

PROJET : RUNTRACK RÉSEAU

Sommaire :

Job 1.....1

Job 2.....1

Job 3.....2

Job 4.....3

Job 5.....4

Job 6.....5

Job 7.....6

Job 8.....6

Job 9.....8

Job 10.....8

Job 11.....9

Job 12.....12

Job 13.....13

Job 14.....13

Job 15.....14

## Job 1

Installation de **Cisco Packet Tracer** via le lien : <https://www.netacad.com/portal/node/488>



## Job 2

### I/ Qu'est-ce qu'un réseau ?

Un **réseau** est un **ensemble de dispositifs** (ex : entités, systèmes, etc...) interconnectés qui **permettent de communiquer des informations ou des ressources** entre eux. Ces dispositifs peuvent être par exemple, des ordinateurs, des serveurs ou un ensemble de personnes.

### II/ À quoi sert un réseau informatique ?

Un **réseau informatique** est défini par **plusieurs dispositifs informatiques interconnectés grâce à un câble ou sans fil afin de communiquer, partager des informations ou des ressources** (par exemple : 2 ordinateurs reliés entre eux peuvent partager un espace de stockage).

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

Afin de construire un réseau informatique nous allons avoir besoin de **différents composants** :



D'**ordinateurs** équipés d'une carte Ethernet ou wifi afin qu'il puissent se connecter au réseau informatique.



Un **modem** (abréviation de modulateur et démodulateur) est délivré par un fournisseur d'accès (par exemple, Orange, SFR, Bouygues Telecom, etc...) et va **fournir la connexion au réseau Internet**.



Un **routeur** est relié au modem et permet de **connecter tous les dispositifs informatiques au réseau internet** fourni par le modem via un réseau wifi. La plupart des routeurs peuvent analyser les informations grâce à un pare-feu.



Un **switch** ou **commutateur** est un boîtier équipé de ports Ethernet qui permet de **connecter plusieurs appareils ou réseaux informatiques à un même réseau** et ainsi assurer la communication, la réception et la redistribution d'informations entre les différents dispositifs informatiques qui sont reliés au même réseau.



Un **pare-feu** (ou firewall) est un **appareil ou logiciel de protection qui permet de contrôler les informations entrantes et sortantes** qui circulent entre les réseaux internes (ex : ordinateurs) et les réseaux externes (ex : internet) en autorisant ou en bloquant ces informations. Certains routeurs sont dotés de pare-feu.



Un **serveur informatique** est un système qui peut être matériel (hardware), logiciel (software) ou virtuel (via un hyperviseur), celui-ci **fournit des données, programmes, et services** (par exemple : stockage, programme de messagerie électronique, hébergement d'un site web) **à des dispositifs informatiques appelés "clients"** et qui sont accessibles via un réseau internet ou intranet.



Des **câbles réseau** ou câbles Ethernet (ex : câble RJ45, câble coaxial) sont spécialement conçus pour différents dispositifs informatiques et **permettent la transmission de données et de signaux au sein d'un réseau**. Ils sont essentiels pour établir des connexions filaires fiables entre les ordinateurs, les serveurs, les routeurs, les commutateurs, et d'autres équipements réseau.

## Job 3

Afin de relier le PC Pierre et le PC Alicia, j'ai choisi le **câble croisé** car celui-ci est conçu pour **relier deux dispositifs du même type** (dans notre cas les deux dispositifs à relier sont deux ordinateurs).

## Job 4

### I/ Qu'est-ce qu'une adresse IP ?

L'**adresse IP** (abréviation de "Internet Protocol") est une **série de chiffres qui permet l'identification** de chaque appareil (ex : ordinateur, tablette, smartphones, etc...) connecté au réseau internet.

### II/ À quoi sert un IP ?

Le **réseau IP** est défini par un **ensemble de dispositifs informatiques connectés via leur adresse IP**. Celui-ci permet aux différents dispositifs d'un même réseau de **communiquer et d'échanger des données** en toute sécurité.

### III/ Qu'est ce qu'une adresse MAC ?

L'**adresse MAC** (acronyme de "Media Access Control") est également appelée adresse physique ou adresse matérielle. Celle-ci permet d'**identifier un équipement réseau** grâce une série de douze caractères alphanumériques attribuée par le constructeur. Elle est **unique** pour chaque équipement.

### IV/ Qu'est-ce qu'une IP publique et privée ?

- L'adresse IP **publique** est attribuée par un fournisseur d'accès à Internet (FAI) et est utilisée pour **identifier un appareil sur Internet**.
- L'adresse IP **privée** est attribuée par le routeur dans un **réseau local** ou LAN (par exemple dans un domicile ou dans une entreprise). Elle permet d'**identifier les appareils qui y sont connectés**.

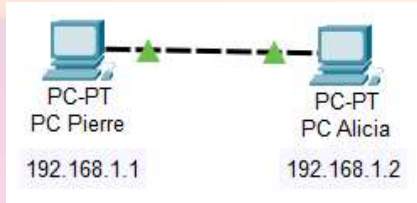
### V/ Quelle est l'adresse de ce réseau ?

Afin d'obtenir l'**adresse d'un réseau**, il suffit de **remplacer le dernier chiffre de l'adresse ip d'un équipement relié au réseau par le dernier chiffre du masque sous-réseau**.

Dans notre cas : Adresse IP de PC Pierre : **192.168.1.1**  
Masque de sous-réseau : **255.255.0.0**

L'adresse de ce réseau est donc : **192.168.1.0**

Réseau :



## Job 5

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

Nous allons utiliser la commande **ipconfig** afin de vérifier l'adresse IP des PC de Pierre et d'Alicia :

PC de Pierre :

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

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:17FF:FEE3:3974
    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
```

PC d' Alicia :

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

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::260:2FFF:FE89:9A65
    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
```

## Job 6

### I/ Quelle est la commande permettant de Ping entre des PC ?

Pour effectuer un ping entre des PC, il faut utiliser la commande **ping** suivie de l'adresse IP du PC de destination.

- ❖ Adresse IP PC de Pierre : **192.168.1.1**
- ❖ Adresse IP PC d'Alicia : **192.168.1.2**

Ping à partir du PC de Pierre vers le PC d'Alicia :

```
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=2ms 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 = 2ms, Average = 0ms

C:\>
```

Ping à partir du PC d'Alicia vers le PC de 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<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:\>
```

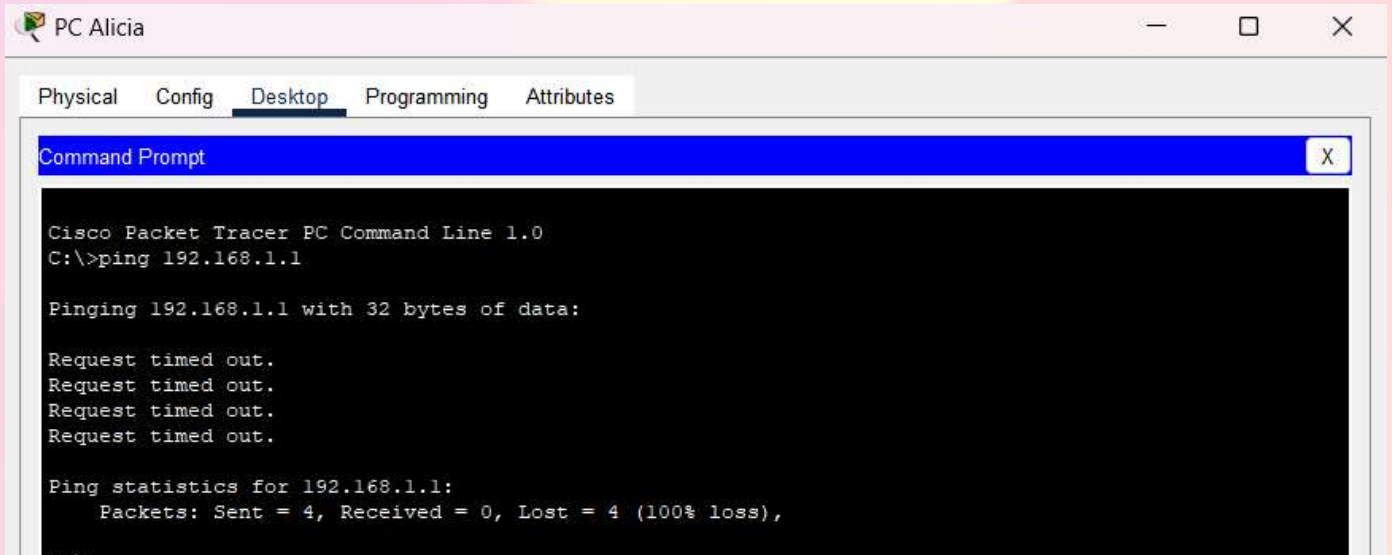


## Job 7

### I/ 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 via la commande **ping** car celle-ci ne fonctionne que si l'ordinateur destination est actif et connecté au réseau.

Ping effectué à partir de l'ordinateur d'Alicia vers le PC de Pierre (qui est éteint) :



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

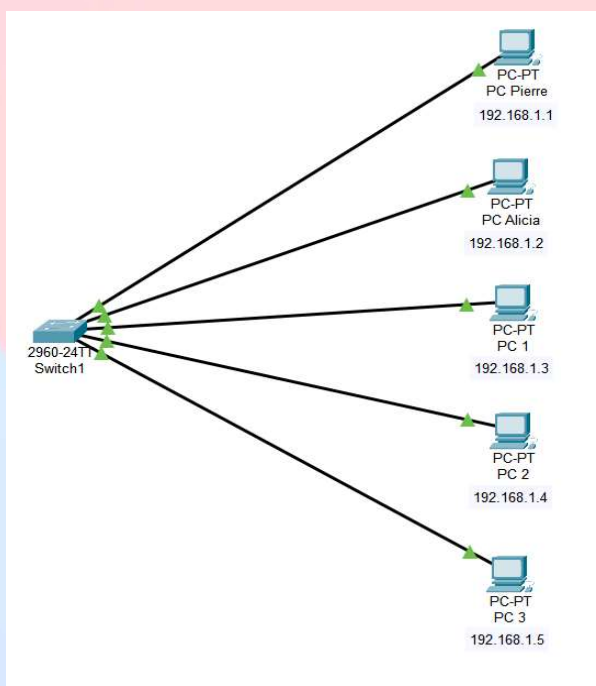
Pinging 192.168.1.1 with 32 bytes of data:

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

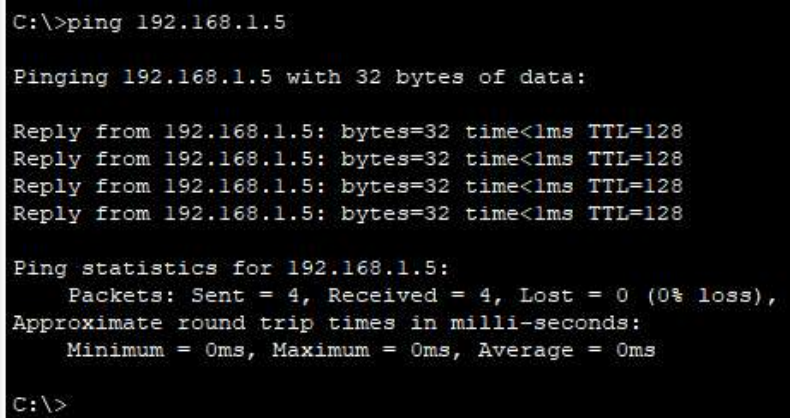
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

## Job 8

Sous réseau :



Ping à partir du PC de Pierre vers PC 3 :



```
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:\>
```

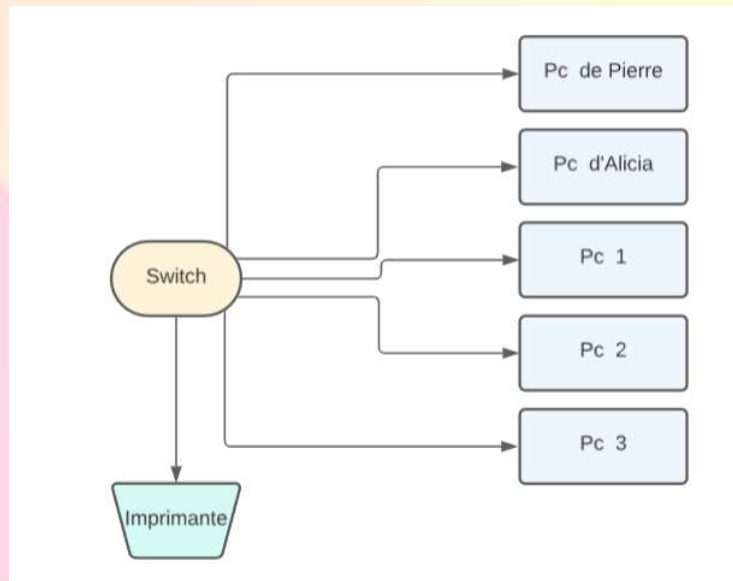
**I/ Quelle est la différence entre un hub et un switch, quels sont leurs avantages et inconvénients ?**

	HUB	SWITCH
FONCTIONNEMENT	Le hub reçoit un paquet de données d'un port et le <b>transmet à tous les autres ports, sans prendre en compte l'adresse de destination</b> . Cela signifie que toutes les machines connectées à un hub reçoivent toutes les données.	Le switch examine l'adresse MAC de destination de chaque paquet de données et les <b>transmet uniquement vers le port où se trouve la machine cible</b> .
EFFICACITÉ	Le hub <b>peut générer beaucoup de trafic inutile sur le réseau</b> , ce qui peut entraîner un encombrement et une <b>performance médiocre, en particulier dans des réseaux avec un grand nombre de machines</b> .	Le switch est <b>beaucoup plus efficace</b> car il <b>filtre le trafic</b> et ne l'envoie qu'aux machines cibles. Cela <b>améliore considérablement la performance du réseau</b> en réduisant la charge inutile.
SÉCURITÉ	Il est <b>difficile de sécuriser le trafic</b> sur un réseau hub, car <b>toutes les machines connectées à un hub reçoivent les mêmes données</b> donc toute machine peut potentiellement intercepter des données destinées à d'autres.	Un switch <b>offre une meilleure sécurité</b> , car il isole le trafic entre les machines. Les <b>données sont acheminées uniquement vers le port approprié</b> , réduisant ainsi le risque d'interception par des dispositifs non autorisés.
COÛT	Le hub est généralement <b>moins cher</b> que le switch <b>en raison de sa simplicité</b> . Cependant, son utilisation devient de plus en plus rare dans les réseaux modernes en raison des inconvénients qu'il présente.	Le switch est <b>plus coûteux</b> , mais il est largement utilisé dans les réseaux modernes <b>en raison de son efficacité</b> et de sa capacité à gérer de manière optimale le trafic.



## Job 9

Schéma du réseau :



Réaliser le schéma de notre réseau présente **plusieurs avantages** :

- Il permet de visualiser la structure du réseau, ce qui **facilite la compréhension** de son fonctionnement.
- Une meilleure compréhension du réseau permet également de **mieux sécuriser le réseau** en identifiant efficacement les problèmes et/ou risques potentiels.
- Une documentation de la structure permet de **faciliter la planification de l'amélioration ou la modification du réseau** en identifiant les futurs besoins et ressources nécessaires (ex : mises à jour de certaines machines).

## Job 10

### I/ Quelle est la différence entre une adresse IP statique et une adresse IP attribuée par DHCP ?

L'**adresse IP fixe** est configurée **manuellement par l'administrateur réseau** sur les dispositifs du réseau. Chaque dispositif possède une adresse IP fixe qui ne change pas, sauf si l'administrateur modifie celle-ci.

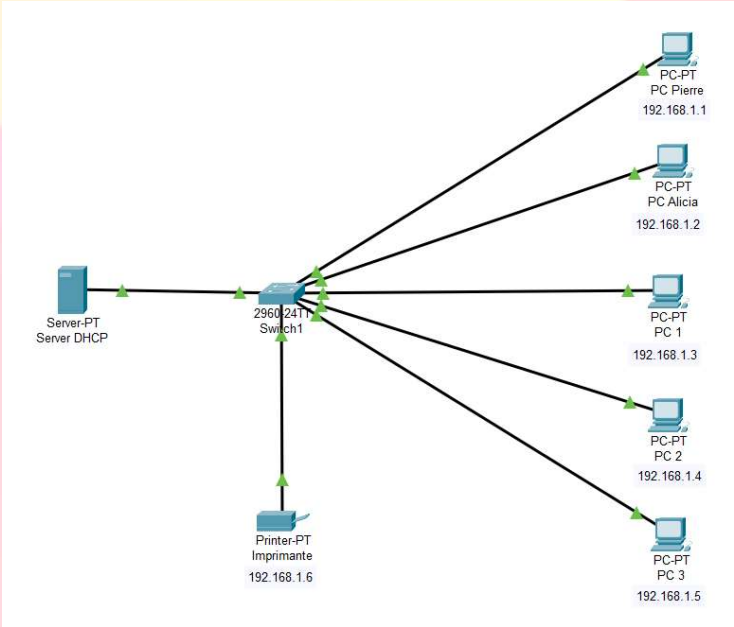
Les adresses IP statiques sont **stables et prévisibles**. Chaque dispositif a toujours la même adresse IP, ce qui **facilite la gestion et le dépannage**.

Cependant, **la gestion des adresses IP statiques peut devenir complexe** à mesure que le réseau grandit. L'administrateur réseau doit s'assurer qu'il n'y a pas de conflits d'adresses IP.

Le **DHCP attribue automatiquement des adresses IP aux dispositifs du réseau** au moment de leur connexion. Chaque dispositif reçoit une adresse IP à partir d'un pool d'adresses géré par le serveur DHCP.

L'utilisation du DHCP **simplifie la gestion des adresses IP** et est conçue pour éviter les conflits d'adresses IP en surveillant les adresses déjà attribuées et en attribuant uniquement des adresses non utilisées.

Réseau avec un serveur DHCP :



## Job 11

❖ 1 sous réseau de 12 hôtes :

Pool d'adresses IP	Masque sous réseau	Adresse réseau	Adresse de diffusion	Nombre d'hôtes
10.0.0.1 - 10.0.0.14	255.255.255.240	10.0.0.0	10.0.0.15	$2^4 - 2$ (adresse réseau + adresse diffusion) = 16 - 2 = <b>14</b>

❖ 5 sous réseau de 30 hôtes :

Sous réseaux	Pool d'adresses IP	Masque sous réseau	Adresse réseau	Adresse de diffusion	Nombre d'hôtes
<b>Sous réseau 1</b>	10.0.0.17 - 10.0.0.46	255.255.255.224	10.0.0.16	10.0.0.47	$2^5 - 2$ (adresse réseau + adresse diffusion) = 32 - 2 = <b>30</b>
<b>Sous réseau 2</b>	10.0.0.49 - 10.0.0.78	255.255.255.224	10.0.0.48	10.0.0.79	<b>30</b>
<b>Sous réseau 3</b>	10.0.0.81 - 10.0.0.110	255.255.255.224	10.0.0.80	10.0.0.111	<b>30</b>
<b>Sous réseau 4</b>	10.0.0.113 - 10.0.0.142	255.255.255.224	10.0.0.112	10.0.0.143	<b>30</b>
<b>Sous réseau 5</b>	10.0.0.145 - 10.0.0.174	255.255.255.224	10.0.0.144	10.0.0.175	<b>30</b>

❖ 5 sous réseau de 120 :

Sous réseaux	Pool d'adresses IP	Masque sous réseau	Adresse réseau	Adresse de diffusion	Nombre d'hôtes
<b>Sous réseau 1</b>	10.0.0.177 - 10.0.1.46	255.255.255.128	10.0.0.176	10.0.1.47	$2^7 - 2$ (adresse réseau + adresse de diffusion) = 128 - 2 = <b>126</b>
<b>Sous réseau 2</b>	10.0.1.49 - 10.0.1.174	255.255.255.128	10.0.1.48	10.0.1.175	<b>126</b>
<b>Sous réseau 3</b>	10.0.1.177 - 10.0.2.46	255.255.255.128	10.0.1.176	10.0.2.47	<b>126</b>
<b>Sous réseau 4</b>	10.0.2.49 - 10.0.2.174	255.255.255.128	10.0.2.48	10.0.2.175	<b>126</b>
<b>Sous réseau 5</b>	10.0.2.177 - 10.0.3.46	255.255.255.128	10.0.2.176	10.0.3.47	<b>126</b>

## ❖ 5 sous réseau de 160 :

Sous réseaux	Pool d'adresses IP	Masque sous réseau	Adresse réseau	Adresse de diffusion	Nombre d'hôtes
Sous réseau 1	10.0.3.49 - 10.0.4.46	255.255.255.1	10.0.3.48	10.0.4.47	$2^8 - 2$ (adresse réseau + adresse de diffusion) = 256 - 2 = <b>254</b>
Sous réseau 2	10.0.4.49 - 10.0.5.46	255.255.255.1	10.0.4.48	10.0.5.47	<b>254</b>
Sous réseau 3	10.0.5.49 - 10.0.6.46	255.255.255.1	10.0.5.48	10.0.6.47	<b>254</b>
Sous réseau 4	10.0.6.49 - 10.0.7.46	255.255.255.1	10.0.6.48	10.0.7.47	<b>254</b>
Sous réseau 5	10.0.7.49 - 10.0.8.46	255.255.255.1	10.0.7.48	10.0.8.47	<b>254</b>

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

Le choix d'une adresse de classe A (contrairement à une adresse de classe B ou C) repose sur **la large plage d'adresses IP** (de 0.0.0.0 à 127.255.255.255) qu'elle peut offrir, ce qui signifie qu'elle peut **détenir un grand nombre d'adresses IP**. Cela permet d'apporter de la flexibilité pour créer des sous-réseaux et segmenter un réseau interne, mais également une gestion plus simple des adresses IP.

### II/ Quelle est la différence entre les différents types d'adresses ?

#### ➤ Les adresses de classe A :

Comme cité précédemment, les adresses de classe A sont **conçues pour prendre en charge de très grands réseaux avec un grand nombre d'hôtes**. Celles-ci sont utilisées par de grandes organisations ou entreprises à l'échelle mondiale.

#### ➤ Les adresses de classe B :

Les adresses de classe B **conviennent aux réseaux de taille moyenne avec un nombre modéré d'hôtes**. Celles-ci sont utilisées par des organisations de taille moyenne.

#### ➤ Les adresses de classe C :

Les adresses de classe C sont destinées à de **petits réseaux**, tels que des réseaux domestiques ou de petites entreprises. Celles-ci sont courantes pour les petits réseaux locaux (LAN) et les réseaux domestiques.

## Job 12

### Modèle OSI

Couches	Description	Matériels/Protocoles
1. Physique	Responsable de l' <b>équipement qui facilite le transfert des données</b> , comme les câbles et les routeurs installés sur le réseau.	<ul style="list-style-type: none"><li>• Câble RJ45</li><li>• Fibre optique</li></ul>
2. Liaison des données	Responsable du <b>transfert des informations sur le même réseau</b> et les erreurs et le flux pour garantir la réussite de la transmission des données.	<ul style="list-style-type: none"><li>• Ethernet</li><li>• MAC</li><li>• PPTP</li><li>• Wi-Fi</li></ul>
3. Réseau	Responsable de <b>décomposer les données sur l'appareil de l'expéditeur et de les réassembler sur l'appareil du destinataire</b> lorsque la transmission s'effectue sur deux réseaux différents.	<ul style="list-style-type: none"><li>• IPv4</li><li>• IPv6</li><li>• PPTP</li></ul>
4. Transport	Chargée de <b>prendre les données et de les décomposer en petits morceaux</b> pour rendre les transferts plus efficaces et plus rapides.	<ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li></ul>
5. Session	Chargée d' <b>établir une connexion logique entre deux systèmes</b> . Cette connexion porte le nom de « session ». Celle-ci est unique. La couche session assure également le contrôle de ces sessions.	<ul style="list-style-type: none"><li>• SSL/TLS</li></ul>
6. Présentation	Chargée de la <b>préparation des données pour qu'elles puissent être affichées à l'utilisateur</b> . Responsable de l'encodage et du décodage des informations afin qu'elles puissent être affichées en clair.	<ul style="list-style-type: none"><li>• SSL/TLS</li></ul>
7. Application	Elle <b>communique directement avec l'utilisateur</b> . Les protocoles d'application comprennent le SMTP (Simple Mail Transfer Protocol) et le HTTP, qui est le protocole de communication entre les navigateurs et les serveurs Web.	<ul style="list-style-type: none"><li>• FTP</li><li>• HTTP</li></ul>



## Job 13

### I/ Quelle est l'architecture de ce réseau ?

Ce réseau est un **réseau en étoile** (ou hub and spoke). On le reconnaît car tous les dispositifs sont connectés à un même périphérique central : le switch.

### II/ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est : **192.168.1.0**

### III/ Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?

Toutes les machines du réseau (serveurs et PC) sont dans la plage d'adresses IP **192.168.10.0/24** (de **192.168.10.1** à **192.168.10.254**), et ils utilisent le même masque de sous-réseau (**255.255.255.0**), ce qui signifie que nous disposons de 250 adresses IP potentielles pour les futures machines (en déduisant les 4 adresses IP déjà attribuées aux PC qui sont déjà branchés au réseau).

### IV/ Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion **192.168.10.255**. Si nous envoyons un message à l'adresse de diffusion, il sera diffusé à toutes les machines du réseau.

## Job 14

### Conversion des adresses binaires en octet :

Adresse IP	Adresse IP en binaire
145.32.59.24	10010001.00100000.00111111.00011000
200.42.129.16	11001000.00101010.10000001.00010000
14.82.19.54	00001110.01010010.00010011.00110110

## Job 15

### I/ Qu'est-ce que le routage ?

Le **routage réseau** est le **processus de sélection d'un chemin à travers un ou plusieurs réseaux**. Il améliore l'efficacité des communications réseau en déterminant comment acheminer les données d'un point à un autre à travers un réseau de manière efficace et fiable. Le routage permet aux **données de circuler entre les différents périphériques** (ex : ordinateurs, routeurs, etc...).

### II/ Qu'est-ce qu'un gateway ?

Une **gateway** (ou passerelle) désigne **un dispositif matériel et logiciel qui permet de relier deux réseaux** informatiques, ou deux réseaux de télécommunications, **aux caractéristiques différentes** (ex : la box internet).

### III/ Qu'est-ce qu'un VPN ?

Un **VPN** crée une connexion réseau privée entre des appareils via Internet. Il sert à **transmettre des données de manière sûre et anonyme** sur des réseaux publics et fonctionne en **masquant les adresses IP des utilisateurs**.

### IV/ Qu'est-ce qu'un DNS ?

Les **serveurs DNS traduisent des demandes de noms en adresses IP**, en contrôlant à quel serveur un utilisateur final va se connecter quand il tapera un nom de domaine dans son navigateur. Ces **demandes sont appelées requêtes**. Ils permettent à notre **message d'atteindre son destinataire** et non quelqu'un d'autre possédant un nom de domaine similaire.