Job 2

➔ Qu’est-ce qu’un réseau ?

Un réseau informatique est un ensemble d'ordinateurs interconnectés qui communiquent entre eux pour partager des ressources, des données et des informations. Il existe de nombreux types de réseaux informatiques, mais en général, ils servent à plusieurs fins essentielles, notamment.

➔ À quoi sert un réseau informatique ?

Un réseau informatique sert à relier plusieurs dispositifs informatiques, tels que des ordinateurs, des serveurs, des routeurs, des imprimantes, des smartphones, et d'autres appareils, pour permettre la communication, le partage de ressources et la collaboration. Voici quelques-unes des principales fonctions d'un réseau informatique.

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

Pour construire un réseau, que ce soit un réseau informatique, un réseau électrique, un réseau de télécommunications ou tout autre type de réseau, vous aurez besoin de divers composants matériels. Les composants nécessaires varient en fonction du type de réseau que vous souhaitez mettre en place. Voici une liste générale des composants matériels couramment utilisés dans un réseau informatique, avec une brève explication de leurs fonctions.

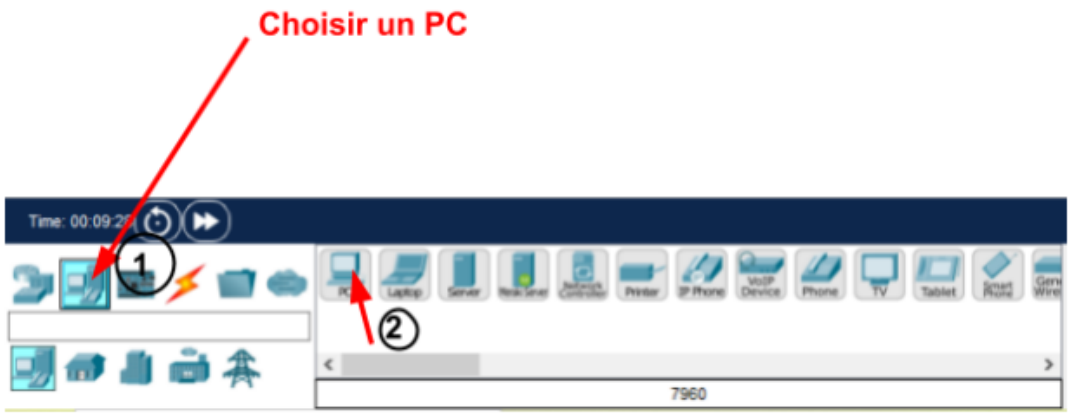
Job 3

➔Maintenant que vous commencez à comprendre le réseau et que Packet Tracer est installé, vous allez pouvoir commencer à créer votre premier réseau.

installé, vous allez pouvoir commencer à créer votre premier réseau.Commencez par mettre dans votre zone de travail deux ordinateurs de bureau, reliés

entre eux par un câble. Pour cela, il suffit de suivre les étapes :

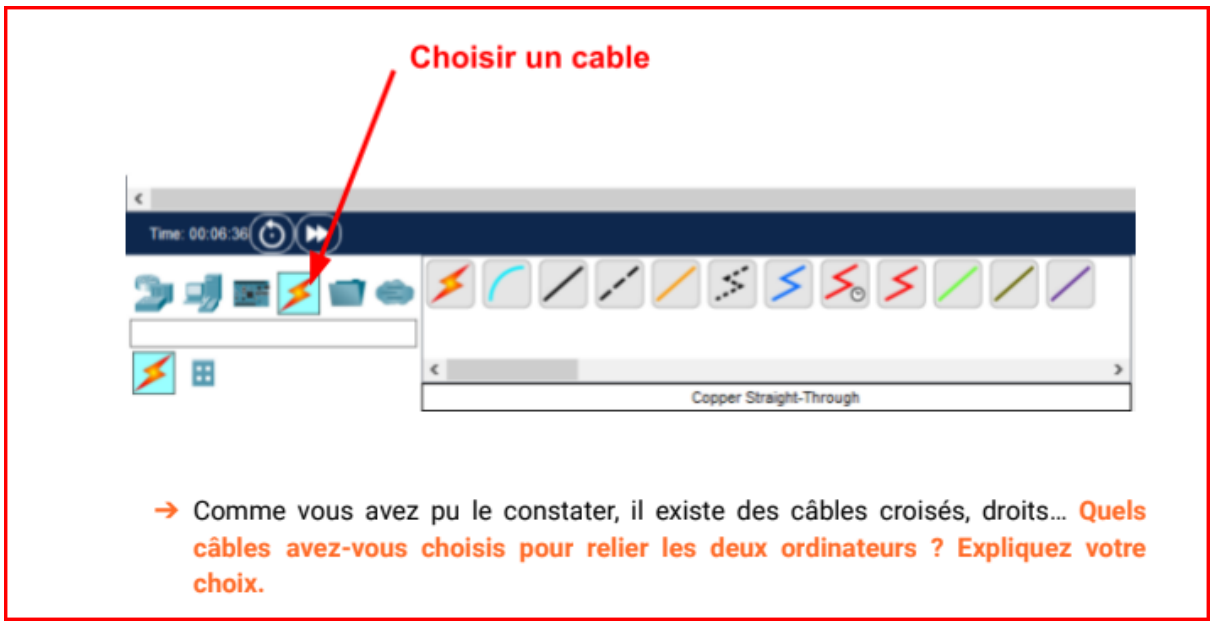
➔ En bas à gauche, cliquez sur l'icône représentant les ordinateur:



➔ Sélectionnez un poste de travail classique et faites le glisser dans votre de travail.

➔ Renommez les PCs en **PC Pierre** et **PC Alicia.**

➔ Dans la même zone en bas à gauche, sélectionnez "**câble**", et à nouveau dans la zone à côté, sélectionnez un câble. Cliquez sur le premier ordinateur, puis sur le deuxième. Indiquez ensuite qu'il s'agit d'une connexion réseau "Fast Ethernet".



➔ Comme vous avez pu le constater, il existe des câbles croisés, droits... Quels câbles avez-vous choisis pour relier les deux ordinateurs? Expliquez votre choix ?

j'ai pris le cross over car c'est celui à utiliser lorsque l'on connecte deux même machine ensemble

Job 4

Maintenant que votre premier réseau est en place, configurez PC Pierre et PC Alicia comme suit :

PIERRE Adresse IP : 192.168.1.1 test OK

```
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
```

ALICIA Adresse IP: 192.168.1.2 test OK

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

➔ Qu’est-ce qu’une adresse IP ?

Une adresse IP, ou adresse de protocole Internet, est une série de numéros qui identifie de manière unique un appareil connecté à un réseau informatique, tel qu'Internet. Les adresses IP sont essentielles pour le routage des données sur Internet, car elles permettent aux routeurs et aux serveurs de diriger les informations vers la destination appropriée. Les adresses IP peuvent être utilisées pour identifier des ordinateurs, des serveurs, des routeurs, des imprimantes, des appareils mobiles et d'autres équipements réseau.

➔ À quoi sert un IP ?

Identification : Chaque appareil connecté à Internet est attribué une adresse IP unique, qui lui sert d'identifiant. Il existe deux versions principales de l'IP : IPv4 (version 4) et IPv6 (version 6). Les adresses IPv4 sont sous la forme de 4 nombres séparés par des points (par exemple, 192.168.1.1), tandis que les adresses IPv6 sont plus longues et complexes pour répondre à la demande croissante d'adresses.

Communication : L'IP permet aux appareils de communiquer entre eux sur Internet en envoyant des paquets de données d'un point à un autre. Chaque paquet contient des informations sur l'expéditeur, le destinataire et le contenu des données.

➔ Qu’est-ce qu'une adresse MAC ?

Une adresse MAC, ou adresse de contrôle d'accès au support, est un identifiant unique attribué à chaque interface réseau d'un appareil. Les adresses MAC sont utilisées pour identifier de manière unique les périphériques sur un réseau local (LAN). Elles sont assignées au niveau matériel et sont généralement constituées de 48 bits, organisés en six groupes de deux caractères hexadécimaux, séparés par des deux-points

ou des tirets. Par exemple, une adresse MAC pourrait ressembler à ceci : "00:1A:2B:3C:4D:5E".

Les adresses MAC sont inscrites en usine sur les cartes réseau (ou adaptateurs réseau) des appareils, qu'il s'agisse d'ordinateurs, de téléphones, d'imprimantes, de routeurs, ou d'autres équipements réseau. Elles sont uniques à chaque carte réseau dans le monde, ce qui permet d'identifier de manière précise et non ambigüe chaque appareil connecté à un réseau.

➔ Qu’est-ce qu’une IP publique ?

Adresse IP publique : Une adresse IP publique est utilisée pour identifier un appareil ou un réseau sur Internet. Chaque appareil connecté à Internet a besoin d'une adresse IP publique unique pour pouvoir communiquer avec d'autres appareils à travers le monde. Les fournisseurs de services Internet (FAI) attribuent généralement une adresse IP publique à un routeur ou un modem, qui est ensuite partagée par plusieurs appareils au sein d'un réseau domestique ou d'entreprise.

➔ Qu’est-ce qu’une IP privée ?

Adresse IP privée : Les adresses IP privées sont utilisées pour identifier les appareils au sein d'un réseau local (LAN). Elles sont généralement attribuées par un routeur ou un serveur DHCP (Dynamic Host Configuration Protocol) au sein d'un réseau domestique ou d'entreprise. Les adresses IP privées ne sont pas routables sur Internet, ce qui signifie qu'elles ne sont pas accessibles depuis l'extérieur du réseau local. Elles sont conçues pour permettre aux appareils de communiquer en interne, mais elles ne sont pas visibles sur le réseau mondial.

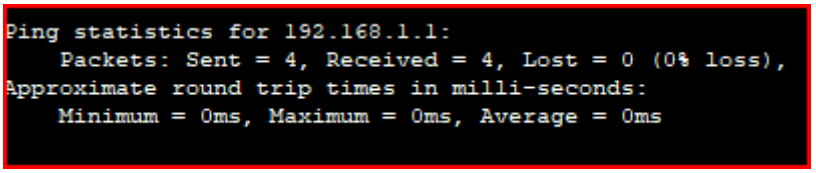
➔ Quelle est l’adresse de ce réseau ?

Le nom de l' adresse de ce réseaux est le Masque de sous-réseau : 255.255.255.0

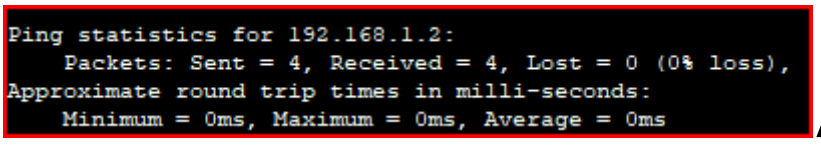
Voici le Masque de sous-réseau.

Job 5

À l’aide du terminal, vérifier que l’IP du PC Pierre est correcte. Faites une capture
d’écran et ajoutez l’image à votre documentation. Répétez les mêmes étapes avec le PC
Alicia.



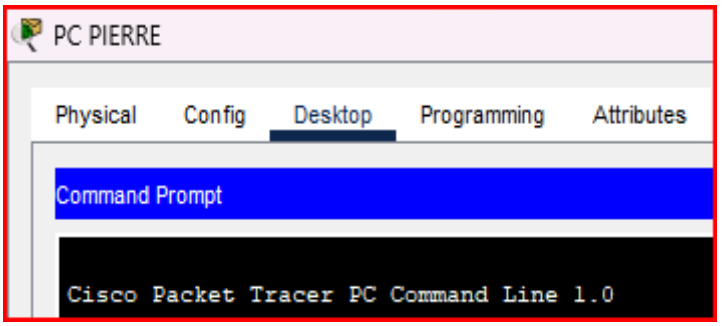
PIERRE



Alicia

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

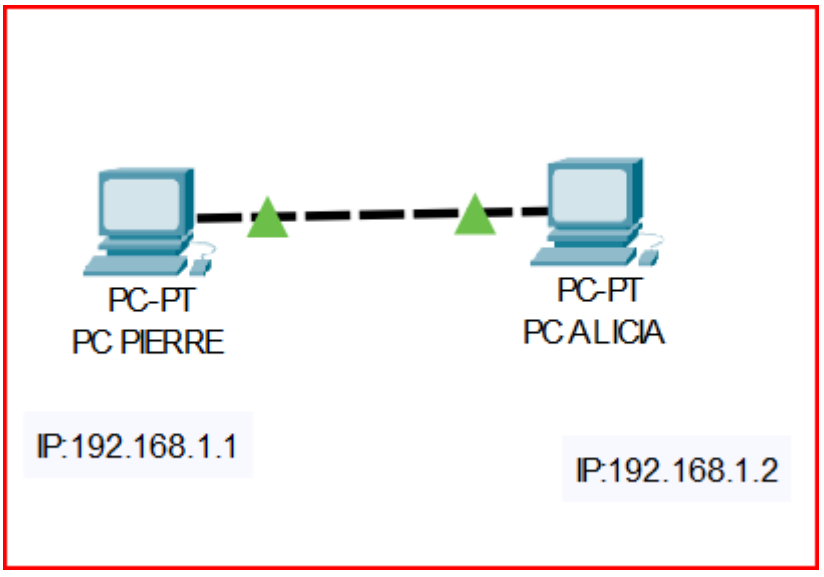
Voici la ligne de commande que j ai utiliser pour vérifier l' id de la machine



Job 6

Maintenant, testez si la connectivité est bonne entre le PC de Pierre et celui d'Alicia, en utilisant la commande Ping.

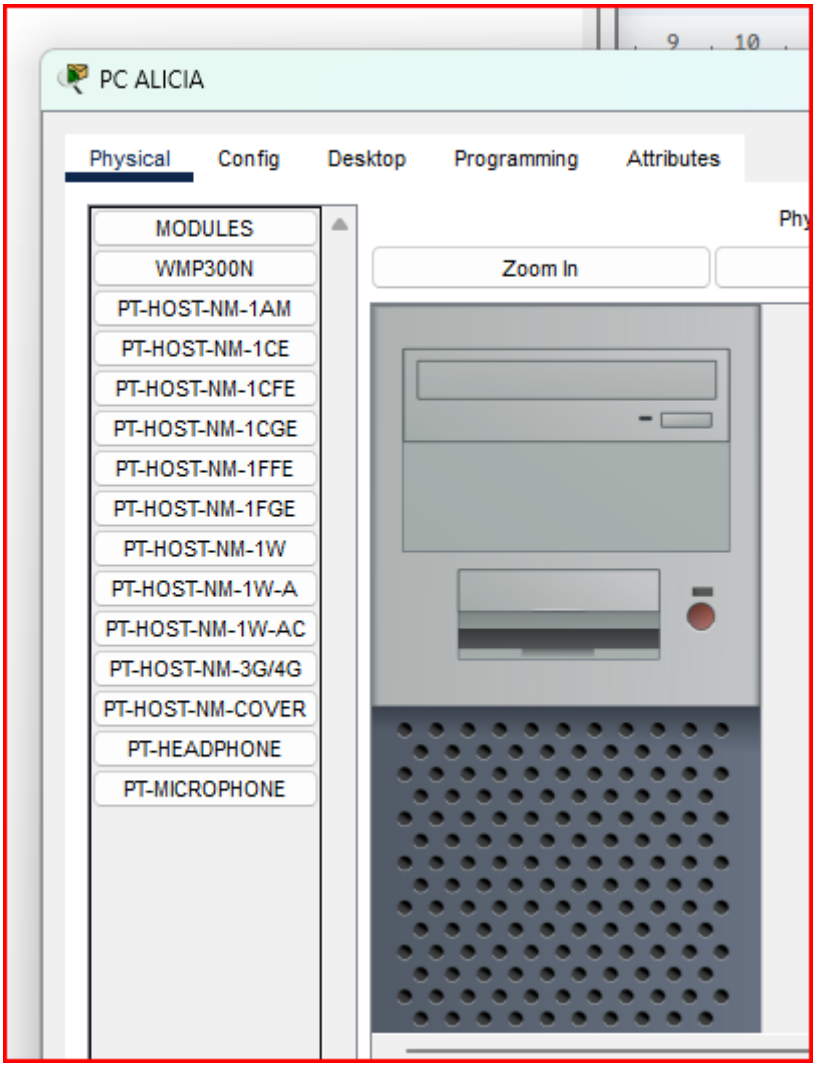
➔ Quelle est la commande permettant de Ping entre des PC ?



Job 7

Éteignez le PC de Pierre. Utilisez le terminal du PC d'Alicia et PING le PC le Pierre.

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

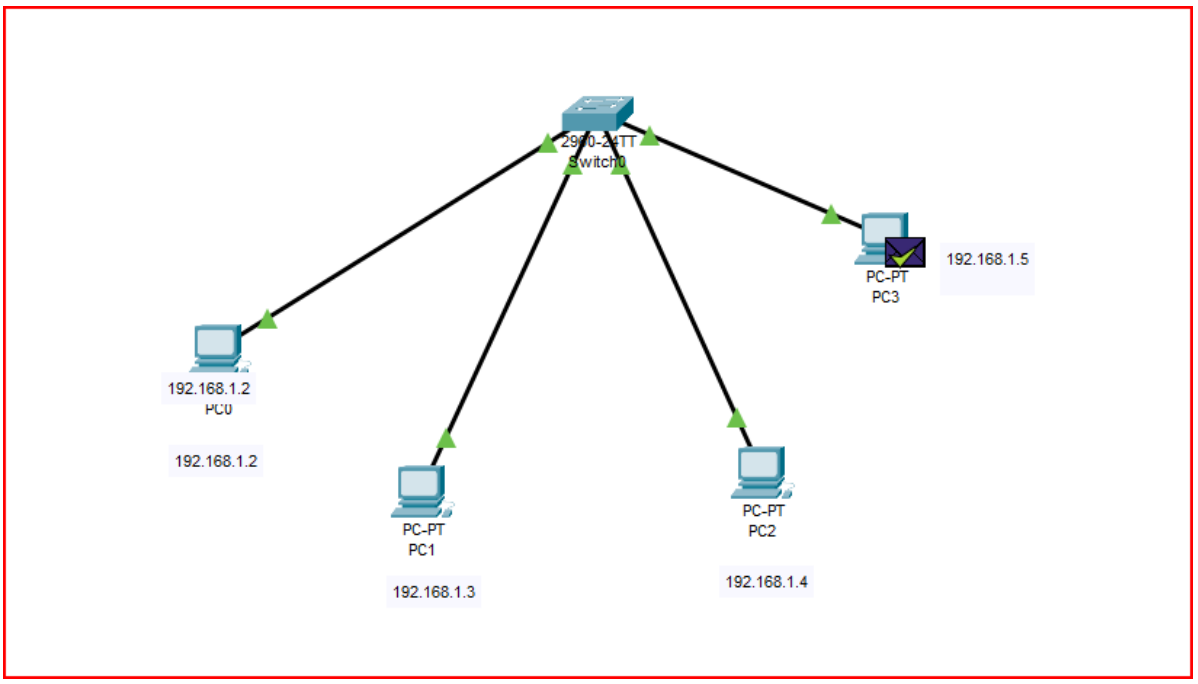


➔ Expliquez pourquoi.

j’ai connecté l' adresse ip de alicia sur le pc avec une carte réseaux et je configurer le bouton pour quand je appuis sa éteint et ça s'allume

Job 8

Agrandissez votre sous réseau avec cinq ordinateurs, et configurez vos ordinateurs sur
le même réseau. Vérifiez qu’ils soient tous bien connectés en affectant un PING en utilisant le terminal prompt.



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

- Un hub est un dispositif simple qui opère au niveau de la couche physique du modèle OSI (couche 1).
- Il transmet les données à tous les ports sans distinction, ce qui signifie que lorsque des données arrivent à un port, elles sont envoyées à tous les autres ports du hub.
- Les hubs sont peu intelligents et ne tiennent pas compte des adresses MAC (Media Access Control) des appareils connectés.
- Ils sont souvent utilisés pour étendre un réseau physique, mais ils ne sont pas efficaces pour gérer le trafic, car ils créent des collisions dans le réseau, ce qui peut entraîner des performances médiocres.

- Un switch est un dispositif plus intelligent qui opère au niveau de la couche de liaison de données du modèle OSI (couche 2).
- Il examine les adresses MAC des appareils connectés pour déterminer à quel port envoyer les données, ce qui signifie qu'il ne diffuse pas les données sur tous les ports comme le fait un hub.
- Les switches sont plus efficaces que les hubs en termes de gestion du trafic, car ils minimisent les collisions et offrent un débit plus élevé.
- Ils sont couramment utilisés dans les réseaux locaux (LAN) pour connecter de multiples appareils.

Un hub, dans le contexte des réseaux informatiques, est un dispositif matériel qui permet de connecter plusieurs périphériques (comme des ordinateurs, des imprimantes ou d'autres équipements) au sein d'un réseau local (LAN). Il fonctionne en agissant comme un concentrateur de données, où il reçoit les données provenant d'un périphérique et les transmet à tous les autres périphériques connectés. Voici comment un hub fonctionne:

Réception des données : Lorsqu'un périphérique connecté envoie des données au hub, celui-ci les reçoit.
Diffusion : Le hub transmet ensuite ces données à tous les autres périphériques connectés, qu'ils en aient besoin ou non. Il ne fait pas de distinction entre les destinataires, ce qui signifie que tous les périphériques reçoivent les données.

➔ Avantages des hubs :

Simplicité : Les hubs sont simples à configurer et à utiliser. Il n'y a généralement pas besoin de configuration complexe.
Coût : Les hubs sont généralement moins chers que d'autres dispositifs de réseau, comme les commutateurs (switches).

Inconvénients des hubs :

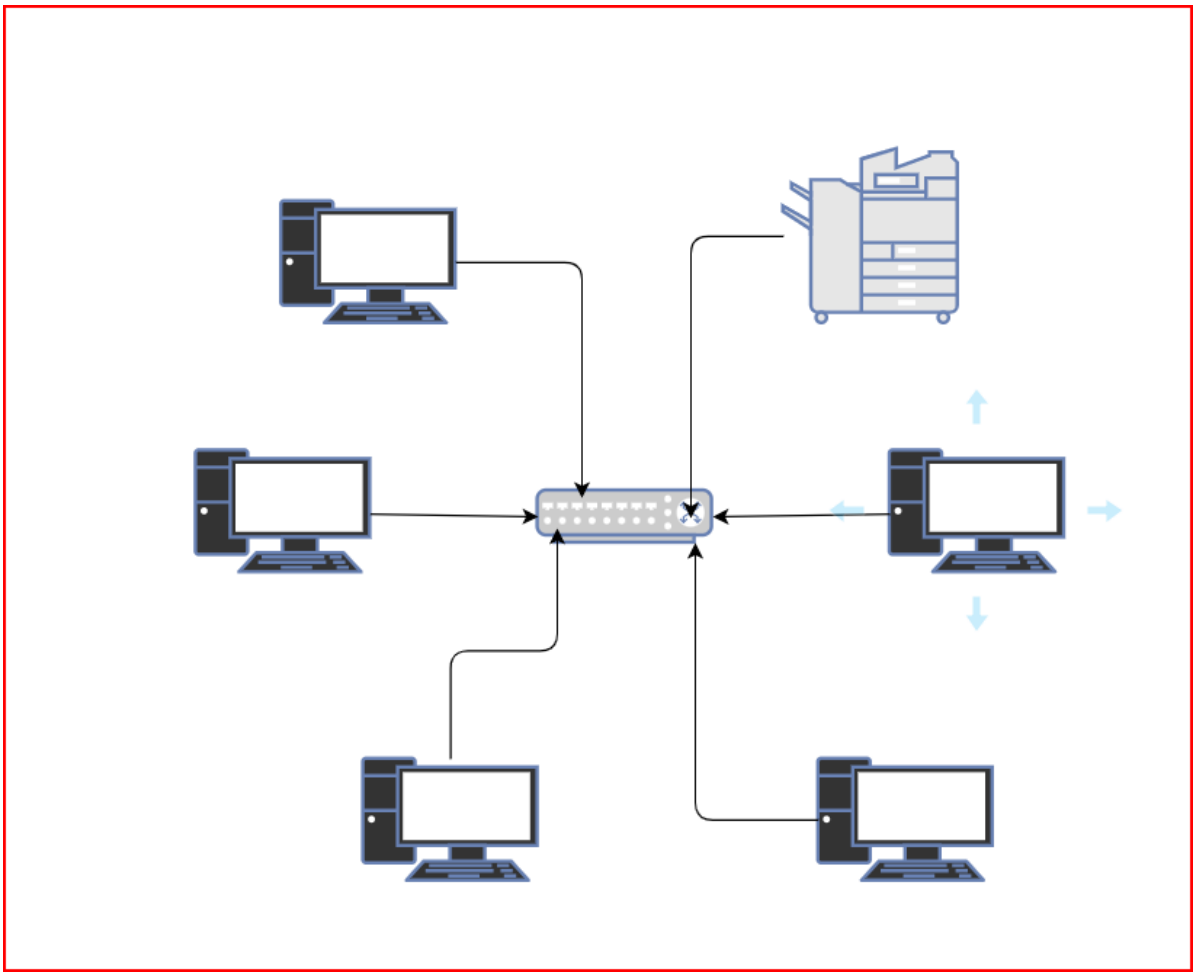
Inefficacité : L'envoi de données à tous les périphériques connectés, même s'ils n'en ont pas besoin, peut entraîner une utilisation inefficace de la bande passante du réseau.
Collision de données : Dans les réseaux Ethernet, les hubs peuvent entraîner des collisions de données, car plusieurs périphériques peuvent essayer de transmettre des données en même temps. Cela peut réduire les performances du réseau.
Manque de sécurité : Les données sont diffusées à tous les périphériques, ce qui signifie que n'importe quel périphérique connecté peut potentiellement intercepter les données destinées à d'autres périphériques, ce qui peut poser des problèmes de sécurité.

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

Apprendre les adresses MAC : Lorsqu'un commutateur est mis en service, il démarre avec une table de commutation vide. Au fur et à mesure que les dispositifs sont connectés au commutateur et envoient des trames, le commutateur apprend les adresses MAC de ces dispositifs. Il enregistre ces adresses MAC dans sa table de commutation.
Table de commutation : La table de commutation est une liste qui associe chaque adresse MAC à un port spécifique du commutateur. Ainsi, le commutateur sait par quel port se trouve chaque dispositif sur le réseau.

Job 9

Ajoutez une imprimante. Vérifiez qu’elle soit bien connectée. Réalisez un schéma de
votre réseau en utilisant le logiciel de votre choix. Celui-ci devra représenter la topologie
et la configuration de votre réseau, en incluant les composants (ordinateurs,
commutateurs, ...). Ensuite, identifiez au moins trois avantages importants d'avoir un
schéma et ajoutez le schéma ainsi que vos explications sur votre documentation.



*

Job 10

Tous vos ordinateurs sont maintenant connectés. Mais, c'est à vous de renseigner à la
main les différentes adresses IP de votre réseau.
Vous allez donc mettre en place un serveur DHCP, pour permettre la distribution
automatique d'adresse IP.
Cela va permettre aux ordinateurs de pouvoir communiquer entre eux sans que vous
adressez des IP fixes.

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

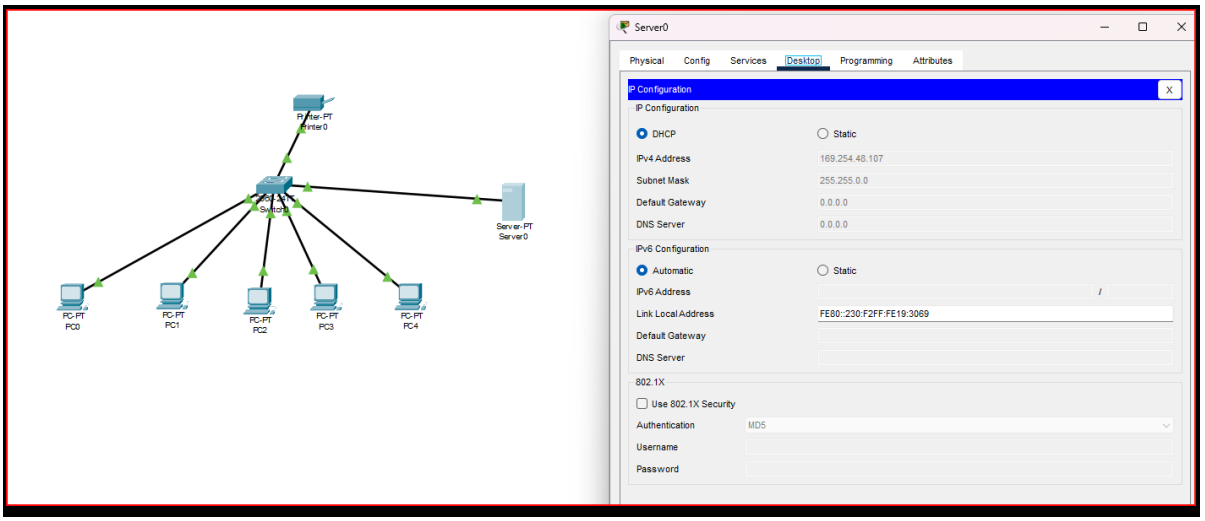
IP statique :

- Une adresse IP statique est configurée manuellement par un administrateur réseau.
- Elle ne change pas tant que l'administrateur ne la modifie pas manuellement.
- Les adresses IP statiques sont généralement utilisées pour des périphériques réseau critiques tels que les serveurs, les routeurs ou les imprimantes, car elles garantissent que ces périphériques ont toujours la même adresse IP.

Les adresses IP statiques sont plus faciles à gérer, mais elles nécessitent une configuration manuelle pour chaque périphérique.Adresse.

Adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) :

- DHCP est un protocole de réseau qui attribue automatiquement des adresses IP aux périphériques sur un réseau.
- L'attribution est gérée par un serveur DHCP, qui attribue des adresses IP aux périphériques en fonction de règles prédéfinies.
- Les adresses IP attribuées par DHCP sont temporaires et peuvent changer chaque fois qu'un périphérique se connecte au réseau. Cependant, le serveur DHCP peut être configuré pour attribuer la même adresse IP à un périphérique particulier pendant un certain temps (ce que l'on appelle une "bail" DHCP).
- Les adresses IP attribuées par DHCP sont couramment utilisées pour les ordinateurs de bureau, les ordinateurs portables, les smartphones et d'autres périphériques qui se connectent régulièrement au réseau.



Job 11

Commençons l’adressage réseau pour voir comment ça fonctionne !
On vous a attribué une adresse réseau de classe A 10.0.0.0.
On vous demande de
créer 21 sous-réseaux :

Il doit prendre en charge :
- 1 sous-réseau de 12 hôtes
- 5 sous-réseaux de 30 hôtes
- 5 sous-réseaux de 120 hôtes
- 5 sous-réseaux de 160 hôtes

12 hôtes

10.0.0.2 à 10.0.0.13
255.255.255.243

30 hôtes

10.1.0.1 à 10.1.0.30
255.255.255.225

30 hôtes

10.2.0.1 à 10.2.0.30
255.255.255.225

30 hôtes

10.3.0.1 à 10.3.0.30
255.255.255.225

30 hôtes

10.4.0.1 à 10.4.0.30
255.255.255.225

30 hôtes

10.5.0.1 à 10.5.0.30
255.255.255.225

120 hôtes

10.6.0.1 à 10.6.0.120
255.255.255.135

120 hôtes

10.7.0.1 à 10.7.0.120
255.255.255.135

120 hôtes

10.8.0.1 à 10.8.0.120
255.255.255.135

120 hôtes

10.9.0.1 à 10.9.0.120
255.255.255.135

120 hôtes

10.10.0.1 à 10.10.0.120
255.255.255.135

160 hôtes

10.11.0.1 à 10.11.0.160
255.255.255.95

160 hôtes

10.12.0.1 à 10.12.0.160
255.255.255.95

160 hôtes

10.13.0.1 à 10.13.0.160
255.255.255.95

160 hôtes

10.14.0.1 à 10.14.0.160
255.255.255.95

160 hôtes

10.15.0.1 à 10.15.0.160
255.255.255.95

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

Le choix de l’adresse 10.0.0.0 de classe se fait principalement pour sa large disponibilité d’adresse IP. Les réseaux de classe A peuvent prendre en charge un grand nombre d'hôtes (environ 16 millions).

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

Les différentes classes d'adresses IP (A, B, C, D et E) définissent des plages d'adresses IP spécifiques qui sont utilisées pour diverses fins dans le cadre du protocole Internet (IP). Chaque classe a ses propres caractéristiques et est destinée à des types

de réseaux spécifiques. Voici un aperçu des principales différences entre les classes d'adresses IP :

Classe A :

Plage d'adresses : 1.0.0.0 à 126.0.0.0
Masque de sous-réseau : 255.0.0.0
Utilisation : Les adresses de classe A sont principalement utilisées pour les réseaux de grande taille. Le premier octet identifie le réseau, tandis que les trois octets restants sont utilisés pour les hôtes. Les réseaux de classe A peuvent prendre en charge un grand nombre d'hôtes (environ 16 millions).

Classe B :

Plage d'adresses : 128.0.0.0 à 191.0.0.0
Masque de sous-réseau : 255.255.0.0
Utilisation : Les adresses de classe B sont utilisées pour les réseaux de taille moyenne. Les deux premiers octets identifient le réseau, tandis que les deux derniers octets sont utilisés pour les hôtes. Les réseaux de classe B peuvent prendre en charge un nombre considérable d'hôtes (environ 65 000).

Classe C :

Plage d'adresses : 192.0.0.0 à 223.0.0.0
Masque de sous-réseau : 255.255.255.0
Utilisation : Les adresses de classe C sont utilisées pour les réseaux de petite taille. Les trois premiers octets identifient le réseau, tandis que le dernier octet est utilisé pour les hôtes. Les réseaux de classe C prennent en charge un nombre limité d'hôtes (254 hôtes au maximum).

Classe D :

Plage d'adresses : 224.0.0.0 à 239.0.0.0
Masque de sous-réseau : Non applicable
Utilisation : Les adresses de classe D sont réservées pour la multidiffusion (broadcast sélectif) et ne sont pas utilisées pour l'adressage des hôtes individuels.

Classe E :

Plage d'adresses : 240.0.0.0 à 255.0.0.0
Masque de sous-réseau : Non applicable
Utilisation : Les adresses de classe E sont réservées à des fins expérimentales et ne sont pas couramment utilisées dans les réseaux publics.

En résumé, les différentes classes d'adresses IP sont conçues pour répondre aux besoins de réseaux de différentes tailles. Les classes A, B et C sont les plus couramment utilisées dans les réseaux IP, tandis que les classes D et E ont des utilisations spéciales. Il convient de noter qu'avec l'épuisement des adresses IPv4, les plages d'adresses IP privées, telles que celles de la classe A (10.0.0.0 à 10.255.255.255), sont souvent utilisées pour créer des réseaux privés et éviter la pénurie d'adresses IP publiques. IPv6, une nouvelle version du protocole IP, a été développée pour remédier à la pénurie d'adresses IPv4.

Job 12

1) Couche Physique : Cette couche s'occupe de la transmission des signaux bruts sur un support physique, comme des câbles ou des ondes électromagnétiques. Elle définit les caractéristiques physiques du support, telles que la topologie, les connecteurs, et les taux de transmission. Fibre optique / Wi-Fi / Routeur / Câble RJ45.

2) Couche Liaison de Données : La couche liaison de données gère la communication entre des dispositifs directement connectés. Elle est responsable de la détection et de la correction d'erreurs, du contrôle d'accès au support, et de la segmentation des données en trames. Ethernet / MAC / Fibre optique / PPTP / Wi-Fi / Routeur / Câble RJ45.

3) Couche Réseau : La couche réseau est chargée de la transmission de données à travers différents réseaux. Elle prend en charge le routage des données et l'acheminement des paquets à travers des réseaux interconnectés. Fibre optique / PPTP / IPv4 / Wi-Fi / IPv6 / Routeur / HTML.

4) Couche Transport : La couche transport assure la livraison fiable et ordonnée des données entre deux dispositifs. Elle gère également le contrôle de flux et la correction d'erreurs, si nécessaire. TCP / SSL/TSL / UDP / HTML.

5) Couche Session : La couche session établit, gère et termine les sessions de communication entre des applications sur différents dispositifs. Elle peut également gérer la synchronisation et la reprise de sessions en cas de défaillance

6) Couche Présentation : La couche présentation est responsable de la traduction, de la compression, du chiffrement et de la mise

en forme des données afin de garantir qu'elles sont comprises par les applications de chaque côté de la communication.

7) La Couche Application : La couche application est la couche la plus haute du modèle OSI. Elle fournit une interface pour les applications utilisateur, telles que les navigateurs web, les clients de messagerie électronique et d'autres logiciels. Elle gère la communication directe avec les applications et leur interaction avec les couches inférieures. SSL/TSL / UDP / FTP / HTML.