

Runtrack Réseau

Job 2

→ ****Qu'est-ce qu'un réseau ?****

Un réseau est un ensemble d'ordinateurs, de serveurs, d'appareils mobiles, ou même d'autres dispositifs connectés entre eux, permettant de partager des ressources, d'échanger des données, et de communiquer. Ces connexions peuvent être établies à travers des fils (comme l'Ethernet) ou sans fil (comme le Wi-Fi).

→ ****À quoi sert un réseau informatique ?****

Un réseau informatique permet de :

1. ****Partager des ressources**** : cela inclut l'accès à Internet, l'utilisation de fichiers et d'imprimantes partagés, etc.
2. ****Échanger des données**** : les utilisateurs peuvent envoyer et recevoir des informations, comme des emails ou des fichiers.
3. ****Communiquer**** : outre les emails, cela inclut la messagerie instantanée, la visioconférence, etc.
4. ****Centraliser la gestion**** : par exemple, dans un réseau d'entreprise, il est plus facile de gérer la sécurité, les mises à jour logicielles, etc., à partir d'un point central.
5. ****Accéder à des applications et des services**** : de nombreuses applications d'entreprise sont hébergées sur des serveurs réseau, permettant aux utilisateurs d'y accéder via le réseau.
6. ****Backup et récupération**** : facilite la mise en place de solutions de sauvegarde centralisées et de plans de récupération après sinistre.

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

Voici une liste des composants couramment utilisés pour construire un réseau, avec leurs fonctions :

Câbles et connecteurs : tels que les câbles Ethernet (RJ-45) pour connecter physiquement les dispositifs.

Cartes réseau : aussi connues sous le nom de NIC (Network Interface Card), elles permettent à un ordinateur ou un autre dispositif de se connecter à un réseau.

Switch (ou commutateur)** : c'est un dispositif qui connecte plusieurs dispositifs au sein d'un réseau local (LAN) et utilise des adresses MAC pour acheminer les paquets de données vers le bon destinataire.

Routeur : il dirige le trafic entre différents réseaux. Par exemple, un routeur domestique relie généralement un réseau local (LAN) à Internet.

Points d'accès sans fil (WAP ou Wireless Access Points)** : ils permettent aux dispositifs de se connecter au réseau via Wi-Fi.

Modem : c'est un dispositif qui permet la connexion à Internet, en convertissant les signaux numériques de votre réseau en signaux analogiques pour la transmission par des lignes téléphoniques, câbles coaxiaux ou liaisons satellite.

Firewall (pare-feu) : il peut être matériel ou logiciel et est conçu pour protéger un réseau en filtrant le trafic entrant et sortant.

Serveurs : ce sont des ordinateurs puissants conçus pour stocker des données, exécuter des applications et fournir des ressources aux autres ordinateurs du réseau.

Répéteurs et amplificateurs : utilisés dans les grands réseaux pour amplifier le signal et étendre la portée du réseau.

Chaque composant joue un rôle crucial pour garantir que les données soient acheminées correctement et efficacement à travers le réseau.

Job 3

Le câble cat6 dit câble copper ou câble Ethernet permet un échange croisé des données entre les 2 PC,

Job 4

→ Qu'est-ce qu'une adresse IP ?

Une adresse IP (Internet Protocol) est une étiquette numérique unique assignée à chaque appareil connecté à un réseau informatique utilisant le protocole IP pour la communication.

→ À quoi sert un IP ?

Cette adresse sert deux fonctions principales :

- l'identification de l'hôte ou du réseau d'interface. Elle identifie de manière unique un dispositif sur un réseau. C'est comparable à une adresse postale pour les maisons, permettant à chaque dispositif d'être distingué des autres.
- La localisation de l'adresse.
- Les adresses IP facilitent le routage des paquets de données sur le réseau. Lorsqu'un dispositif souhaite envoyer des données à un autre, il utilise l'adresse IP destinataire pour transmettre l'information correctement.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control) est une adresse physique unique associée à l'interface réseau d'un dispositif, comme la carte réseau. Généralement inscrite dans la ROM (Read-Only Memory).

Contrairement aux adresses IP, qui peuvent être modifiées et sont dépendantes du réseau, les adresses MAC sont uniques et restent constantes, bien qu'elles puissent être usurpées ou modifiées via des méthodes logicielles.

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

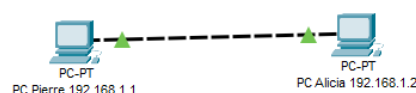
IP Publique: C'est une adresse IP unique qui est assignée à un dispositif réseau pour le rendre directement accessible sur Internet. Si vous avez un site web ou un serveur, il sera accessible via une IP publique. Chaque IP publique est unique dans l'ensemble d'Internet.

IP Privée : C'est une adresse IP utilisée à l'intérieur d'un réseau privé. Elles ne sont pas routables sur Internet public, ce qui signifie qu'elles ne peuvent pas communiquer directement avec les dispositifs sur Internet sans un intermédiaire, tel qu'un routeur ou un pare-feu. Des plages spécifiques d'adresses IP ont été réservées pour une utilisation privée par les dispositifs à l'intérieur des réseaux locaux. Par exemple, les adresses commençant par "192.168." sont toujours des adresses privées.

En résumé, les adresses IP sont essentielles pour la communication entre les dispositifs sur les réseaux, tandis que les adresses MAC assurent une identification unique au niveau de l'interface matériel. Les IP publiques permettent aux dispositifs de communiquer sur l'Internet public, tandis que les IP privées sont utilisées à l'intérieur des réseaux locaux.

→ Quelle est l'adresse de ce réseau ?

Voici l'adresse : 192.168.1.0



IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

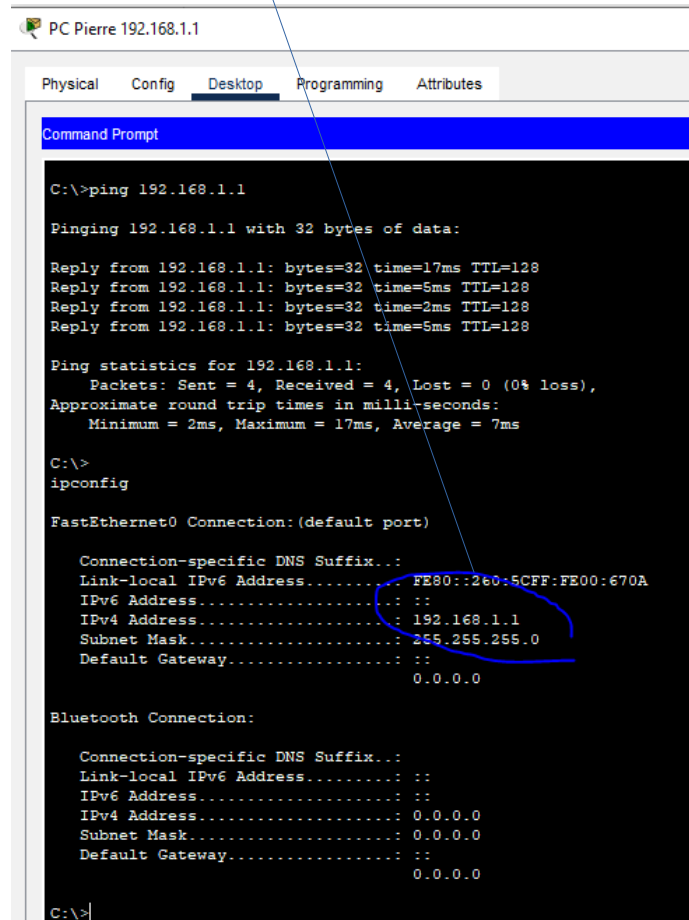
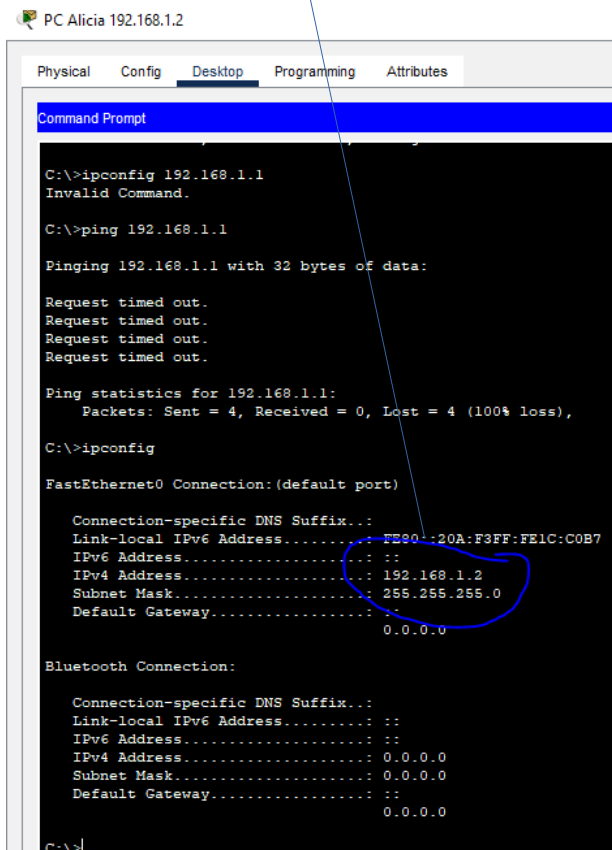
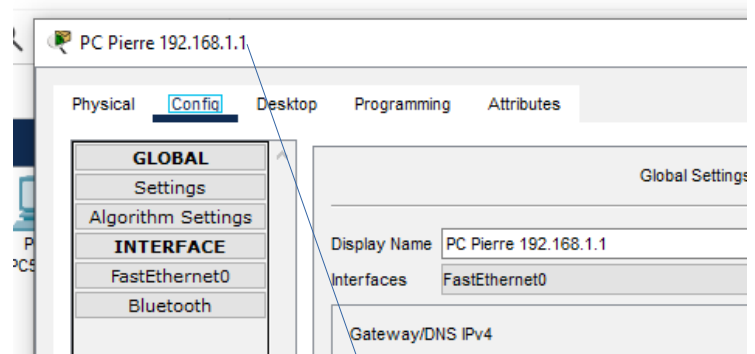
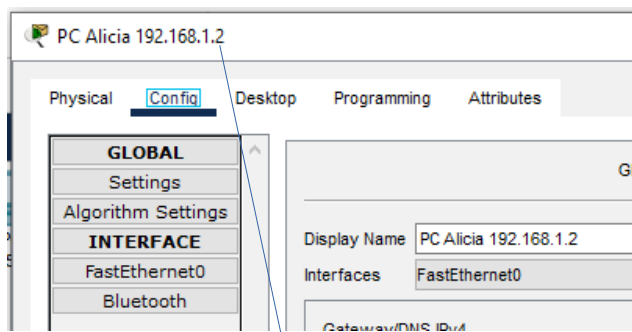
IPv6 Address: /

Link Local Address: FE80::260:5CFF:FE00:670A

Default Gateway:

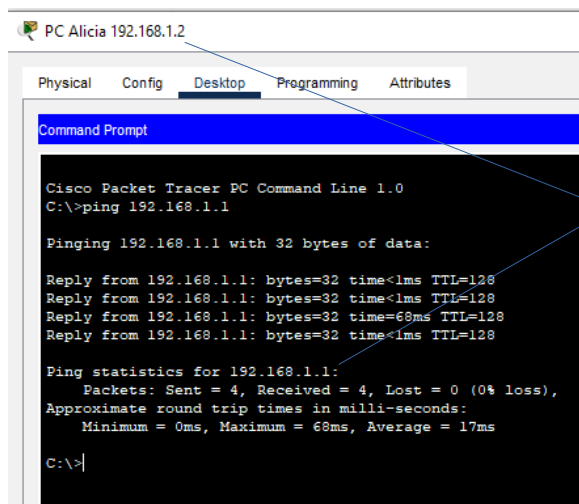
DNS Server:

Job 5



Job 6

→ Quelle est la commande permettant de Ping entre des PC ?
Ping adresse

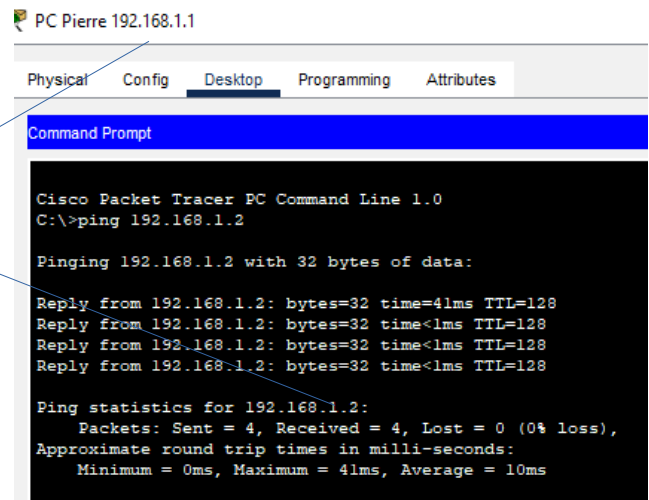


```
PC Alicia 192.168.1.2
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

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=68ms 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 = 68ms, Average = 17ms
C:\>
```



```
PC Pierre 192.168.1.1
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=41ms 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

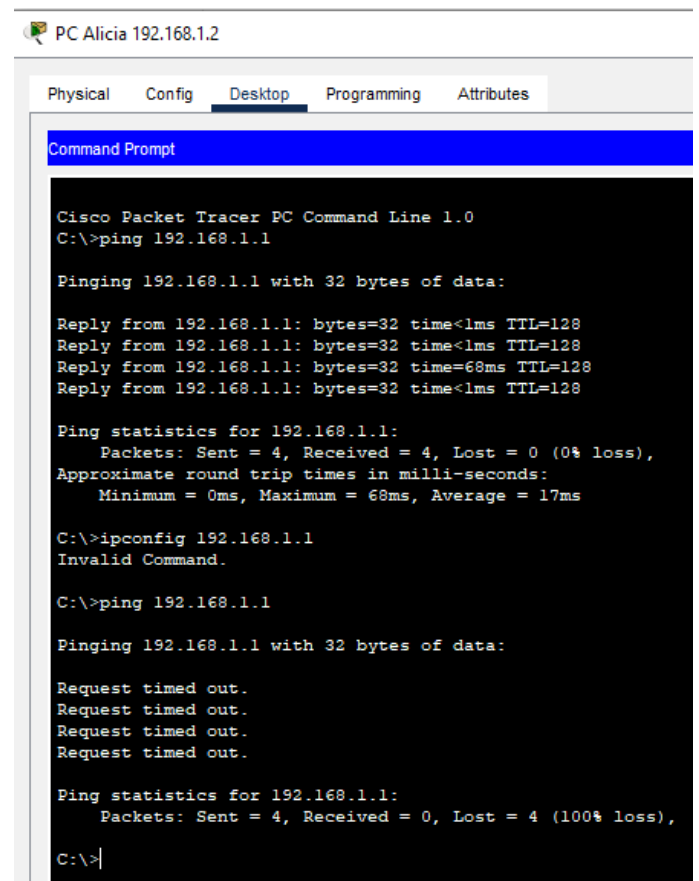
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 41ms, Average = 10ms
C:\>
```

Job 7

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

Non, car il n'y a pas de courant, et donc de carte mère active, donc pas de bios pas de ROM pas de carte réseaux active etc pas de possibilité de réception.

L'ordinateur d'Alicia envoie une requête ARP pour déterminer l'adresse MAC à l'adresse IP. Si l'ordinateur de Pierre est éteint, il ne répondra pas à cette requête ARP.



```
PC Alicia 192.168.1.2
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=68ms 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 = 68ms, Average = 17ms

C:\>ipconfig 192.168.1.1
Invalid Command.

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),
C:\>
```

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 ?

Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée. C'est comme une multiprise. Un hub contient plusieurs ports. Lorsqu'un paquet est reçu sur un port, celui-ci est envoyé aux autres ports afin que tous les segments du réseau local puissent accéder à tous les paquets. Le hub n'a aucun moyen de distinguer vers quel port une trame doit être envoyée.

Contrairement à un concentrateur (hub) ou à un commutateur (switch) Ethernet qui s'occupe de la transmission de trames, un routeur doit acheminer des paquets vers d'autres réseaux jusqu'à ce que ceux-ci atteignent finalement leur destination. L'une des caractéristiques principales d'un paquet est qu'il contient non seulement des données mais aussi l'adresse IP de destination.

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

Un hub reçoit un paquet sur l'un de ses ports et le diffuse à tous les autres ports sans discrimination.

Avantages :

Simplicité : Facile à installer et à configurer.

Coût : Généralement moins cher qu'un switch.

Inconvénients :

Bande passante : Puisque tous les paquets sont diffusés à tous les ports, cela peut entraîner une congestion du réseau.

Pas de segmentation : Tous les dispositifs sont sur le même segment de collision, ce qui réduit les performances.

Sécurité : Comme les paquets sont diffusés à tous, un dispositif malveillant peut facilement "écouter" le trafic.

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

Avantages :

Efficacité : Les paquets sont envoyés uniquement à l'appareil destinataire, ce qui réduit la congestion du réseau.

Segmentation : Chaque port est essentiellement son propre segment de collision.

Tableau d'adresses MAC : Permet de savoir quel appareil est connecté à quel port.

Support pour VLANs : Les switches avancés peuvent gérer les VLANs pour segmenter logiquement le réseau.

Inconvénients :

Coût : Généralement plus cher qu'un hub.

Complexité : Peut nécessiter une configuration plus avancée, surtout pour des fonctionnalités plus complexes.

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

Lorsqu'un switch reçoit un paquet, il examine l'adresse MAC de destination du paquet. Il utilise son tableau d'adresses MAC pour déterminer le port sur lequel l'adresse MAC de destination est connectée. Le paquet est alors transmis uniquement sur ce port.

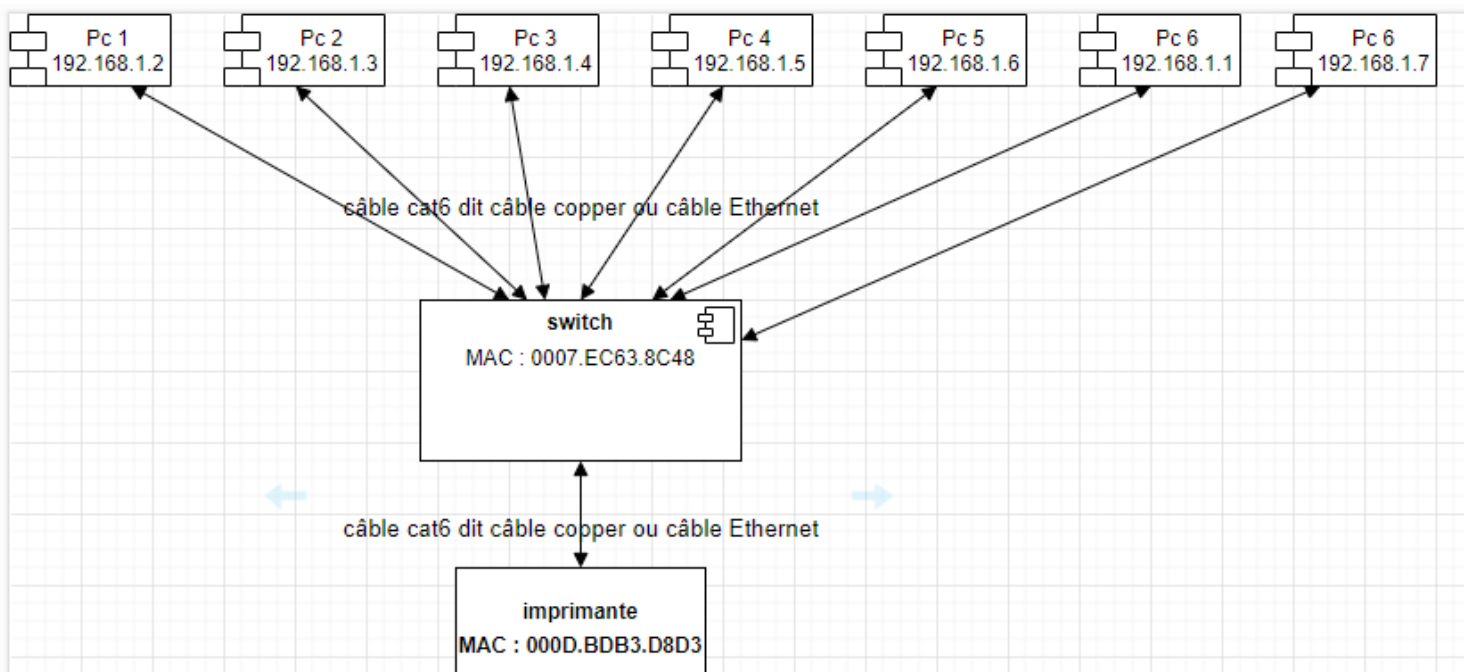
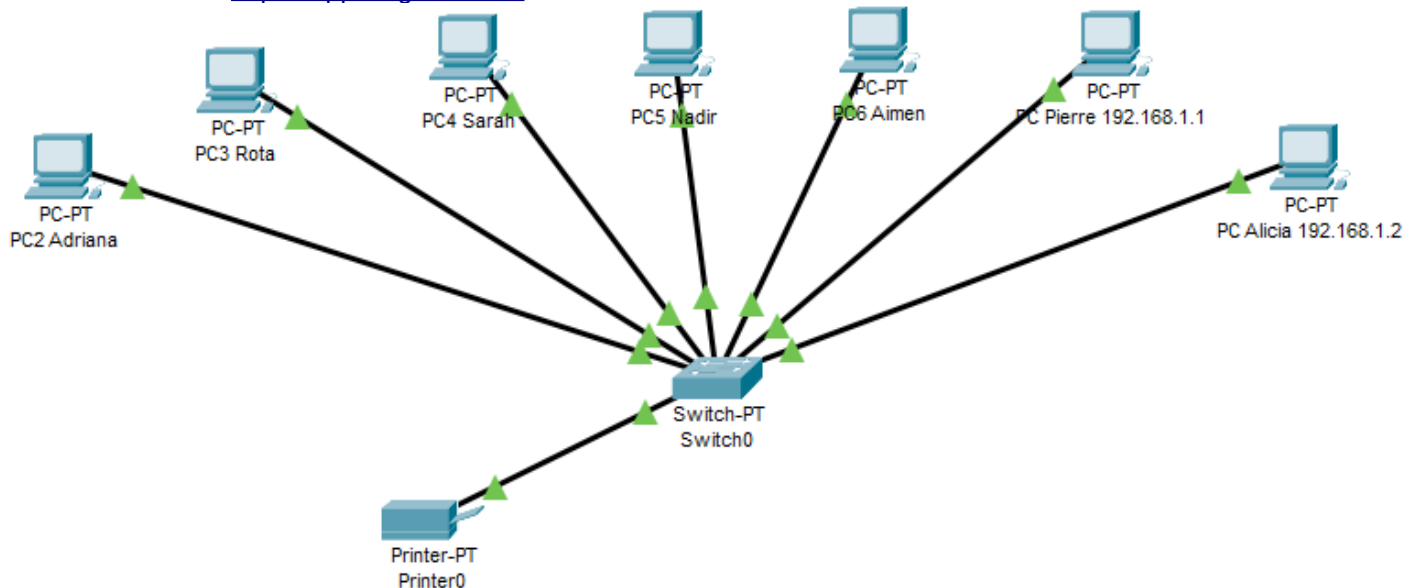
Si l'adresse MAC de destination n'est pas dans le tableau du switch, ou si elle est associée à un port qui n'est plus actif, le switch diffuse le paquet sur tous les ports (comme le ferait un hub). Cependant, une fois qu'il reçoit une réponse de l'appareil de destination, il met à jour son tableau d'adresses MAC avec l'adresse MAC de l'appareil et le port associé.

Ainsi, un switch gère efficacement le trafic réseau en se souvenant des appareils (adresses MAC) connectés à ses différents ports et en acheminant les paquets uniquement vers les appareils destinataires.

Job 9

Réalisez un schéma de votre réseau en utilisant le logiciel de votre choix.

J'utilise Draw io sur <https://app.diagrams.net/>



Un schéma de réseau d'un parc informatique, aussi appelé plan ou topologie du réseau, Voici les principaux avantages d'avoir un tel schéma :

1. ****Compréhension claire**** : Un schéma offre une vue d'ensemble du réseau, facilitant la compréhension de sa structure et de son fonctionnement.
2. ****Facilité de dépannage**** : En cas de problème, le schéma de réseau permet d'identifier rapidement les éléments ou les connexions susceptibles d'être en cause. Cela accélère la résolution des problèmes.
3. ****Planification et mise à niveau**** : Avec un schéma en main, il est plus facile de planifier des extensions, des mises à niveau ou des modifications du réseau en visualisant les zones potentielles d'impact.

4. ****Documentation**** : Un schéma sert de documentation de référence pour le réseau, ce qui est essentiel pour les nouveaux membres de l'équipe ou les prestataires externes qui peuvent intervenir.
5. ****Optimisation des performances**** : En visualisant la topologie du réseau, on peut identifier des goulots d'étranglement potentiels ou des configurations inefficaces et apporter les ajustements nécessaires.
6. ****Gestion de la sécurité**** : Le schéma permet d'identifier les points d'accès, les zones sensibles ou les équipements cruciaux. Cela facilite la mise en place de mesures de sécurité ciblées.
7. ****Gestion des coûts**** : En ayant une vision claire du réseau et de ses composants, il est possible d'optimiser les coûts en évitant les dépenses inutiles ou en identifiant les équipements obsolètes à remplacer.
8. ****Formation**** : Pour les nouveaux employés ou pour la formation interne, un schéma de réseau est un outil pédagogique qui facilite l'apprentissage de la structure et du fonctionnement du réseau.
9. **Communication**: Que ce soit pour présenter un projet à la direction, discuter avec des fournisseurs ou échanger avec d'autres départements, un schéma facilite la communication en offrant une base visuelle commune.
10. **Continuité des activités** : En cas d'incident majeur (catastrophe naturelle, incendie, etc.), disposer d'un schéma de réseau détaillé est précieux pour la reconstitution ou la reconfiguration rapide du réseau.

Pour profiter pleinement de ces avantages, il est essentiel de maintenir le schéma à jour, reflétant fidèlement l'état actuel du réseau et des équipements.

Job 10

(Réponse aidé par chatgpt mais j'ai bien compris).

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

Les adresses IP jouent un rôle crucial dans la communication au sein des réseaux. Elles peuvent être assignées de différentes manières, et la manière dont elles sont assignées peut avoir des implications pour le réseau et ses périphériques. Voici les différences entre une adresse IP statique et une adresse IP attribuée par DHCP :

Adresse IP statique :

1. ****Définition**** : Une adresse IP statique est manuellement configurée sur un périphérique par un administrateur réseau. Une fois définie, elle ne change généralement pas, sauf si elle est manuellement reconfigurée.
2. ****Utilisation**** : Elle est souvent utilisée pour les serveurs, les imprimantes réseau, les routeurs et d'autres dispositifs pour lesquels une adresse IP constante est nécessaire pour que les utilisateurs ou d'autres dispositifs puissent y accéder de manière fiable.
3. ****Avantages**** :
 - ****Fiabilité**** : Les dispositifs qui ont besoin d'être accessibles en permanence peuvent bénéficier d'une adresse IP constante.
 - ****Pas de dépendance à un serveur DHCP**** : Le dispositif continuera à avoir la même adresse même si le serveur DHCP est hors ligne.
4. ****Inconvénients**** :
 - ****Configuration manuelle**** : Cela peut être chronophage, surtout dans les grands réseaux, et nécessite des connaissances techniques.
 - ****Risque de conflits d'IP**** : Si un administrateur attribue accidentellement la même IP statique à deux dispositifs différents, cela peut entraîner un conflit d'IP.

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

Job 11

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

Une adresse IP de classe A dispose d'un seul octet pour identifier le réseau et de trois octets pour identifier les machines sur ce réseau. Un réseau de classe A peut comporter jusqu'à $2^3 \times 8 - 2$ postes, soit 224×2 , soit 16 777 214 terminaux.

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

Il existe cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E. Ces différentes classes ont chacune leurs spécificités quant à la répartition du nombre d'octets servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

- Classe A dispose d'une partie id comportant uniquement un seul octet.
- Classe B dispose d'une partie id comportant deux octets.
- Classe C dispose d'une partie id comportant trois octets.
- Classes D et E correspondent à des adresses IP particulières.

Sous-Réseau	Adresse Réseau	Plage IP	Adresse de diffusion	Masque de Sous-Réseau (binaire)	CIDR
1	10.0.0.0	10.0.0.1 - 10.0.0.14	10.0.0.15	11111111.11111111.11111111.1111 0000	/28
2	10.0.0.16	10.0.0.17 - 10.0.0.46	10.0.0.47	11111111.11111111.11111111.1110 0000	/27
3	10.0.0.48	10.0.0.49 - 10.0.0.78	10.0.0.79	11111111.11111111.11111111.1110 0000	/27
4	10.0.0.80	10.0.0.81 - 10.0.0.110	10.0.0.111	11111111.11111111.11111111.1110 0000	/27
5	10.0.0.112	10.0.0.113 - 10.0.0.142	10.0.0.143	11111111.11111111.11111111.1110 0000	/27
6	10.0.0.144	10.0.0.145 - 10.0.0.174	10.0.0.175	11111111.11111111.11111111.1110 0000	/27
7	10.0.0.176	10.0.0.177 - 10.0.1.46	10.0.1.47	11111111.11111111.11111111.1000 0000	/25
8	10.0.1.48	10.0.1.49 - 10.0.1.174	10.0.1.175	11111111.11111111.11111111.1000 0000	/25
9	10.0.1.176	10.0.1.177 - 10.0.2.46	10.0.2.47	11111111.11111111.11111111.1000 0000	/25
10	10.0.2.48	10.0.2.49 - 10.0.2.174	10.0.2.175	11111111.11111111.11111111.1000 0000	/25
11	10.0.2.176	10.0.2.177 - 10.0.3.46	10.0.3.47	11111111.11111111.11111111.1000 0000	/25
12	10.0.3.48	10.0.3.49 - 10.0.4.46	10.0.4.47	11111111.11111111.11111111.0000 0000	/24
13	10.0.4.48	10.0.4.49 - 10.0.5.46	10.0.5.47	11111111.11111111.11111111.0000 0000	/24
14	10.0.5.48	10.0.5.49 - 10.0.6.46	10.0.6.47	11111111.11111111.11111111.0000 0000	/24
15	10.0.6.48	10.0.6.49 - 10.0.7.46	10.0.7.47	11111111.11111111.11111111.0000 0000	/24
16	10.0.7.48	10.0.7.49 - 10.0.8.46	10.0.8.47	11111111.11111111.11111111.0000 0000	/24

Masque de Réseau (décimal) nombre d'hôtes

255.255.255.240 2^4 combinaisons -2 soit $16-2=14$ hôtes

255.255.255.224 2^5 combinaisons -2 soit $32-2=30$ hôtes

255.255.255.224 2^5 combinaisons -2 soit $32-2=30$ hôtes

255.255.255.224 2^5 combinaisons -2 soit $32-2=30$ hôtes

255.255.255.224 2^5 combinaisons -2 soit $32-2=30$ hôtes

255.255.255.128 2^7 combinaisons -2 soit $128-2=126$ hôtes

255.255.255.128 2^7 combinaisons -2 soit $128-2=126$ hôtes

255.255.255.128 2^7 combinaisons -2 soit $128-2=126$ hôtes

255.255.255.128 2^7 combinaisons -2 soit $128-2=126$ hôtes

255.255.255.128 2^7 combinaisons -2 soit $128-2=126$ hôtes

255.255.255.0 2^8 combinaisons-2 soit $256-2=254$ hôtes

255.255.255.0 2^8 combinaisons-2 soit $256-2=254$ hôtes

255.255.255.0 2^8 combinaisons-2 soit $256-2=254$ hôtes

255.255.255.0 2^8 combinaisons-2 soit $256-2=254$ hôtes

255.255.255.0 2^8 combinaisons-2 soit $256-2=254$ hôtes

Job 12

N° de couche	Nom de la couche	Description/Rôle	Matériels/ Protocoles associés	Exemples de Matériel	Relation entre Matériels
7	Application	Fournit une interface pour l'utilisateur.	HTML, FTP, <u>SSL/TLS</u>	PC portable, Serveur Web	Échange d'informations entre PC et serveurs via applications
6	Présentation	Traduit, chiffre et compresse les données pour la couche Session.	<u>SSL/TLS</u>	Serveur de chiffrement	Chiffrement des données entre le serveur et le PC
5	Session	Établit, maintient et termine les connexions.	<u>PPTP</u>	Serveur VPN	Établissement de sessions sécurisées entre PC et serveur VPN
4	Transport	Fournit le transfert de données fiable entre les points de terminaison.	<u>TCP, UDP</u>	PC portable, Serveur d'applications	Échange fiable de données entre PC et serveurs à l'aide de <u>TCP</u> ou <u>UDP</u>
3	Réseau	Établit, maintient et termine les connexions. Route des paquets.	IPv4, IPv6, routeur	Routeur, Firewall	Routage des paquets entre PC et serveurs
2	Liaison de données	Gère la transmission des trames entre les nœuds sur un médium.	Ethernet, MAC, Wi-Fi, <u>cable RJ45</u>	Switch, Carte réseau	Transmission des trames entre PC et serveurs via <u>switches</u>
1	Physique	Transmet les bits bruts sur le médium.	fibres optiques, <u>cable RJ45</u>	Hub, Câble RJ45	Connexion physique entre PC et serveurs via câbles

Job 13

→ Quelle est l'architecture de ce réseau ?
Il s'agit d'un réseau en étoile.

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

→ Déterminer le nombre de machines que l'on peut brancher sur ce réseau ?
253

→ Quelle est l'adresse de diffusion de ce réseau ?
192.168.10.255
Job 14

Job 14

Convertissez les adresse IP suivantes en binaires :

- 145.32.59.24 = 1001 0001 0010 0000 0011 1011 0001 1000
- 200.42.129.16 = 1100 1000 0010 1010 1000 0001 0001 0000
- 14.82.19.54 = 0000 1110 0101 0010 0001 0011 0011 0110

Job 15

→ Qu'est ce que le routage ?

Le routage est l'opération qui consiste à acheminer des données d'un point A vers un point B.

Le but est de trouver le chemin le plus court entre les points d'acheminement des paquets réseaux.

→ Qu'est ce qu'un gateway ?

Une "gateway" (ou "passerelle" en français) est un dispositif ou un logiciel qui sert d'intermédiaire entre deux réseaux informatiques distincts pour faciliter la communication entre eux.

→ Qu'est ce qu'un VPN ?

Un VPN ou Réseau Privé Virtuel en français, est un service ou une technologie qui permet de créer un réseau sécurisé et privé, même lorsque vous êtes connecté à Internet ou à un réseau public.

→ Qu'est ce qu'un DNS ?

Un DNS, ou Domain Name System en anglais, est un système informatique utilisé pour traduire les noms de domaine en adresses IP.