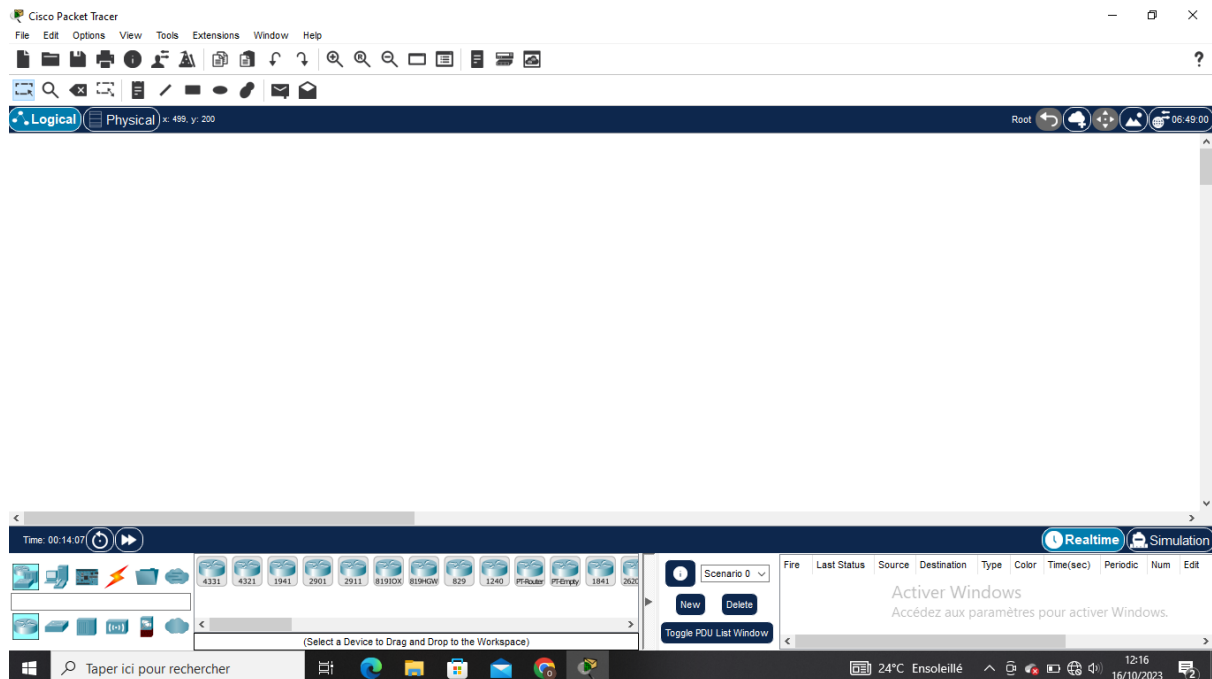


➤ job 01



➤ job 02

Q1:Qu'est-ce qu'un réseau ?

R1:Un réseau est un ensemble d'appareils électroniques interconnectés, capables de communiquer entre eux. Les réseaux informatiques sont utilisés pour partager des ressources, telles que des données, des applications et des périphériques.

Q2:À quoi sert un réseau informatique ?

R2:Les réseaux informatiques servent à plusieurs fins, notamment :

- **Partager des ressources : les réseaux permettent aux utilisateurs de partager des données, des applications et des périphériques. Par exemple, un réseau peut être utilisé pour partager un fichier entre plusieurs ordinateurs, ou pour accéder à une imprimante depuis plusieurs ordinateurs.**
- **Faciliter la collaboration : les réseaux permettent aux utilisateurs de collaborer sur des projets. Par exemple, un réseau peut être utilisé pour**

partager des documents, des idées et des commentaires entre plusieurs utilisateurs.

- Fournir un accès à Internet : les réseaux sont souvent utilisés pour fournir un accès à Internet aux utilisateurs.

Q3: Quel matériel avons-nous besoin pour construire un réseau ?

R3 : Pour construire un réseau informatique, nous avons besoin du matériel suivant :

- **Appareils clients** : les appareils clients sont les appareils qui se connectent au réseau. Les appareils clients les plus courants sont les ordinateurs, les smartphones et les tablettes.
- **Équipements de réseau** : les équipements de réseau sont les appareils qui connectent les appareils clients entre eux et au réseau. Les équipements de réseau les plus courants sont les concentrateurs, les commutateurs, les routeurs et les passerelles.
- **Câbles et connecteurs** : les câbles et les connecteurs sont utilisés pour connecter les appareils clients et les équipements de réseau. Les types de câbles et de connecteurs les plus courants sont les câbles Ethernet et les connecteurs RJ45.

Fonctions de chaque pièce

- **Appareils clients** : les appareils clients sont les appareils qui utilisent le réseau. Les appareils clients les plus courants sont les ordinateurs, les smartphones et les tablettes. Les appareils clients sont équipés d'une carte réseau qui leur permet de se connecter au réseau.
- **Équipements de réseau** : les équipements de réseau sont les appareils qui connectent les appareils clients entre eux et au réseau. Les équipements de réseau les plus courants sont les concentrateurs, les commutateurs, les routeurs et les passerelles.
 - **Concentrateur** : le concentrateur est un équipement de réseau qui relie plusieurs appareils clients entre eux. Le concentrateur répète le signal de chaque appareil client à tous les autres appareils clients connectés au concentrateur.
 - **Commutateur** : le commutateur est un équipement de réseau qui relie plusieurs appareils clients entre eux. Le commutateur ne répète le signal d'un appareil client qu'aux appareils clients qui sont connectés à ce même commutateur.
 - **Routeur** : le routeur est un équipement de réseau qui relie deux réseaux différents. Le routeur utilise des tables de routage pour

déterminer l'itinéraire le plus efficace pour acheminer les données entre deux réseaux.

- **Passerelle** : la passerelle est un équipement de réseau qui relie un réseau local à un réseau public, tel qu'Internet. La passerelle utilise des protocoles de routage pour acheminer les données entre le réseau local et le réseau public.
- **Câbles et connecteurs** : les câbles et les connecteurs sont utilisés pour connecter les appareils clients et les équipements de réseau. Les types de câbles et de connecteurs les plus courants sont les câbles Ethernet et les connecteurs RJ45.

Types de réseaux

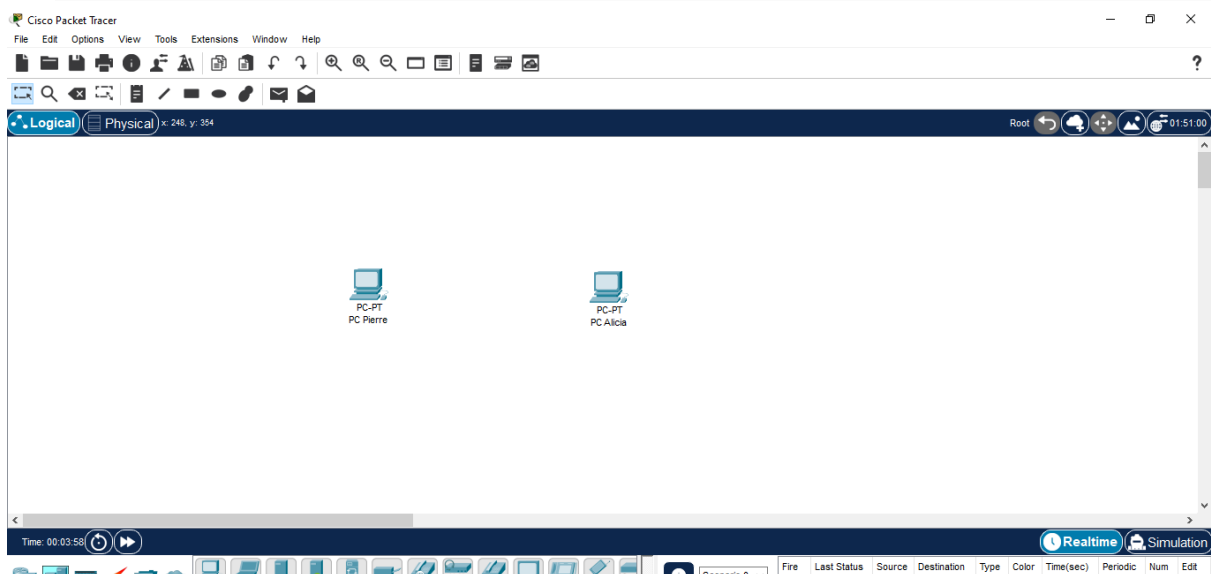
Il existe différents types de réseaux informatiques, en fonction de leur taille, de leur portée et de leur utilisation. Les principaux types de réseaux informatiques sont les suivants :

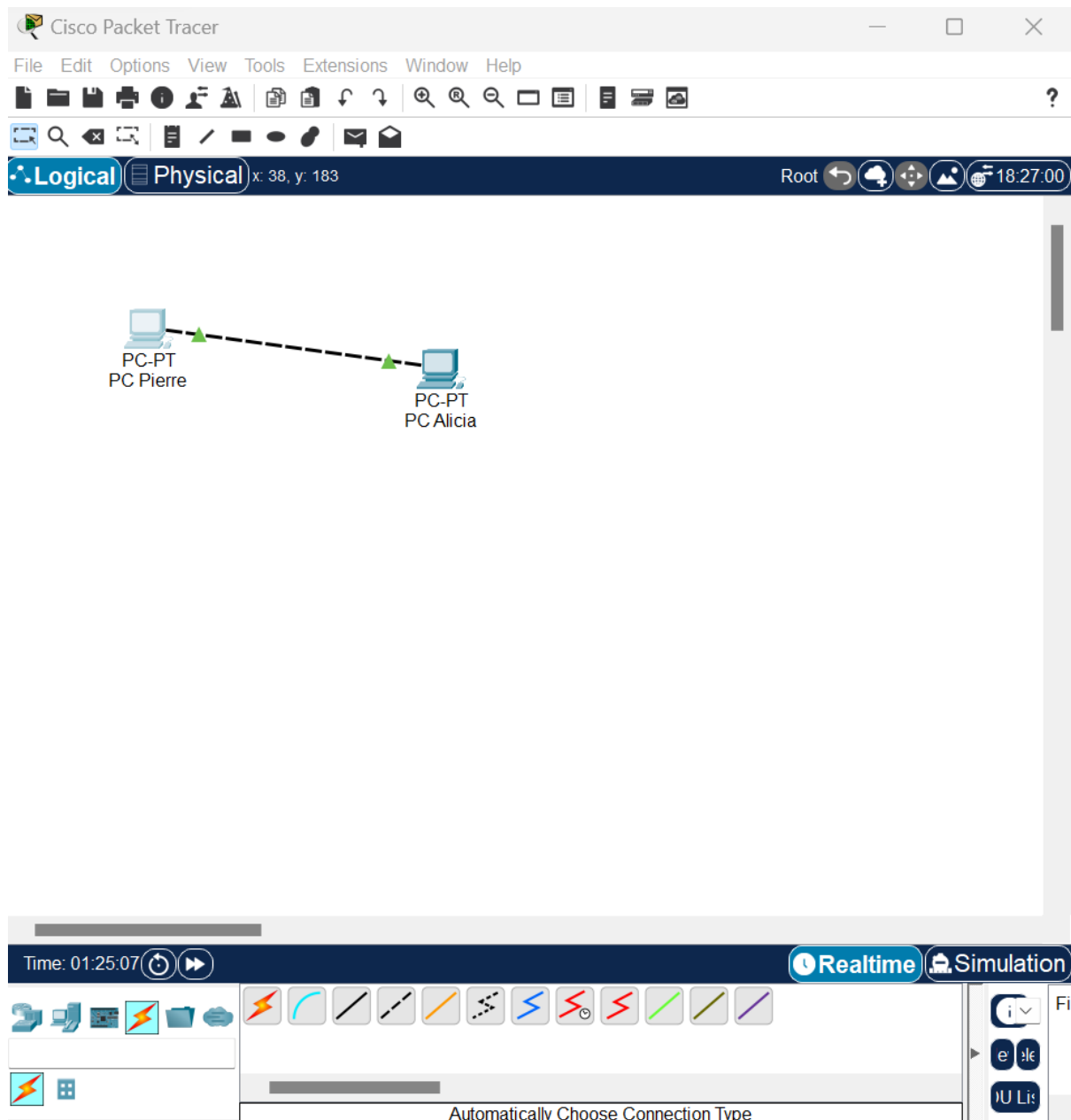
- **Réseau local (LAN)** : un LAN est un réseau informatique qui couvre une zone géographique restreinte, telle qu'un bureau, une maison ou une usine.
- **Réseau métropolitain (MAN)** : un MAN est un réseau informatique qui couvre une zone géographique plus large qu'un LAN, mais plus petite qu'un WAN.
- **Réseau étendu (WAN)** : un WAN est un réseau informatique qui couvre une zone géographique très large, telle qu'un pays ou un continent.

Conclusion

Les réseaux informatiques sont des outils essentiels pour la communication et la collaboration. Ils sont utilisés dans de nombreux contextes différents, tels que les entreprises, les écoles, les hôpitaux et les gouvernements

> job 03

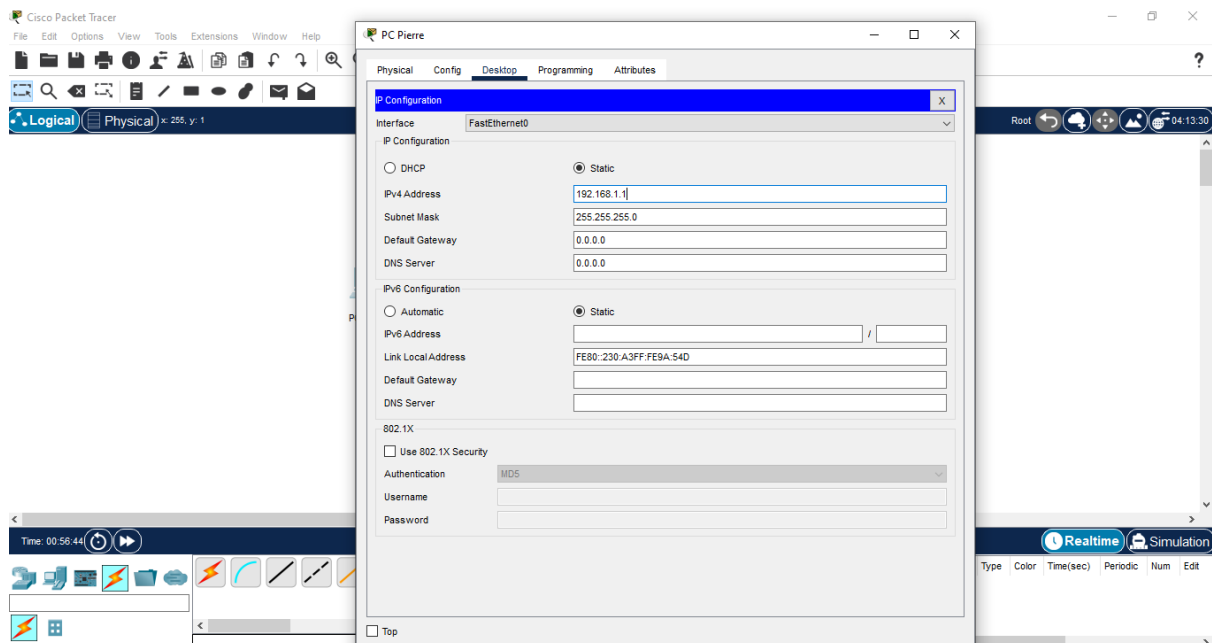


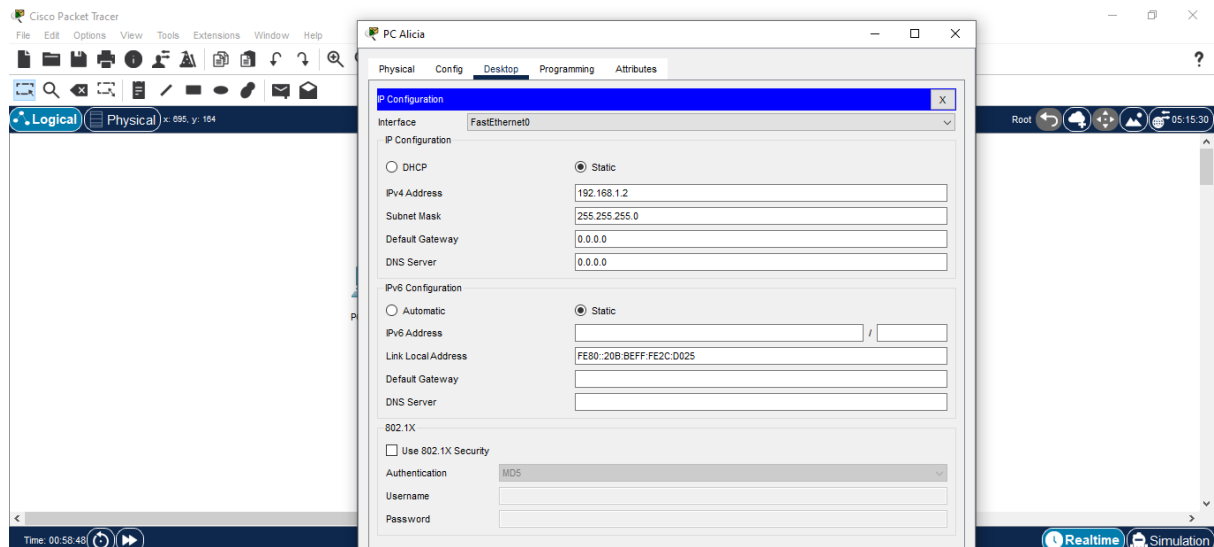


Copper Straight-Through Cable (Câble droit en cuivre) :

- **Choix expliqué :** Les câbles droits en cuivre, couramment désignés sous le nom de "câbles Ethernet" standard, sont conçus pour connecter un ordinateur à un commutateur, un routeur, ou un autre dispositif réseau similaire. Dans le cas de la connexion entre deux ordinateurs, un câble droit en cuivre est approprié.
- **Compatibilité :** Les câbles droits sont utilisés pour connecter des dispositifs de types différents, comme un ordinateur à un commutateur, ce qui est
- typique dans un réseau local ("Fast Ethernet"). Ils permettent une connexion directe sans avoir besoin d'un câble croisé, car les ordinateurs modernes et les équipements réseau peu
- vent détecter automatiquement la configuration

➤ job 04





Qu'est-ce qu'une adresse IP ?

Une adresse IP est un numéro unique attribué à chaque appareil connecté à un réseau informatique. L'adresse IP permet aux appareils de communiquer entre eux en identifiant de manière unique chaque appareil.

À quoi sert un IP ?

Les adresses IP servent à plusieurs fins, notamment :

- Identifier de manière unique chaque appareil : l'adresse IP permet aux appareils de communiquer entre eux en identifiant de manière unique chaque appareil.
- Faciliter le routage des données : l'adresse IP est utilisée par les routeurs pour déterminer l'itinéraire le plus efficace pour acheminer les données entre deux appareils.
- Assurer la sécurité : l'adresse IP peut être utilisée pour identifier la localisation d'un appareil, ce qui peut être utilisé à des fins de sécurité.

Qu'est-ce qu'une adresse MAC ?

Une adresse MAC est un numéro unique attribué à chaque carte réseau. L'adresse MAC est utilisée pour identifier de manière unique chaque carte réseau.

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

Les adresses IP sont divisées en deux catégories : les adresses IP publiques et les adresses IP privées.

- Les adresses IP publiques sont des adresses IP qui sont visibles sur Internet. Les adresses IP publiques sont attribuées par les fournisseurs d'accès Internet (FAI).
- Les adresses IP privées sont des adresses IP qui ne sont pas visibles sur Internet. Les adresses IP privées sont utilisées pour les réseaux locaux (LAN).

Exemples d'adresses IP

Voici quelques exemples d'adresses IP :

- Adresse IP publique : 192.168.1.1
- Adresse IP privée : 10.0.0.1

Conclusion

Les adresses IP sont des éléments essentiels des réseaux informatiques. Elles permettent aux appareils de communiquer entre eux et de faciliter le routage des données.

- Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau est 192.168.1.1. Cette adresse est une adresse IP privée, ce qui signifie qu'elle n'est pas visible sur Internet. L'adresse IP publique de ce réseau est attribuée par le fournisseur d'accès Internet (FAI).

➤ job 05

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::230:A3FF:FE9A:54D
    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::20B:BEFF:FE2C:D025
    IPv6 Address...: ::
    IPv4 Address...: 192.168.1.2
    Subnet Mask...: 255.255.255.0
    Default Gateway...: ::
                        0.0.0.0

Bluetooth Connection:

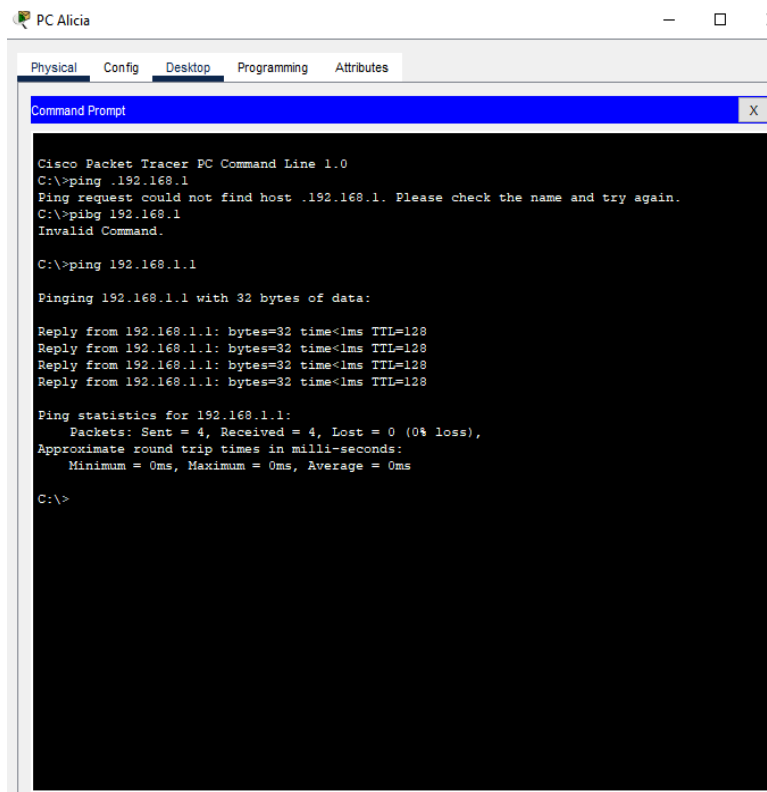
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address...: ::
    IPv6 Address...: ::
    IPv4 Address...: 0.0.0.0
    Subnet Mask...: 0.0.0.0
    Default Gateway...: ::
                        0.0.0.0

C:\>|
```


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

jai utilisee la commande

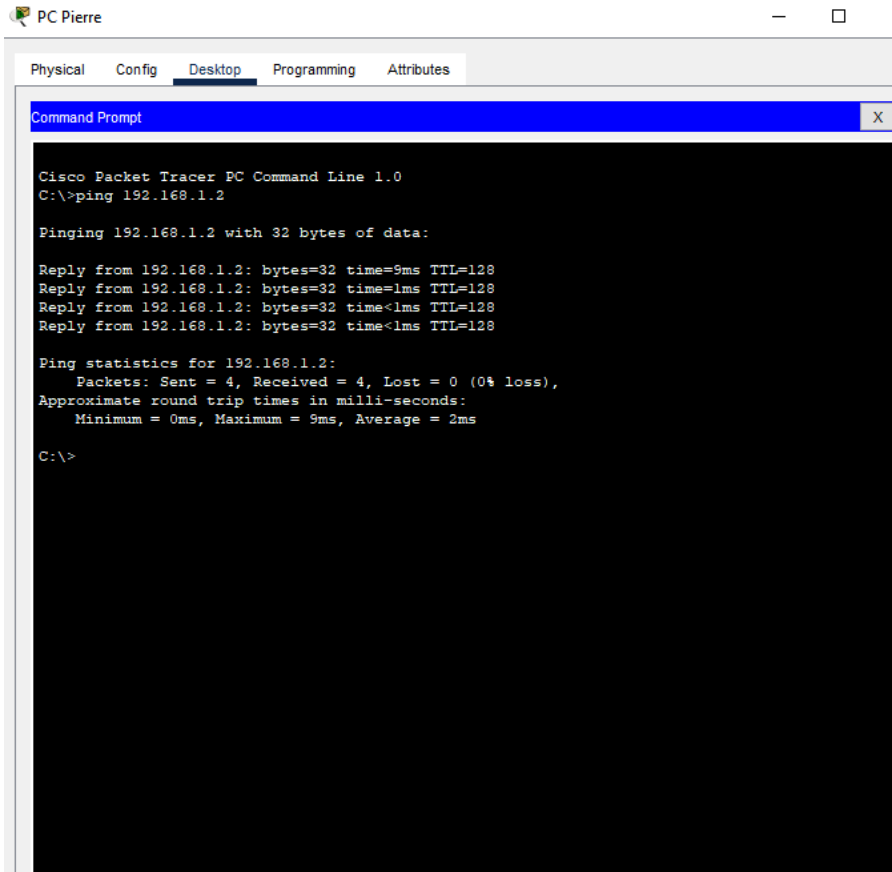
```
Cisco Packet Tracer PC Command Line 1.0  
C:\>ipconfig
```



The screenshot shows a window titled "PC Alicia" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0  
C:\>ping .192.168.1  
Ping request could not find host .192.168.1. Please check the name and try again.  
C:\>pihg 192.168.1  
Invalid Command.  
  
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<1ms 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 = 0ms, Average = 0ms  
  
C:\>
```

job 06



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
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=9ms 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 = 9ms, Average = 2ms

C:\>
```

Quelle est la commande permettant de Ping entre des PC ?

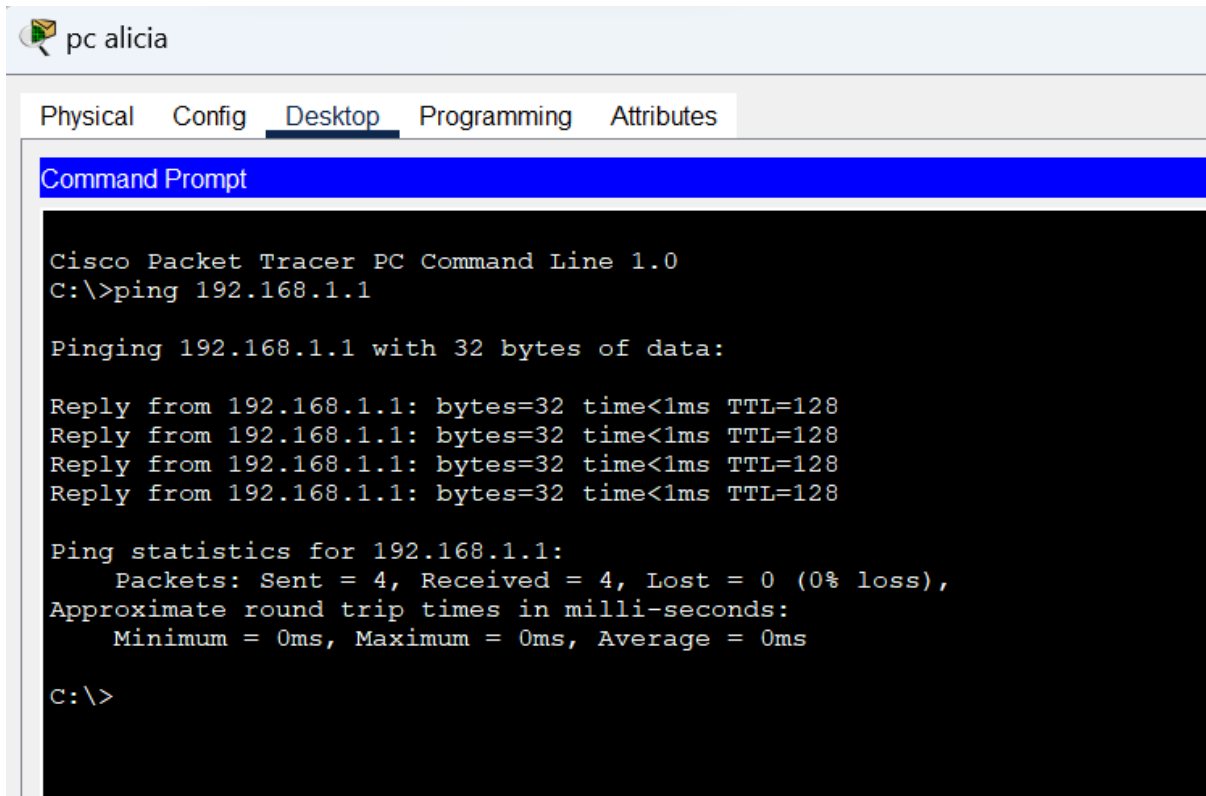
la commande de ping entre deux PC = `ping 192.168.1.x`

x= le pc que te vais ping exemple pc Pierre 192.168.1.1 et pc Alicia 192.168.1.2

➤ job 07

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

→ Expliquez pourquoi



```
pc alicia
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
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<1ms 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 = 0ms, Average = 0ms

C:\>
```

oui le pc de pierre a reçu les paquets envoyé par alicia parce-qu'il est déjà connecté dans un seul réseau donc ils sont liés

➤ job 08

R.Q1: Le switch quant à lui est traduit en français comme étant « commutateur ».

C'est un appareil qui permet de relier plusieurs fragments de réseau informatique entre eux. Cet équipement fonctionne comme un pont de liaison.

-Le hub est un mot anglais qui en français est traduit par : « concentrateur ». Le concentrateur est donc défini dans le cadre de l'informatique, comme étant un appareil reliant plusieurs machines. Il a pour rôle de concentrer les données afin de les transmettre dans un seul canal

R.Q2: La technologie qui se cache derrière les hubs est donc considérée comme étant vulnérable et obsolète. En plus de la perte de vitesse mentionnée ci-dessus et du manque de flexibilité relatif au transfert de données et à la sélection des récepteurs, un système de hubs est souvent assez vulnérable face aux failles de sécurité. Comme un tel système ne peut être mis en quarantaine, le trafic de données n'est pas protégé. Les potentiels problèmes de sécurité ou les éventuelles préoccupations liées à la protection des données concernent forcément tous les hôtes connectés.

-Le hub, ou concentrateur, est un composant clé de la plupart des réseaux informatiques. Il a pour fonction principale de relier des appareils entre eux afin

de leur permettre de communiquer. En tant que tel, son rôle est d'accroître la connectivité et la performance de l'ensemble des réseaux. Dans cet article, nous allons examiner en détail le rôle et l'utilité d'un hub, et comment il peut améliorer les performances des réseaux

R.Q3:

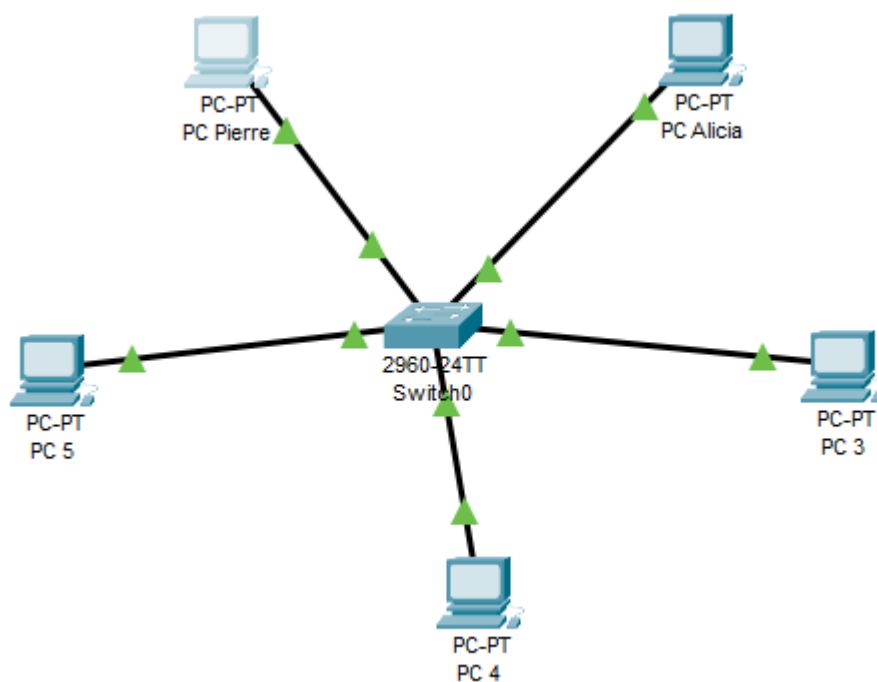
Avantages des Switchs :

1. **Augmente la capacité –**
Ils augmentent la capacité de transfert de données accessible de l'organisation.
2. **Réduit la charge –**
Ils aident à réduire la charge exceptionnelle sur les ordinateurs hôtes individuels.
3. **Incrémenter la présentation –**
Ils incrémentent la présentation de l'organisation.
4. **Moins d'impacts sur le boîtier –**
Les réseaux qui utilisent des commutateurs auront moins d'impacts sur le boîtier. Cela est dû à la façon dont les commutateurs créent des zones d'impact pour chaque association.
5. **Simple –**
Les commutateurs peuvent être directement associés aux postes de travail.
6. **Augmente la bande passante –**
Il augmente la bande passante disponible du réseau.
7. **Moins de collisions de trames –**
Les réseaux qui utilisent des commutateurs auront moins de collisions de trames
8. **Plus sécurisé –**
Étant donné que le commutateur est isolé, les données n'iront qu'à la destination

-Inconvénients des switchs :

1. **Coûteux –**
Ils sont plus coûteux que les étendues de réseau.
2. **Problèmes de disponibilité difficiles –**
Les problèmes de disponibilité du réseau sont difficiles à suivre via le changement d'organisation.
3. **Problèmes de diffusion du trafic –**
Le trafic de diffusion peut être problématique.
4. **Sans défense –**
Si les commutateurs sont en mode aveugle, ils sont sans défense contre les attaques de sécurité, par exemple la caricature d'adresse IP ou la capture de contours Ethernet.
5. **Nécessité d'une planification appropriée –**
Une planification et un agencement appropriés sont nécessaires pour traiter les colis multidiffusion.
6. **Les composants mécaniques peuvent s'user –**
Les composants mécaniques du commutateur peuvent s'user avec le temps.
7. **Le contact physique est obligatoire –**
Doit avoir un contact physique avec l'objet à actionner.

R.Q4: Le switch réseau est une sorte d'agent chargé de diriger le trafic dans la bonne direction. Pour faire simple, si un appareil essaie de récupérer des données depuis une autre source, le switch vérifiera s'il connaît cette destination. Dans la négative, il enverra les données à un autre appareil comme un routeur pour laisser ce dernier gérer



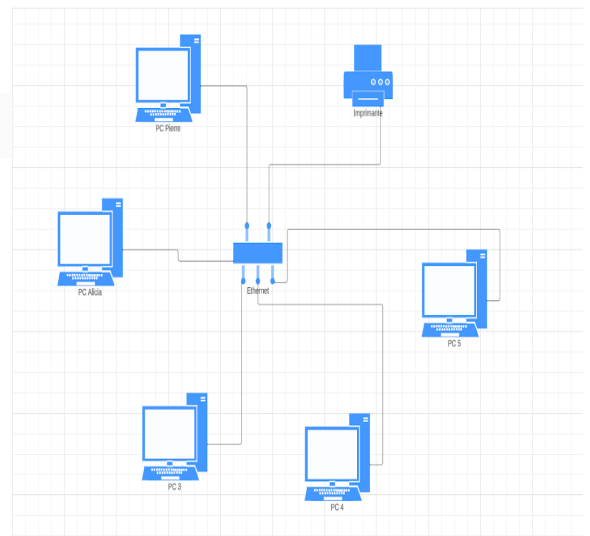
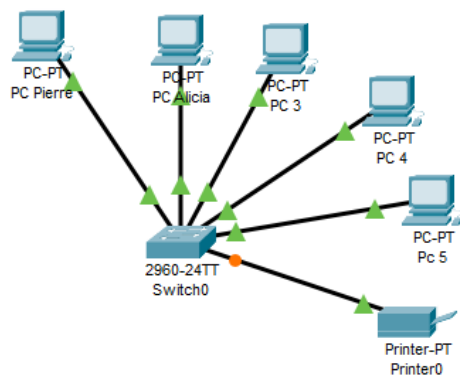
```

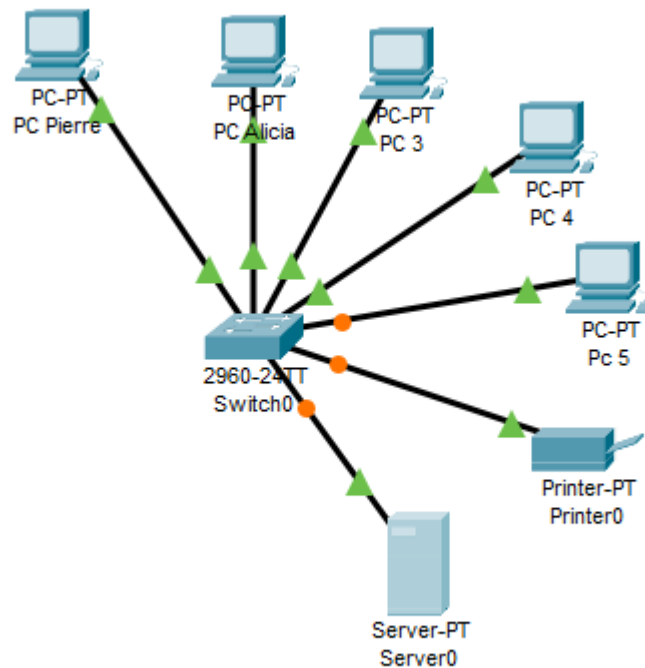
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
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<1ms 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 = 1ms, Average = 0ms
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 = 1ms, Average = 0ms
C:\>

```

> job 09

Le schéma est un outil pédagogique efficace pour favoriser l'apprentissage





R.Q1: La différence fondamentale entre les adresses IP statiques et dynamiques est que l'adresse IP statique est une adresse fixe attribuée manuellement à un périphérique par un administrateur réseau, tandis qu'une adresse IP dynamique est une adresse attribuée automatiquement à un périphérique par un serveur DHCP

➤ job 11

R.Q1: L'adresse IP 10.0.0.0 avec un masque de sous-réseau de /8 (255.0.0.0 en notation décimale) correspond à une plage d'adresses de classe A. Cependant, ce n'est pas nécessairement une classe A au sens strict. Elle est souvent utilisée comme adresse privée (adresse RFC 1918) dans les réseaux locaux et n'est pas soumise aux mêmes règles de distribution que les adresses de classe A attribuées par l'Internet Assigned Numbers Authority (IANA).

R.Q2: Il est important de noter que l'utilisation des classes A, B et C est devenue moins courante en raison de la notation CIDR (Classless Inter-Domain Routing), qui permet une découpe plus flexible des adresses IP en utilisant des masques de sous-réseau de longueur variable. Cette approche permet une gestion plus efficace des adresses IP en fonction des besoins spécifiques du réseau, sans se conformer strictement aux anciennes classes de réseau. Les classes D et E sont réservées à des

utilisations particulières et ne sont pas utilisées pour la configuration standard des réseaux.

12 hôtes	10.0.0.2 a 10.0.0.13
30 hôtes	10.1.0.1 a 10.1.0.30
30 hôtes	10.2.0.1 a 10.2.0.30
30 hôtes	10.3.0.1 a 10.3.0.30
30 hôtes	10.4.0.1 a 10.4.0.30
30 hôtes	10.5.0.1 a 10.5.0.30
120 hôtes	10.6.0.1 a 10.6.0.120
120 hôtes	10.7.0.1 a 10.7.0.120
120 hôtes	10.8.0.1 a 10.8.0.120
120 hôtes	10.9.0.1 a 10.9.0.120
120 hôtes	10.10.0.1 a 10.10.0.120
160 hôtes	10.11.0.1 a 10.11.0.160
160 hôtes	10.12.0.1 a 10.12.0.160
160 hôtes	10.13.0.1 a 10.13.0.160
160 hôtes	10.14.0.1 a 10.14.0.160
160 hôtes	10.15.0.1 a 10.15.0.160

➤ job 12

couche physique	-Elle a pour rôle de transmettre des signaux électriques ou optiques entre les ordinateurs. La couche physique met à disposition des autres couches les informations nécessaires à une connexion fluide	
------------------------	---	--

couche de liaison de données	<ul style="list-style-type: none">-La couche liaison est chargée de découper les données reçues par la couche supérieure , qui seront ensuite transmises à la couche physique.-Cette couche utilise pour cela différents protocoles, dont le protocole Ethernet,	
couche réseau	<ul style="list-style-type: none">-La « couche réseau » est la partie du processus de communication Internet où ces connexions se produisent, en envoyant des paquets de données dans les deux sens entre différents réseaux.	
couche transporteuse	<ul style="list-style-type: none">-La couche transport OSI récupère les données de la couche session et transfère celles-ci à la couche réseau. La couche transport garantit la communication sécurisée et transparente entre deux systèmes. Elle peut décomposer les paquets et gérer la vitesse du transfert.	
couche session	<ul style="list-style-type: none">-La couche session permet de coordonner la connexion et la libération des connexions de dialogue entre les applications communicantes. Elle communique avec la couche transport. La communication peut être de type un à un, plusieurs à un et un à plusieurs. Dans le cas d'une communication un à un, une connexion de la couche session est établie pour chaque connexion de la couche transport.	
couche de présentation		

couche d'application		

➤ job 13

R.Q1: L'architecture de ce réseau semble assez simple et en forme d'étoile . Tous les périphériques ont des adresses IP appartenant au même sous-réseau, et ils utilisent un masque de sous-réseau de 255.255.255.0 .

R.Q2: normalement l'adresse IP du réseau est 192.168.10.0

R.Q3: normalement on peut brancher 256 machine parce-qu'on a 256 adresse IP et on commence de 0 et on arrête à 255

R.Q4: l'adresse IP de diffusion de ce réseau est 192.168.10.255

➤ job 14

-145.32.59.24:

10010001.00100000.00111011.00011000

-200.42.129.16:

11001000.00101010.10000001.00010000

-14.82.19.54:

00001110.01010010.00010011.00110110

➤ job 15

Q1: Le routage réseau est le processus de sélection d'un chemin à travers un ou plusieurs réseaux. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP pour se rendre de leur origine à leur destination. Ces décisions de routage Internet sont prises par des périphériques réseau spécialisés appelés routeurs.

Q2: Gateway est un dispositif permettant de relier deux réseaux informatiques différents, comme par exemple un réseau local et l'Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à l'Internet par l'intermédiaire de la passerelle. Le plus souvent, elle sert aussi de pare-feu, ce qui permet de contrôler tous les transferts de données entre le local et l'extérieur.

Q3: VPN 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.

Q4: Le système de noms de domaine (DNS, Domain Name System) est la méthode par laquelle une adresse IP (Internet Protocol), un ensemble de chiffres (173.194.39.78), est convertie sur un ordinateur ou un autre dispositif connecté en un nom de domaine lisible par l'homme, tel que www.google.com.