La Plateforme

Run Track Réseau

Documentation

“

Job 2:

- - - -

-Qu’est-ce qu’un réseau ?

Un réseau est un ensemble de dispositifs informatiques connectés entre eux, tels que des ordinateurs, des serveurs, des routeurs, des commutateurs, des imprimantes, etc. Ces dispositifs sont

reliés les uns aux autres par des câbles ou par des connexions sans fil, permettant ainsi le partage de ressources, d'informations et de données entre les différents membres du réseau.

-A quoi sert un réseau informatique ?

Un réseau informatique permet aux ordinateurs et autres appareils électroniques de partager des ressources, des informations et des services entre. Les utilisations les plus courantes d'un réseau sont :

- **Partage de fichier:** Les utilisateurs peuvent partager et accéder aux fichiers et aux données stockés sur d'autres ordinateurs du réseau.
- **Impression en réseau:** Plusieurs utilisateurs peuvent partager une imprimante connectée au réseau, ce qui leur permet d'imprimer des documents depuis leur propre ordinateur.
- **Accès à distance:** Les réseaux permettent aux utilisateurs de se connecter à distance à d'autres ordinateurs ou serveurs via des connexions sécurisées, ce qui facilite le travail à distance et la collaboration.
- **Communication:** Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux via des services de messagerie électronique, de chat en ligne, de vidéoconférence…
- **Accès à Internet:** Les réseaux informatiques permettent aux utilisateurs de se connecter à Internet et d'accéder à une vaste gamme de ressources en ligne,
- **Sauvegarde et récupération des données:** Les réseaux permettent de stocker des données sur des serveurs dédiés, ce qui facilite la sauvegarde régulière des données et leur récupération en cas de panne ou de perte.
- **Partage de périphériques:** Les utilisateurs peuvent partager des périphériques tels que des scanners, des caméras, des

haut-parleurs, etc., ce qui permet une utilisation plus efficace des ressources.

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

Pour construire un réseau, nous avons besoin de plusieurs éléments matériels :

- **Concentrateurs (hub):**

Ils permettent de connecter plusieurs appareils électroniques entre eux, leur permettant ainsi de communiquer et d'échanger des données. Les hubs sont souvent utilisés dans les réseaux informatiques pour connecter des ordinateurs, des imprimantes, des routeurs et d'autres périphériques en utilisant des câbles Ethernet.

- **Commutateurs réseau (switch):**

Ils permettent de relier les différents appareils du réseau entre eux et de faciliter la communication des données.

- **Routeur:**

Ces appareils gèrent le trafic réseau entre différents réseaux, en déterminant le chemin optimal pour les données à travers le réseau.

- **Câbles Ethernet:**

Ils sont utilisés pour connecter les appareils au réseau. Les câbles catégorie 5e ou supérieure sont généralement recommandés pour des connexions filaires plus rapides et plus fiables.

- **Point d'accès sans fil (Access Points):**

Ils permettent la connexion sans fil des appareils au réseau. Les points d'accès sans fil sont nécessaires si vous souhaitez avoir une connectivité Wi-Fi.

- **Serveur:**

Ils sont utilisés pour stocker et gérer les données, héberger des services réseau et fournir des fonctionnalités spécifiques au réseau.

- **Par-feu (Firewall):**

Il s'agit d'un dispositif matériel ou logiciel qui protège le réseau contre les intrusions et les attaques en bloquant ou filtrant les trafics non autorisés.

- **Câbles de connexion(RJ45):**

Ils sont utilisés pour connecter les appareils réseau aux commutateurs ou aux points d'accès sans fil.

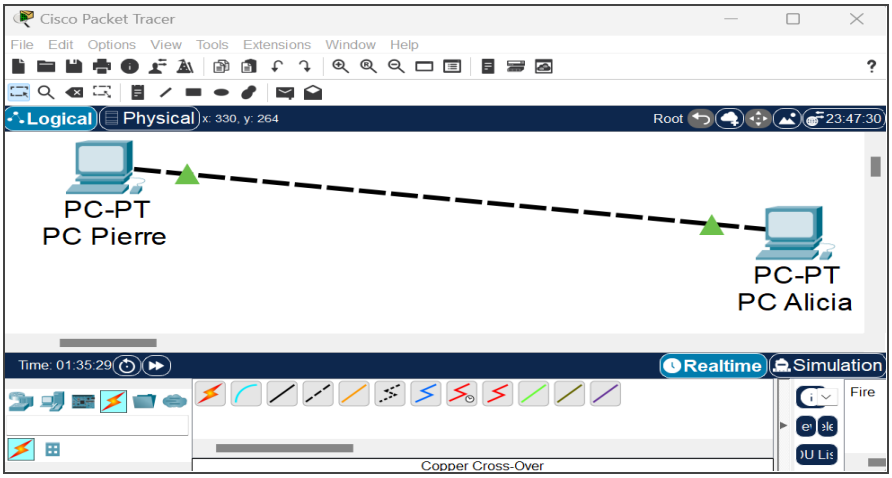
- **Cartes réseau:**

Elles sont nécessaires pour permettre aux appareils de se connecter au réseau. Les cartes réseau peuvent être intégrées à l'ordinateur ou ajoutées séparément.

- **Appareils terminaux:**

Ils comprennent les ordinateurs, les smartphones, les tablettes, les imprimantes, etc. Ils sont utilisés pour accéder au réseau et échanger des informations.

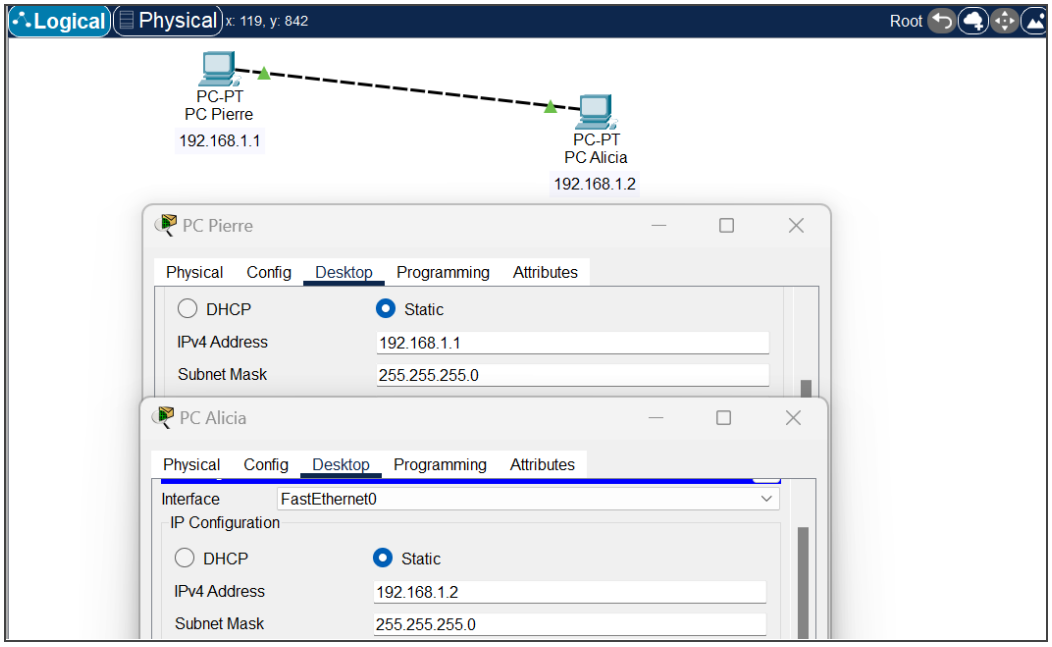
Job 3:



-Le type de câble choisis:

Un Copper Cross-Over est un type de câble utilisé pour connecter deux appareils ou composants réseau, tels que des ordinateurs, des routeurs ou des commutateurs.
Il est spécifiquement conçu pour les connexions directes entre deux appareils similaires, tels que deux ordinateurs, sans passer par un commutateur ou un routeur intermédiaire. Il est utilisé lorsque les deux appareils ne sont pas directement compatibles pour une connexion directe, souvent en raison de la configuration interne de leur port Ethernet.
Le câble Copper Cross-Over est généralement doté de fils de cuivre torsadés, d'où son nom, et offre une connexion fiable et stable entre les appareils. Il est souvent utilisé dans les petites installations ou les réseaux locaux où seules quelques connexions directes sont nécessaires.

Job 4:



-Qu’est ce une adresse IP ?

Une adresse IP (Internet Protocol) est une étiquette numérique qui identifie un appareil connecté à un réseau informatique utilisant Internet Protocol pour la communication.

L’adresse IP est composée de 4 octets allant de 0 à 255 séparés par des points. Chaque adresse IP appartient à une classe qui correspond à une plage d’adresses IP.

Au total 5 classes existent A, B, C, D et E, cela sert à adapter l’adressage selon la taille du réseau.

Voici les plages d’adresse selon les classes :

- La classe A de l’adresse IP 0.0.0.0 à 126.255.255.255
- La classe B de l’adresse IP 128.0.0.0 à 191.255.255.255
- La classe C de l’adresse IP 192.0.0.0 à 223.255.255.255
- La classe D de l’adresse IP 224.0.0.0 à 239.255.255.255
- La classe E de l’adresse IP 240.0.0.0 à 255.255.255.255

Les adresses IP des classes D (adresses de multicast) et E (adresses réservées par IETF) sont des adresses IP réservées donc non utilisables.

-A quoi sert un IP ?

Un IP (Internet Protocol) est un protocole de communication utilisé pour identifier et localiser les appareils connectés à un réseau informatique, tels que des ordinateurs, des serveurs, des routeurs, des imprimantes, etc. Il permet d'attribuer une adresse unique à chaque appareil afin de garantir une communication efficace.

L'adresse IP est essentielle pour permettre le fonctionnement d'Internet, car elle permet de diriger le trafic de données entre les différents appareils connectés. L'IP permet également de localiser géographiquement un appareil, ce qui est utile pour diverses applications, telles que la géolocalisation des utilisateurs, le filtrage d'accès basé sur la localisation, etc.

-Qu’est-ce qu’une adresse MAC ?

Une adresse MAC (Media Access Control) est une identifiant unique attribué à une interface réseau d'un périphérique. Cet identifiant, généralement représenté sous la forme d'une série de chiffres et de lettres, permet de distinguer chaque périphérique connecté à un réseau local (LAN). L'adresse MAC est gravée dans la carte réseau du périphérique lors de sa fabrication et ne peut pas être modifiée.

-Qu’est-ce qu’une IP publique et privée ?

- **Les adresses IP privées** sont toutes les adresses IP qui ne sont pas utilisables sur internet, par exemple le réseau de votre entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les plages d’adresses IP non accessibles depuis Internet. Elles permettent de communiquer localement avec vos différents périphériques.

Les adresses IP privées se trouvent dans les classes A, B et C.

Voici les plages d'adresse IP privé selon les classes :

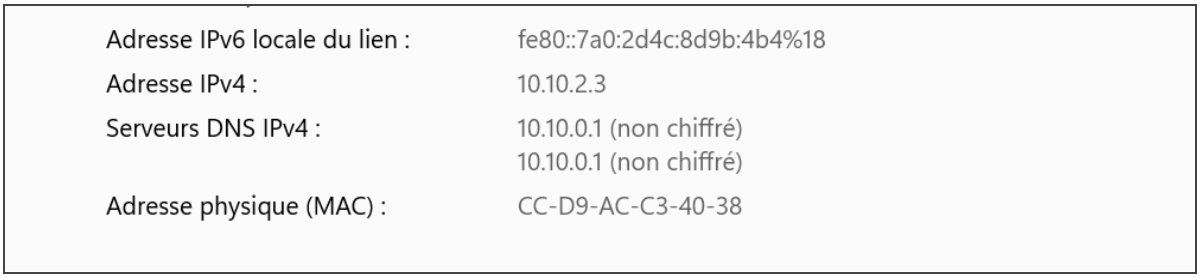
- Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255 (comprend 16 millions d'adresses)
- Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255 (comprend 65535 adresses)
- Les adresses privées de la classe C : 192.168.0.0 à 192.168.255.255 (comprend 256 adresses)

❖ **Les adresses IP publiques** ne sont pas utilisées dans un réseau local mais uniquement sur internet.

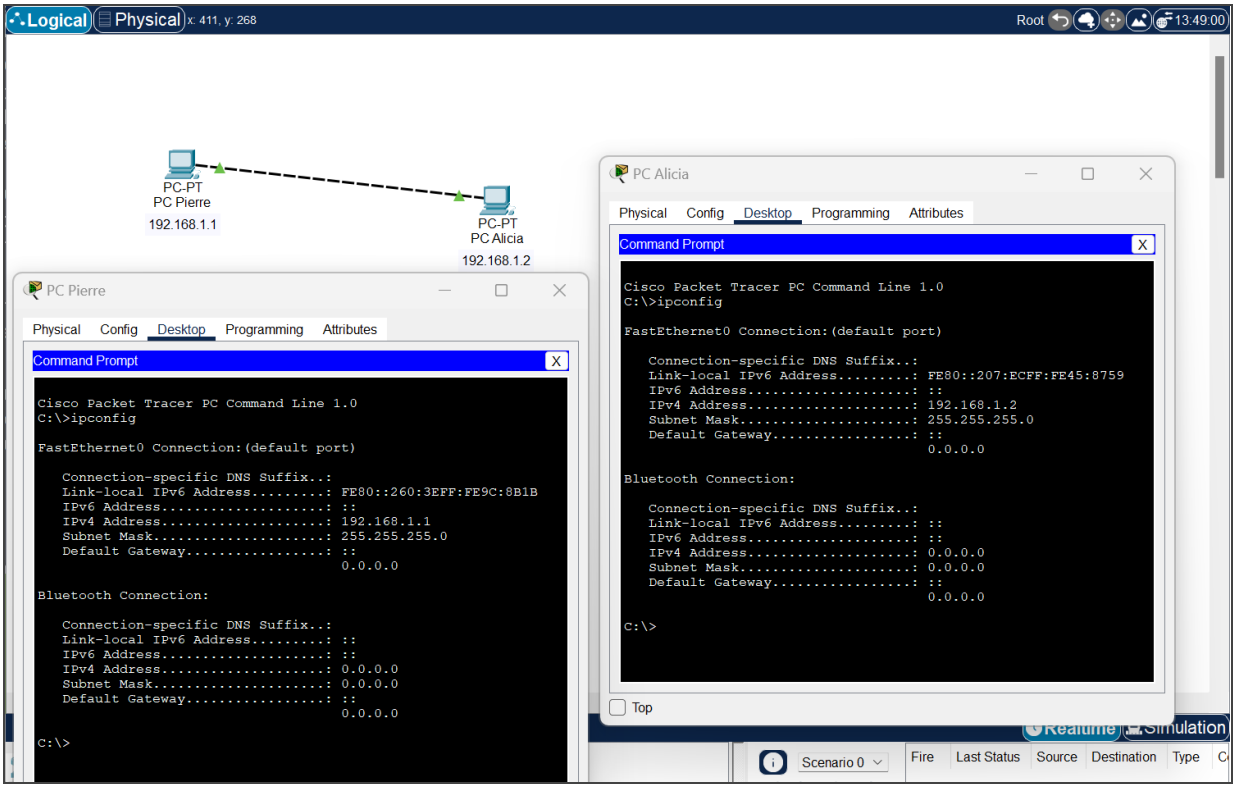
Une adresse IP publique est unique dans le monde alors que pour une adresse IP privée c'est dans le réseau local qu'elle est unique.

Les adresses IP publiques représentent toutes les adresses IP des classes A, B et C qui ne font pas partie de la plage d'adresses privées de ces classes ou des exceptions de la classe A qui sont le réseau 127.0.0.0 qui est réservé pour les tests de boucle locale et le réseau 0.0.0.0 qui est réservé pour définir une route par défaut sur un routeur.

-Quelle est l'adresse de ce réseau ?



Job 5:

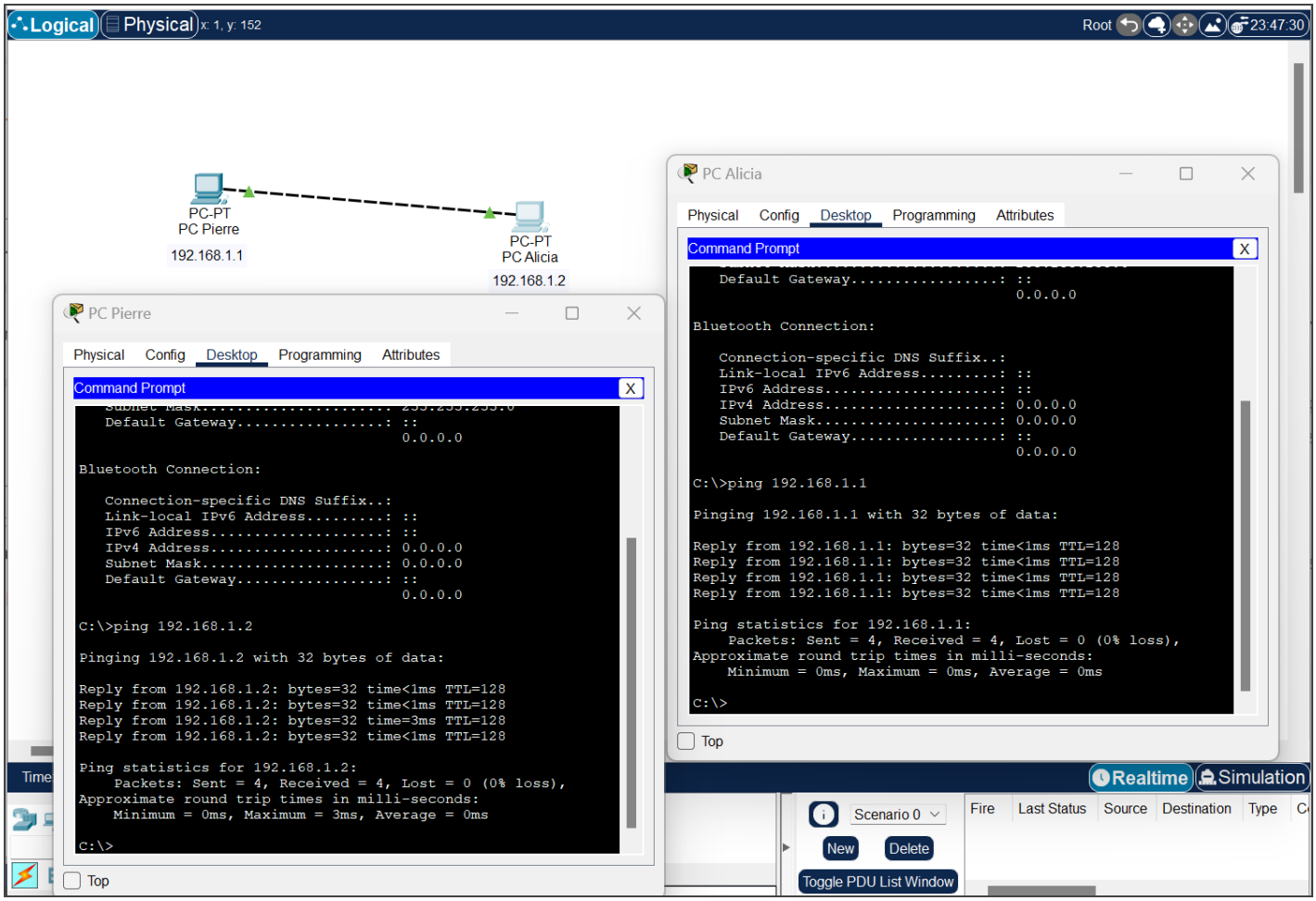


-Quelle ligne de commande avez-vous utilisé pour vérifier l'ip des machines ?

Dans la fenêtre du terminal, tapez la commande suivante : `ipconfig` .

La sortie de la commande affichera les informations réseau du PC, y compris son adresse IP. Recherchez l'adresse IP dans la liste, généralement sous la section “IPv4 Address" ou "inet addr".

Job 6:



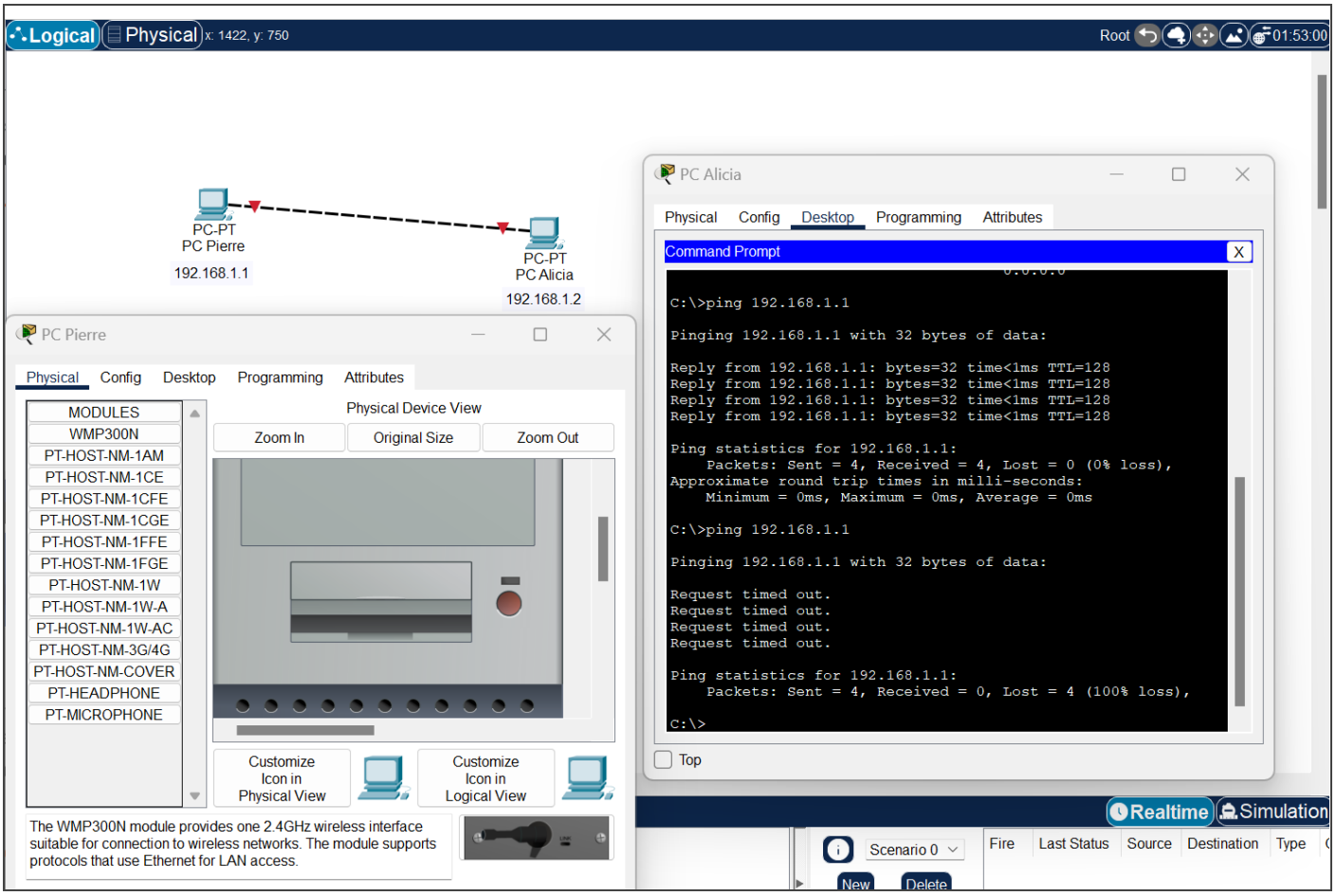
-Quelle est la commande permettant de Ping entre des PC?

La commande “ping” permet de faire un ping entre des PC. Par exemple, pour pinger l'adresse IP d'un autre PC sur le réseau, vous pouvez utiliser la commande suivante dans le terminal :

```
ping adresse_IP
```

On remplace “adresse_IP” par l’adresse de PC cible qu’on souhaite pinger.

Job 7:



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

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

Le résultat de ping :

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

-Explication:

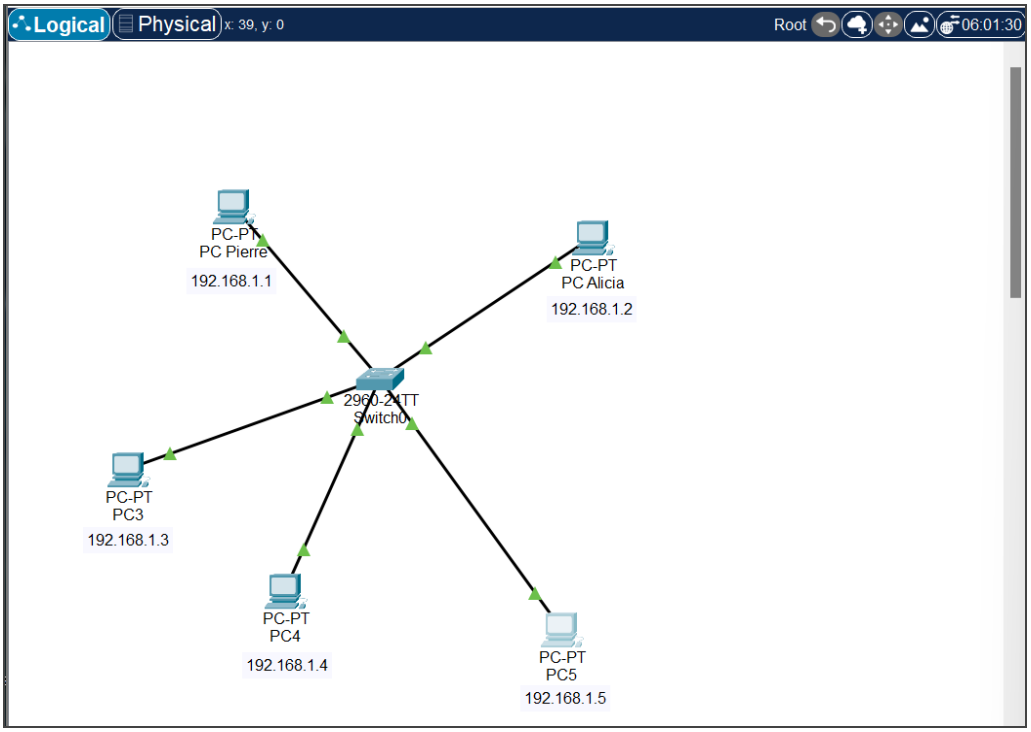
Lorsqu'un ordinateur est éteint, il ne peut pas communiquer sur le réseau car tous ses services réseau sont arrêtés, y compris ceux qui répondent aux requêtes PING.

Le PING est un outil de diagnostic qui envoie des paquets de test à une adresse IP spécifique pour vérifier si un ordinateur distant est accessible et actif. Si l'ordinateur cible (dans ce cas, le PC de Pierre) ne répond pas aux paquets PING, cela peut signifier qu'il est éteint, qu'il a des problèmes de réseau ou qu'il bloque les requêtes PING en raison d'une configuration spécifique.

Donc, si le PC de Pierre est éteint, il ne va pas recevoir les paquets PING envoyés par Alicia.

Job 8:

- - - -



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

Hub	Switch
Fonctionnement	
Fonctionne au niveau physique et transmet les données reçues à tous les appareils connectés sur le hub.	Fonctionne au niveau de la couche liaison de données et envoie les données uniquement à l'appareil destinataire.
Gestion du trafic	
Collisions de données si plusieurs appareils essaient d'envoyer des	Gère le trafic réseau en utilisant des tables d'adresses MAC pour

données simultanément. Cela peut entraîner une baisse des performances.	diriger les données uniquement vers les appareils destinataires, ce qui évite les collisions et améliore les performances du réseau.
Sécurité	
Ne possède aucune fonctionnalité de sécurité avancée. Étant donné qu'il transmet les données à tous les appareils, toutes les données sont potentiellement visibles pour les appareils connectés au hub.	Possède des fonctions de sécurité supplémentaires telles que filtrage d'adresses MAC, qui permet de restreindre les appareils autorisés à se connecter au réseau.
Extensibilité	
Utilisés dans de petites installations réseau,car ils ne peuvent pas gérer efficacement un grand nombre d'appareils connectés.	Ils sont conçus pour gérer plusieurs connexions simultanées et sont plus adaptés aux réseaux de taille moyenne à grande .

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

Un hub est un appareil qui permet de connecter plusieurs périphériques sur un réseau local (LAN). Son fonctionnement est relativement simple. Lorsqu'un périphérique est connecté à un hub, le hub reçoit les données provenant de ce périphérique. Il vérifie alors l'adresse de destination des données pour déterminer quel périphérique doit recevoir ces données.
Le hub copie ensuite ces données et les envoie à tous les périphériques connectés à son port, à l'exception du périphérique d'origine. Cela signifie que tous les périphériques connectés reçoivent les données, même s'ils ne sont pas spécifiquement destinataires.

- **Avantages:**
  - Simplicité d'utilisation: très simple à installer et à utiliser.
  - Augmentation du nombre de ports: les hubs sont idéaux pour ajouter des ports supplémentaires.
  - Centralisation des connexions: on peut utiliser un seul câble pour connecter le hub. Cela permet de réduire l'encombrement des câbles et de rendre l'espace de travail plus organisé.
  - Flexibilité de connexion: un hub permet de connecter différents types de périphériques à un seul appareil.Cela offre une plus grande flexibilité pour les connexions.

- **Inconvénients:**
  - Vitesse de transfert limitée: la vitesse de transfert de données d'un hub,en particulier si on utilise plusieurs périphériques simultanément. Cela peut entraîner des délais de transfert plus longs et une performance inférieure.
  - Puissance limitée: les hubs USB ont souvent une puissance limitée pour alimenter les périphériques connectés.
  - Risque de surcharge: Si plusieurs périphériques sont connectés au hub, cela peut surcharger et causer des problèmes de performance.
  - Incompatibilité de périphériques: Certains périphériques peuvent ne pas être compatible avec certains hubs en raison de différences de protocole ou de normes.

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

- **Avantages:**
  - Connectivité réseau améliorée; Un x=switch permet de connecter plusieurs appareils sur un réseau local, cela facilite le partage de ressources et la communication entre eux.
  - Haute performance; les switchs offrent une bande élevée et des temps de lance réduits, ce qui permet un transfert de données rapide et efficace.
  - Sécurité renforcée : Les switches réseau peuvent mettre en place des fonctionnalités de sécurité avancées, telles que la gestion des listes de contrôle d'accès, pour protéger le

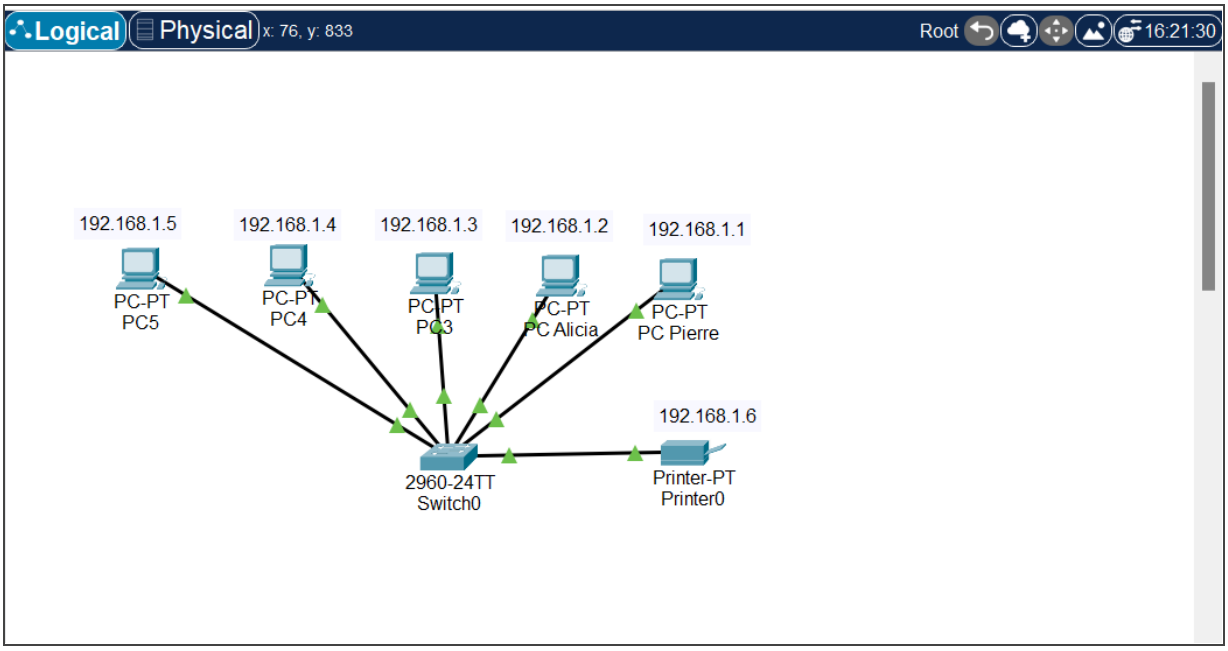
réseau des menaces potentielles.
  - Facilité de gestion : Les switchs sont généralement faciles à configurer et à gérer, avec des outils de gestion graphique conviviaux. Ils permettent également une meilleure visibilité sur le réseau et facilitent le dépannage des problèmes de connectivité.

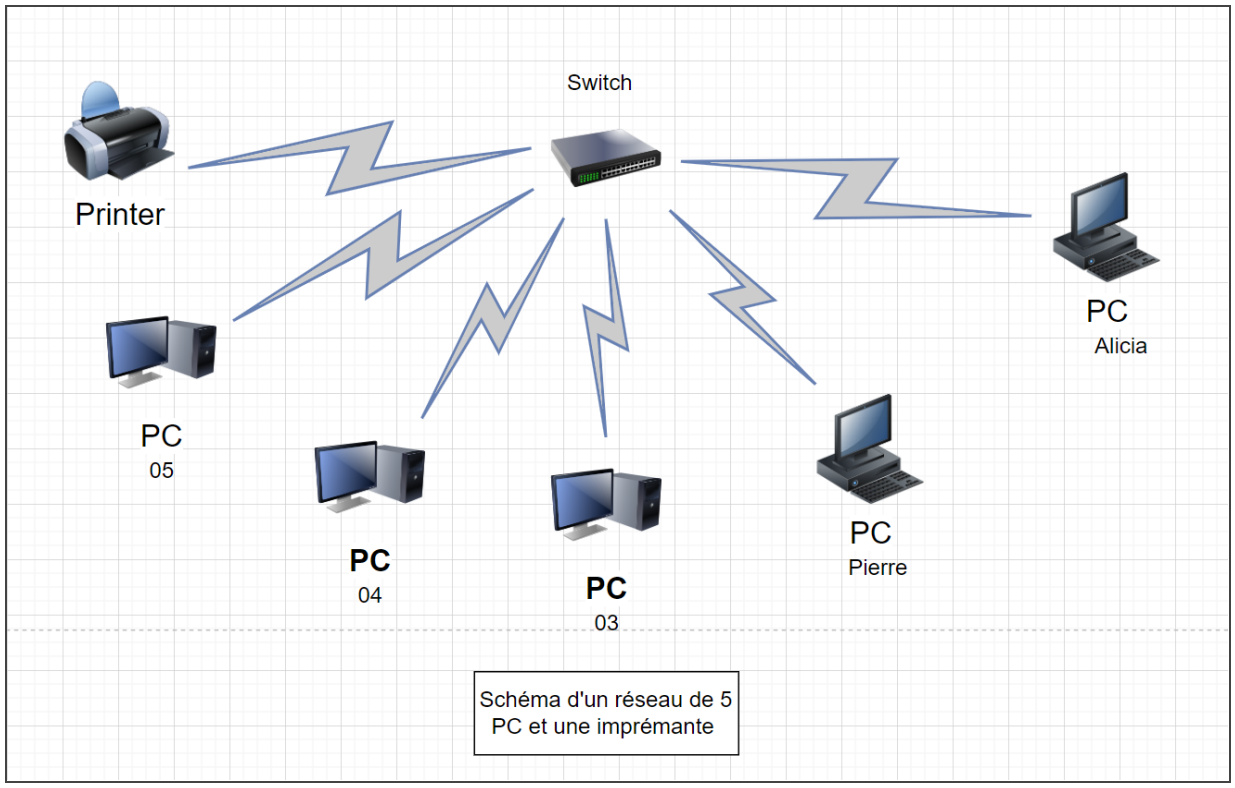
- **Inconvénients:**
  - Coût : Les switchs peuvent être relativement coûteux, en particulier pour les modèles haut de gamme offrant des fonctionnalités avancées.
  - Gestion complexe : Si on est pas familier avec la configuration des switches, cela peut être un processus complexe qui nécessite des connaissances techniques.
  - Limitations de taille et de portée : Les switchs ont une limite sur le nombre de ports qu'ils peuvent prendre en charge, ce qui peut être insuffisant pour les grandes infrastructures réseau. De plus, ils ne peuvent se connecter qu'aux appareils situés à proximité physique, ce qui limite leur portée.
  - Vulnérabilités bloquantes : En cas de panne d'un switch, tous les appareils connectés à ce switch peuvent perdre leur connectivité réseau, ce qui peut avoir un impact significatif sur la productivité.

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

Un switch gère le trafic réseau en utilisant des adresses MAC (Media Access Control) pour diriger les paquets de données vers la bonne destination. Lorsqu'un paquet arrive sur un port du switch, le switch lit l'adresse MAC source du paquet et la compare à sa table de correspondance des adresses MAC.
Si l'adresse MAC de destination est déjà présente dans la table, le switch envoie le paquet uniquement au port approprié où se trouve cette adresse. Si l'adresse MAC de destination n'est pas répertoriée dans la table, le switch transmet le paquet à tous les autres ports (à l'exception du port d'origine) afin de trouver la bonne destination.

Job 9:


Logical
Physical
x: 76, y: 833
Root
16:21:30
192.168.1.5
192.168.1.4
192.168.1.3
192.168.1.2
192.168.1.1
PC-PT
PC5
PC-PT
PC4
PC-PT
PC3
PC-PT
PC Alicia
PC-PT
PC Pierre
192.168.1.6
2960-24TT
Switch0
Printer-PT
Printer0


Switch
Printer
PC
05
PC
04
PC
03
PC
Pierre
PC
Alicia
Schéma d'un réseau de 5
PC et une imprémante

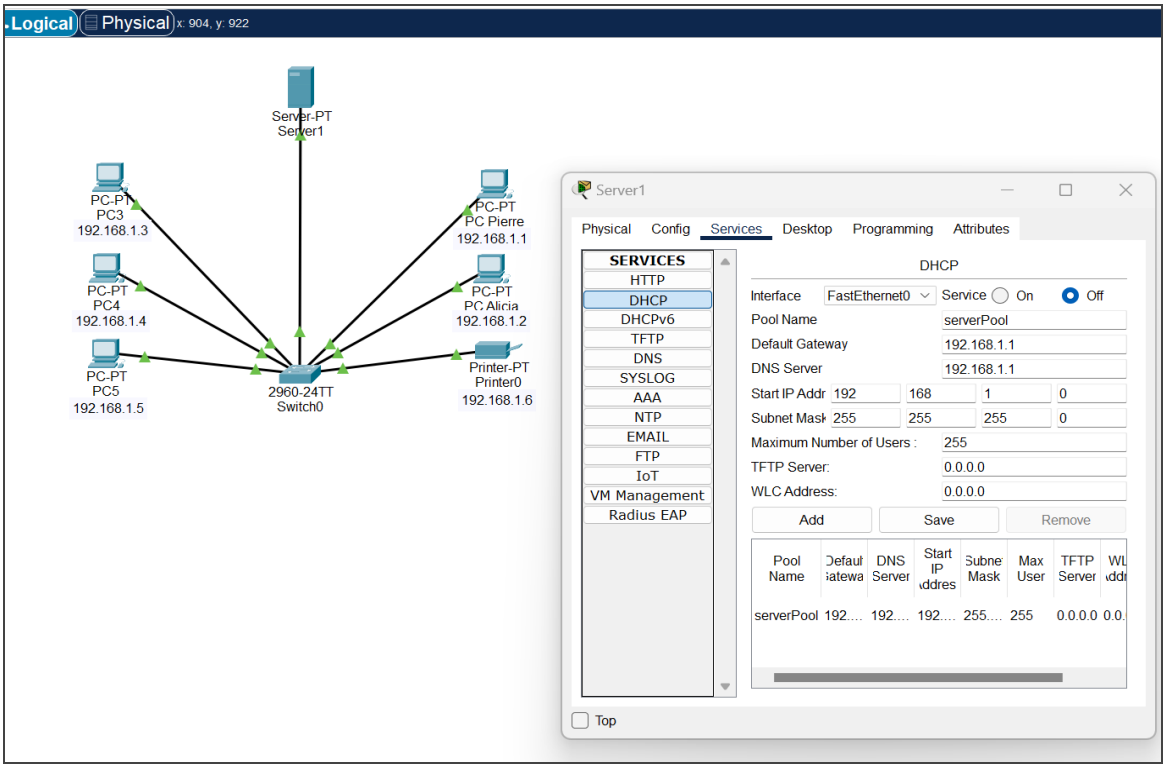
-Avantages d’avoir un schéma réseau?

- Organisation et structuration des idées : Un schéma permet de visualiser clairement les différentes parties d'un ensemble et de les organiser de manière cohérente. Cela facilite la compréhension globale du sujet traité et aide à relier les informations entre elles.

- Mémorisation et rétention de l'information : En créant un schéma, on engage activement notre cerveau dans le processus d'assimilation de l'information. Cette activité stimule la mémoire et favorise la rétention à long terme des connaissances. Le schéma devient un outil visuel de référence pour se rappeler des informations importantes.

- Communication efficace : Un schéma peut être utilisé pour simplifier des concepts complexes et les rendre plus accessibles à un large public. Il facilite la transmission d'idées et permet de communiquer de manière claire et concise. Les schémas peuvent également être utilisés lors de présentations pour illustrer visuellement les informations et captiver l'attention de l'auditoire.

Job 10:



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

Une adresse IP statique: est une adresse IP fixe qui est manuellement attribuée à un appareil sur un réseau. Elle est souvent utilisée pour des serveurs, des imprimantes réseau ou des appareils qui nécessitent des adresses IP permanentes. Une fois qu'une adresse IP statique est attribuée, elle ne changera pas à moins qu'elle ne soit modifiée manuellement.
Une adresse IP attribuée par DHCP: (Dynamic Host Configuration Protocol) est une adresse IP dynamique qui est automatiquement attribuée à un appareil par un serveur DHCP. Le serveur DHCP dispose d'une plage d'adresses IP disponibles qu'il peut distribuer aux appareils lorsqu'ils se connectent au réseau. L'adresse IP attribuée par DHCP est temporaire et peut changer chaque fois que l'appareil se connecte au réseau, selon les paramètres du serveur DHCP.

Job 11:

- - - -

-Le plan d'adressage:

Pour créer 21 sous-réseaux; on prend le masque de sous-réseau de l'adresse 10.0.0.0 qui est une adresse de classe A (255.0.0.0) et on alloue 5 bits à la partie réseau du masque pour avoir 2^5=32 réseaux >21 réseaux demandés
On à donc le nouveau masque de sous réseau 255.248.0.0qui peut accueillir jusqu'à 2^19 hôtes.

- Pour chaque sous réseau on change les 5 bits alloué à la partie réseau pour obtenir 32 sous réseau différents :

```
10.0000 0000.0.0      1er sous-réseau:  10.0.0.0/13
10.0000 1000.0.0      2ème sous-réseau: 10.8.0.0/13
10.0001 0000.0.0      3ème sous-réseau: 10.16.0.0/13
10.0001 1000.0.0      4ème sous-réseau: 10.24.0.0/13
10.0010 0000.0.0…     5ème sous-réseau: 10.32.0.0/13
…
10.1111 1000.0.0      32ème sous-réseau:10.248.0.0/13
```

- Comme on peut incrémenter le premier octet de la partie réseau de 1 , on peut obtenir jusqu'à 255 sous-réseaux différents .

		adresses de sous-réseau	Rang d'adresses utilisables	Broadcast	Masque de sous-réseau
sous-réseau de 12 hôtes		10.0.0.0	10.0.0.1 - 10.0.0.14	10.0.0.15	255.255.255.240 /28
5 sous-réseau de 30 hôtes	1	10.0.0.16	10.0.0.17 - 10.0.0.46	10.0.0.47	255.255.255.224 /27
	2	10.0.0.48	10.0.0.49 - 10.0.0.78	10.0.0.79	255.255.255.224 /27
	3	10.0.0.80	10.0.0.81 - 10.0.0.110	10.0.0.111	255.255.255.224 /27

	4	10.0.0.112	10.0.0.113 - 10.0.0.142	10.0.0.143	255.255.255.224 /27
	5	10.0.0.144	10.0.0.145 - 10.0.0.174	10.0.0.175	255.255.255.224 /27
5 sous-réseau de 120 hôtes	1	10.0.0.176	10.0.0.177 - 10.0.1.46	10.0.1.47	255.255.255.128 /25
	2	10.0.1.48	10.0.1.49 - 10.0.1.174	10.0.1.175	255.255.255.128 /25
	3	10.0.1.176	10.0.1.177 - 10.0.2.46	10.0.2.47	255.255.255.128 /25
	4	10.0.2.48	10.0.2.49 - 10.0.2.174	10.0.2.175	255.255.255.128 /25
	5	10.0.2.176	10.0.2.177 - 10.0.3.46	10.0.3.47	255.255.255.128 /25
5 sous-réseau de 160 hôtes	1	10.0.3.48	10.0.3.49 - 10.0.4.46	10.0.4.47	255.255.255.0 /24
	2	10.0.4.48	10.0.4.49 - 10.0.5.46	10.0.5.47	255.255.255.0 /24
	3	10.0.5.48	10.10.5.49 - 10.0.6.46	10.0.6.47	255.255.255.0 /24
	4	10.0.6.48	10.0.6.49 - 10.0.7.46	10.0.7.47	255.255.255.0 /24
	5	10.0.7.48	10.0.7.49 - 10.0.8.46	10.0.8.47	255.255.255.0 /24

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

Cette classe offre une grande plage d'adresses IP utilisables. La classe A a une adresse réseau de 8 bits et permet donc d'avoir 2^24-2

adresses IP disponibles pour les hôtes. Cette classe convient donc parfaitement pour créer de nombreux sous-réseaux avec une quantité suffisante d'adresses IP pour chaque sous-réseau.

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

Les différentes classes d'adresse réseau sont utilisées dans le modèle d'adressage IPv4 pour diviser l'espace d'adressage en différentes parties pour les réseaux privés et publics.
La principale différence entre les classes d'adresse réseau réside dans la plage d'adresses IP qu'elles peuvent fournir pour les réseaux et les hôtes.

Voici un aperçu des différentes classes d'adresse réseau :

Classe A :
Les adresses de classe A commencent par un premier octet compris entre 1 et 126 . L'adressage de classe A est conçu pour les grands réseaux et peut fournir jusqu'à 16 777 214 adresses IP pour les hôtes sur un réseau (255.0.0.0).

Classe B :
Les adresses de classe B commencent par un premier octet compris entre 128 et 191. L'adressage de classe B est conçu pour les réseaux de taille moyenne et peut fournir jusqu'à 65 534 adresses IP pour les hôtes sur un réseau (255.255.0.0).

Classe C :
Les adresses de classe C commencent par un premier octet compris entre 192 et 223. L'adressage de classe C est conçu pour les petits réseaux et peut fournir jusqu'à 254 adresses IP pour les hôtes sur un réseau(255.255.255.0).

Job 12:

- - - -

-Le modèle OSI :

Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel qui définit comment les systèmes réseau communiquent et envoient des données d'un expéditeur à un destinataire.

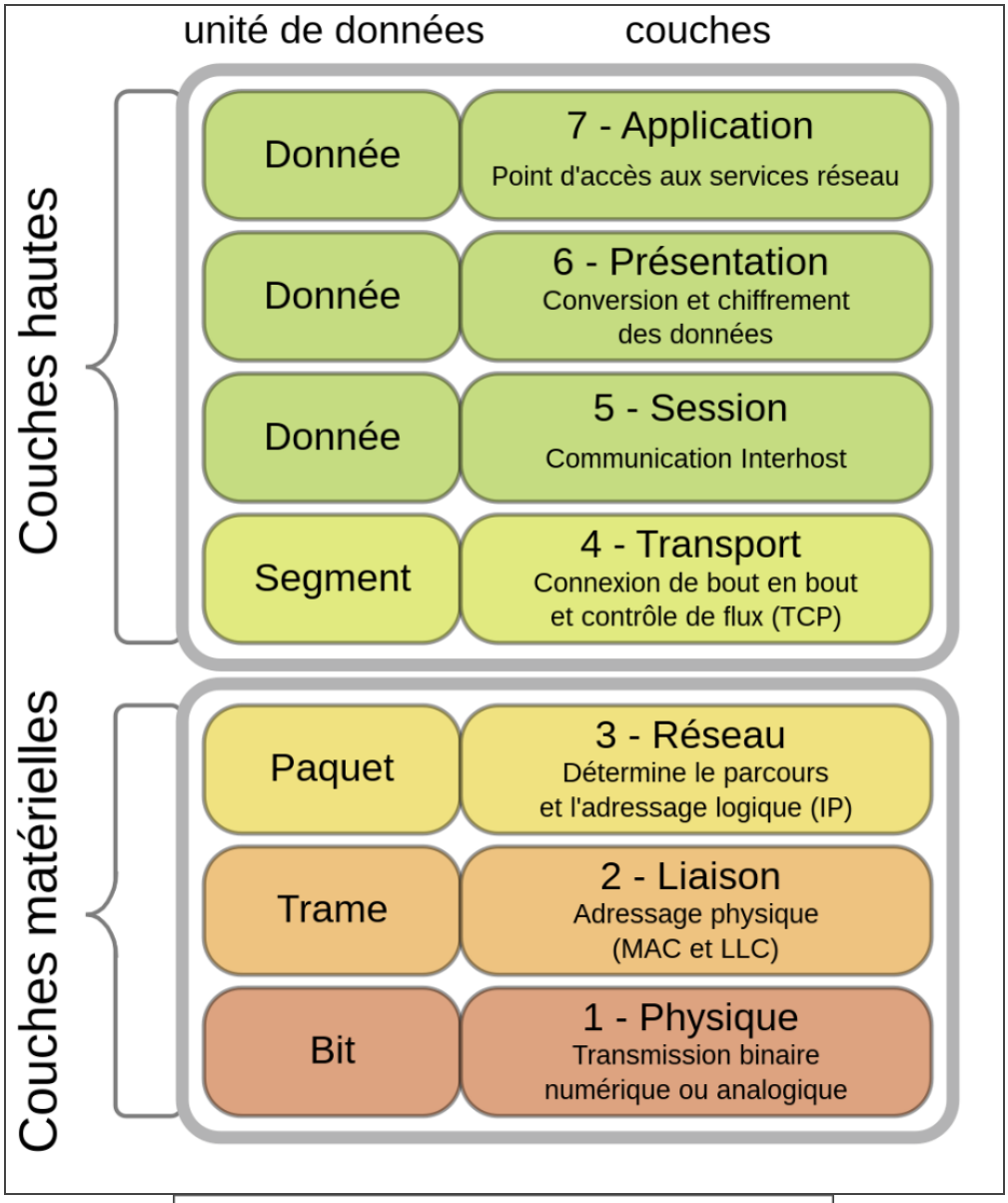
Le modèle est utilisé pour décrire chaque composant de la communication de données pour pouvoir établir des règles et des normes pour les applications et l'infrastructure du réseau.

Le modèle OSI contient sept couches qui s'empilent conceptuellement de bas en haut.

-Les sept couches du modèle OSI?

Couches	Rôles	Matériels/ Protocoles
Physique	Cette couche est responsable de la transmission des bits bruts sur le support physique. Elle gère les caractéristiques électriques, mécaniques et fonctionnelles des interfaces physiques.	**Fibre optique** **Wi-Fi** **Câble RJ45**
Liaison	Cette couche divise les données en trames et les transmet de manière fiable entre les nœuds du réseau local. Elle gère également le contrôle d'accès au support et la détection d'erreurs	**Ethernet** **MAC**
Réseau	Cette couche est responsable du routage des paquets à travers le réseau. Elle détermine le chemin optimal pour acheminer les données et utilise des adresses logiques	**Routeur** **IPV4** **IPV6**

	(ex: IPv4, IPv6) pour identifier les périphériques de réseau.	
Transport	Cette couche assure l'acheminement des segments de données entre les hôtes de bout en bout. Elle garantit une communication fiable en effectuant un contrôle d'erreur, une segmentation et un contrôle de flux.	**TCP** **UDP**
Session	Cette couche établit, maintient et termine les sessions entre les applications en cours de communication. Elle gère également les synchronisations et le contrôle des dialogues.	
Présentation	Cette couche assure la traduction des données dans un format compréhensible par l'application. Elle gère également la compression, le chiffrement et la conversion des données.	
Application	Cette couche fournit les services de réseau aux applications utilisateurs. Elle offre une interface pour l'accès aux services de communication	**PPTP** **SSL/TSL** **FTP** **HTML**



Modèle OSI - schéma

Job 13:

-Quelle est l'architecture de réseau ?

L'architecture de ce réseau est une architecture en réseau local (LAN) avec une plage d'adresses IP privées du réseau local 192.168.10.0/24.

Une architecture en réseau local (LAN) fait référence à la conception et à la structure d'un réseau informatique local qui relie les ordinateurs et les périphériques au sein d'un espace restreint, comme un foyer, un bureau ou un bâtiment.
Une architecture en réseau local peut être constituée de différents éléments, notamment :

- Les ordinateurs
- Les périphériques (routeur, switch, hub,...)
- Les câbles
- Les protocoles de réseau

-L'adresse IP du réseau ?

Pour trouver l'adresse réseau à partir d'une adresse IP et d'un masque de sous-réseau, on effectue une opération logique appelée "bitwise AND" entre l'adresse IP et le masque de sous-réseau.
Voici les étapes à suivre :

1. Convertir l'adresse IP et le masque de sous-réseau en notation binaire.

2. Effectuer l'opération "bitwise AND" entre les deux valeurs en comparant les bits correspondants :
   - Si un bit est à 1 dans les deux valeurs, le résultat sera 1.
   - Si un bit est à 0 dans l'une des valeurs, le résultat sera 0.

3. Convertir le résultat binaire en notation décimale pour obtenir l'adresse réseau.

```
192.168.0.6 en binaire:   1100 0000.1010 1000.0000 0000.0000 0110
255.255.255.O en binaire: 1111 1111.1111 1111.1111 1111.0000 0000
bitwise AND:              1100 0000.1010 1000.0000 0000.0000 0000
Résultat en décimal :     192      . 168     . 0       . 0
```

➢ L’adresse de réseau est : 192.168.0.0

-Le nombre de machines que l’on peut brancher sur ce réseau :

Le réseau 192.168.0.0 est un réseau de classe C, ce qui signifie qu'il peut prendre en charge jusqu'à 256 machines de 192.168.0.0 à 192.168.0.255.
Toutefois, quelques adresses sont réservées pour des usages spécifiques, comme l'adresse réseau (192.168.0.0) et l'adresse de diffusion (192.168.0.255), ce qui réduit le nombre d'adresses disponibles pour les machines.

➢ En pratique, on peut donc connecter environ 254 machines au réseau 192.168.0.0.

-L’adresse de diffusion de ce réseau :

Une adresse IP de diffusion est une adresse utilisée pour transmettre des données à tous les dispositifs d’un sous-réseau ou d’un réseau. Il est utilisé pour diffuser des informations à tous les dispositifs sur un réseau en utilisant une seule adresse IP.

L’adresse de diffusion est généralement la dernière adresse IP valide dans un réseau.
Par exemple, si un sous-réseau a une adresse de réseau de 192.168.0.0 et un masque de sous-réseau de 255.255.255.0, l’adresse de diffusion serait 192.168.0.255.

Job 14:

-Conversion en binaire:

Conversion à l'aide d'un tableau :

- On commence à lister les puissances de 2 dans un "tableau de base 2" de droite à gauche. Commencez par 2^0 jusqu'à 2^7 (1 octet = 8 bits). Exemple : on veut convertir 145 en base 2.

- Cherchez la plus grande puissance de 2 inférieure ou égale à 145.128 est la plus grande puissance de 2 qui va dans 145.On inscrit un 1 comme chiffre binaire le plus à gauche, et on soustrait 128 de notre nombre décimal 145. Il nous reste maintenant 17.

- On passe à la puissance de 2 immédiatement inférieure. 64 "entre-t-il" dans 17 ? Non,
  Alors écrivez un 0 comme chiffre binaire suivant à droite du premier. Continuez jusqu'à trouver un nombre qui aille dans 17.

- Quand une puissance de 2 est inférieure ou égale à notre reste, marquez 1 et on fait la soustraction de proche en proche. 16 va dans 17, On inscrit 1 sous la case 16 et on fait 17- 16 = 1.
  (et 1 sait le résultat de 2^0 donc on inscrit un 1 sous la case 1.)

- On continue jusqu'à atteindre le bout de notre tableau.Le principe est : on met un 1 quand cette puissance de 2 va dans notre nombre, on met 0 dans le cas contraire.

- Enfin on assemble la réponse binaire. On lit la réponse de gauche à droite : ici, c'est 10010001 ! Ce nombre est l'équivalent binaire de 145. On peut aussi l'écrire sous la forme : (145)10 = (10010001)2.

Base	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Taille	128	64	32	16	8	4	2	1
	128			+16 144				+1 145
	1	0	0	1	0	0	0	1

145 en binaire est: 1001 0001

on fait la même chose pour ce qui reste :

- **145.32.59.24**

```
  145    .   32    .   59    .  24
1001 0001.0010 0000.0011 1011.0001 1000
```

- **200.42.129.16**

```
  200    .   42    .   129    .  16
1100 1000.0010 1010.1000 0001.0001 0000
```

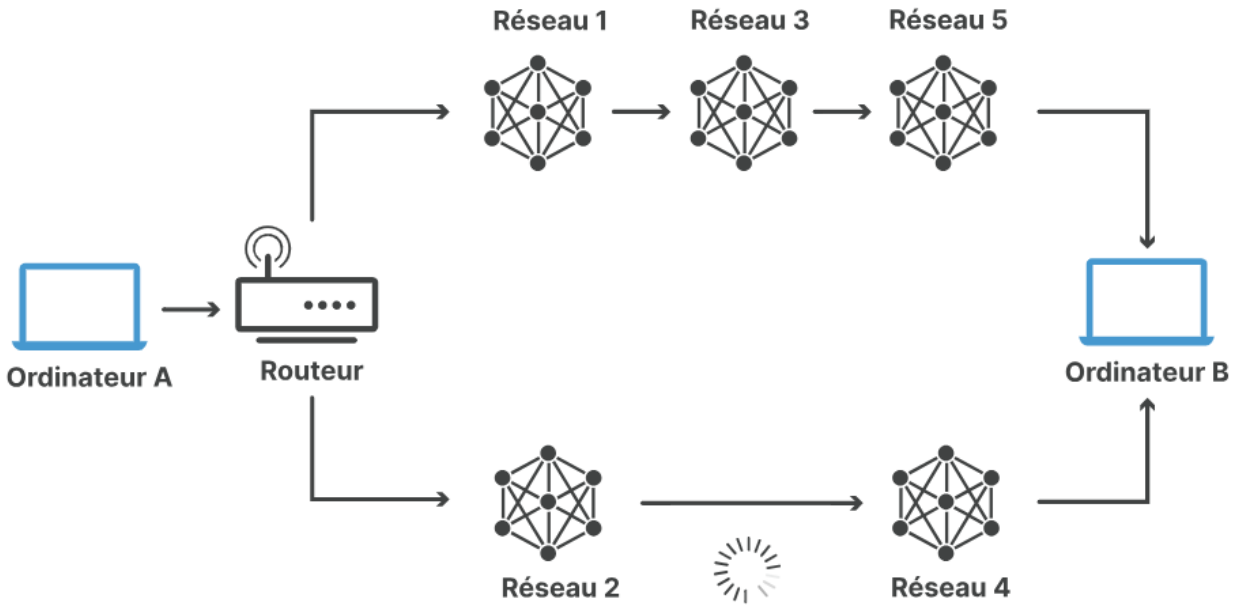
- **14.82.19.54**

```
   14    .   82    .   19    .  54
0000 1110.0101 0010.0001 0011.0011 0110
```

Job 15:

-Qu’est-ce que le routage ?

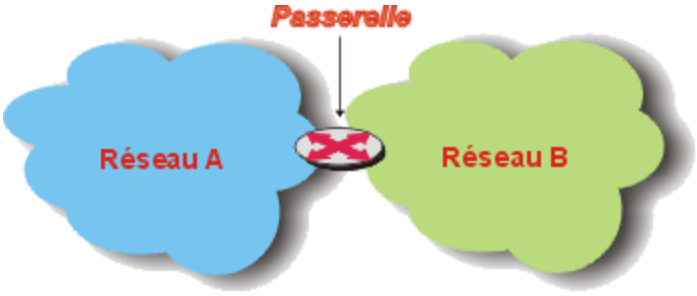
Le routage est le processus de sélection du chemin le plus efficace pour transférer des données d'un réseau à un autre. Il s'agit d'une fonction clé des réseaux de communication, permettant de diriger les paquets de données de manière optimale.
Le routage est effectué par des dispositifs appelés routeurs, qui examinent les adresses des paquets de données et décident du meilleur chemin à emprunter en fonction de différents critères tels que la distance, la vitesse et la congestion du réseau.
L'objectif du routage est de minimiser le temps de transfert des données et d'optimiser l'utilisation du réseau pour fournir une connectivité efficace entre les différentes machines et réseaux.



- Examinons l'image ci-dessus. Pour qu'un paquet de données puisse se rendre de l'ordinateur A à l'ordinateur B, doit-il passer par les réseaux 1, 3 et 5 ou les réseaux 2 et 4 ? Le paquet emprunte un chemin plus court via les réseaux 2 et 4, mais les réseaux 1, 3 et 5 pourraient s'avérer plus rapides pour acheminer les paquets. C'est là le genre de choix que les routeurs réseau effectuent en permanence-

-Qu’est-ce qu’un gateway ?

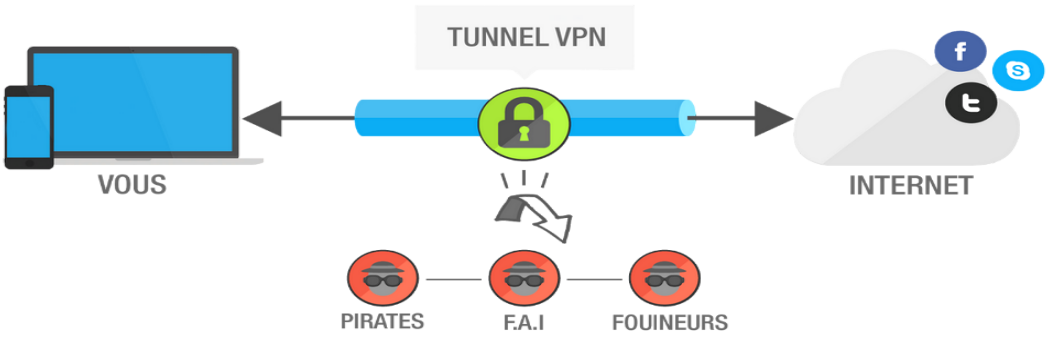
Un gateway, également connu sous le nom de passerelle, est un dispositif qui agit comme un point d'entrée de sortie entre deux réseaux différents, permettant ainsi la communication entre ces réseaux.
Il convertit les protocoles de communication utilisés dans un réseau source en protocoles utilisés dans un réseau de destination, permettant ainsi aux données de circuler entre les réseaux.



-Qu’est-ce qu’un VPN ?

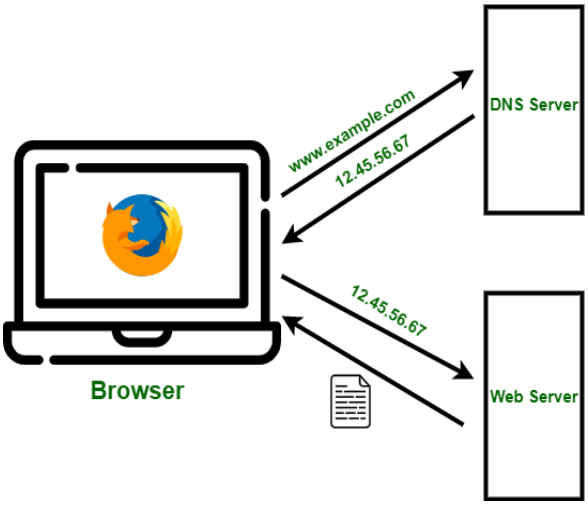
Un VPN est un tunnel sécurisé qui permet de créer une connexion privée et chiffrée entre un périphérique et un réseau distant. Il est souvent utilisé pour garantir la confidentialité et la sécurité des données lors de l'accès à Internet.
L'utilisation d'un VPN permet de masquer l'adresse IP réelle de l'utilisateur, ce qui rend plus difficile pour les tiers de suivre ses activités en ligne. Il peut également contourner les restrictions géographiques en permettant d'accéder à du contenu restreint, comme des sites web ou des services de streaming qui ne sont normalement pas disponibles dans un pays spécifique.

En outre, un VPN crypte les données qui circulent entre l'appareil de l'utilisateur et le serveur distant, ce qui rend les communications plus sécurisées et moins vulnérables aux interceptions ou aux cyberattaques.



-Qu’est-ce qu’un DNS ?

DNS est l'acronyme de Domain Name System (Système de noms de domaines), qui est un système informatique utilisé pour traduire les noms de domaine en adresses IP.



Lorsqu'on saisit un nom de domaine dans un navigateur web, comme www.example.com, l’ordinateur envoie une requête au serveur DNS pour obtenir l'adresse IP correspondante.

Le serveur DNS effectue alors une recherche dans sa base de données pour trouver l'adresse IP associée au nom de domaine demandé.

Une fois que l'adresse IP est trouvée, celle-ci est renvoyée à l’ordinateur, ce qui permet d'établir la connexion entre l’appareil et le serveur correspondant au nom de domaine que on a saisi. Grâce au DNS, nous n'avons pas besoin de connaître l'adresse IP spécifique d'un site web pour y accéder.

- ABDERRAHIM Ryma-

”

Remarque 📜 :

- - - - ✗

le monde était différent avant le réseau informatique mondial. Les informations circulaient beaucoup plus lentement, et il était souvent nécessaire de faire preuve de patience dans l'attente d'une réponse. Aujourd'hui, nous sommes tellement habitués à la connectivité instantanée que nous avons du mal à imaginer à quoi ressemblait la vie avant l'avènement de l'Internet.