255.224	27	10.4.0.0	30	10.4.0.1 à 10.4.0.30	10.4.0.31
10.0.0.0	255.255.255.224	27	10.5.0.0	30	10.5.0.1 à 10.5.0.30	10.5.0.31
10.0.0.0	255.255.255.224	27	10.6.0.0	30	10.6.0.1 à 10.6.0.30	10.6.0.31
10.0.0.0	255.255.255.128	25	10.7.0.0	126	10.7.0.1 à 10.7.0.126	10.7.0.127
10.0.0.0	255.255.255.128	25	10.8.0.0	126	10.8.0.1 à 10.8.0.126	10.8.0.127
10.0.0.0	255.255.255.128	25	10.9.0.0	126	10.9.0.1 à 10.9.0.126	10.9.0.127
10.0.0.0	255.255.255.128	25	10.10.0.0	126	10.10.0.1 à 10.10.0.126	10.10.0.127
10.0.0.0	255.255.255.128	25	10.11.0.0	126	10.11.0.1 à 10.11.0.126	10.11.0.127

10.0.0.0	255.255.255.0	24	10.12.0.0	254	10.12.0.1 à 10.12.0.254	10.12.0.255
10.0.0.0	255.255.255.0	24	10.13.0.0	254	10.13.0.1 à 10.13.0.254	10.13.0.255
10.0.0.0	255.255.255.0	24	10.14.0.0	254	10.14.0.1 à 10.14.0.254	10.14.0.255
10.0.0.0	255.255.255.0	24	10.15.0.0	254	10.15.0.1 à 10.15.0.254	10.15.0.255
10.0.0.0	255.255.255.0	24	10.16.0.0	254	10.16.0.1 à 10.16.0.254	10.16.0.255

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

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

JOB 12

Physique Couche 1 Fibre optique Wi-Fi Câble RJ45	La couche physique dans les réseaux informatiques gère les équipements, tels que les câbles et les routeurs, nécessaires pour le transfert de données. Elle est cruciale pour assurer la communication entre les dispositifs de fabricants différents grâce à l'application de normes. Sans ces normes, la transmission entre ces appareils serait impossible.
Liaison de données Couche 2 Ethernet MAC PPTP	La couche réseau permet la communication entre réseaux différents, tandis que la couche liaison de données gère le transfert d'informations au sein d'un même réseau. Elle transforme les paquets réseau en trames et assure le contrôle des erreurs et du flux pour garantir une transmission réussie au sein du réseau.
Réseau Couche 3 PPTP IPv4 IPv6 Routeur	La couche réseau divise les données à l'émetteur et les reconstitue chez le récepteur lorsqu'il y a une transmission entre deux réseaux distincts. Lorsque la communication s'effectue à l'intérieur d'un même réseau, cette couche n'est généralement pas nécessaire. Cependant, la plupart des utilisateurs se connectent à divers réseaux, notamment des réseaux dans le cloud. Lorsque les données doivent traverser différents réseaux, la couche réseau crée des petits paquets de données qu'elle achemine vers leur destination, où ils sont ensuite réassemblés.
Transport Couche 4 TCP UDP	La couche transport est chargée de fragmenter les données en segments plus petits lors de leur transfert sur un réseau. Cette fragmentation améliore l'efficacité et la vitesse de transmission. Les segments contiennent des informations d'en-tête permettant leur réassemblage sur le périphérique de destination. De plus, ces données segmentées comportent un mécanisme de contrôle d'erreur, signalant à la couche session de rétablir la connexion si des paquets ne parviennent pas entièrement au destinataire cible.

<p>Session Couche 5</p>	<p>Pour permettre la communication entre deux appareils, une application doit créer une session, qui identifie l'utilisateur sur le serveur distant. Cette session doit rester ouverte suffisamment longtemps pour permettre le transfert des données, mais elle doit être fermée une fois le transfert terminé. Lorsque de grandes quantités de données sont transférées, la couche session s'assure que le fichier est transféré en entier et que la retransmission n'a lieu que pour les données manquantes. Par exemple, si 10 Mo de données sont transférés, mais seuls 5 Mo sont complets, la couche session veille à ce que seuls les 5 Mo manquants soient retransmis. Cela améliore l'efficacité de la communication réseau en évitant le gaspillage de ressources et la retransmission inutile de l'ensemble du fichier.</p>
<p>Présentation Couche 6</p>	<p>La couche de présentation dans le modèle OSI prépare les données pour leur affichage à l'utilisateur. Elle effectue des opérations telles que l'encodage et le décodage des informations, notamment dans le cas de la communication via HTTPS qui implique le chiffrement des données. De plus, la couche de présentation gère la compression et la décompression des données lors de leur transfert entre appareils. En résumé, elle s'occupe de rendre les données lisibles et gère leur sécurité et leur efficacité lors de la communication.</p>
<p>Application Couche 7</p> <p>SSL/TLS FTP HTML</p>	<p>La couche 7 du modèle OSI est en relation directe avec l'utilisateur et gère les applications. Par exemple, les clients de messagerie et les navigateurs Web fonctionnent à ce niveau. C'est là que les utilisateurs interagissent avec les applications et les protocoles tels que le SMTP et le HTTP sont utilisés pour des communications spécifiques. En résumé, la couche 7 gère l'interface utilisateur et les applications.</p>

JOB 13

→ Quelle est l'architecture de ce réseau ? l'architecture de ce réseau est en étoile

→ Indiquer quelle est l'adresse IP du réseau ? L'adresse IP du réseau est 192.168.10.0

→ Déterminer le nombre de machines que l'on peut brancher sur ce réseau ? On peut brancher 254 machines sur le réseau.

→ Quelle est l'adresse de diffusion de ce réseau? L'adresse IP de diffusion de ce réseau est 192.168.10.255

JOB 14

Convertissez les adresses IP suivantes en binaires :

• **145.32.59.24**

Binaire : 10010001.00100000.00111011.00011000

• **200.42.129.16**

Binaire : 11001000.00101010.10000001.00010000

• **14.82.19.54**

Binaire : 00001110.01010010.00010011.00110110

JOB 15

→ Qu'est-ce que le routage ?

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

→ Qu'est-ce qu'un gateway ?

un gateway est le nom générique d'un dispositif permettant de relier deux réseaux informatiques de types différents, par exemple un réseau local et le réseau Internet.

→ Qu'est-ce qu'un VPN ?

En informatique, un réseau privé virtuel ou réseau virtuel privé, plus communément abrégé en VPN, est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunications publics.

→ Qu'est-ce qu'un DNS ?

Le Domain Name System ou DNS est un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements