

La Plateforme

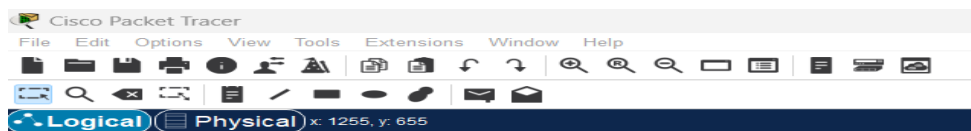
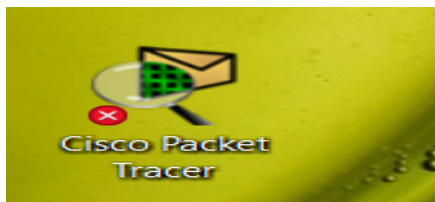
Ahmed Aouad

Bachelor IT, 1ère année.

Runtrack Réseau :

JOB 1 :

Télécharger et installer CISCO



JOB 2 :

→ Qu'est-ce qu'un réseau ?

Un réseau informatique est un groupement de deux ou plusieurs ordinateurs (ou autres appareils électroniques) permettant l'échange de données et le partage de ressources communes.

→ À quoi sert un réseau informatique ?

Le réseau informatique va permettre la mise en communication de différents dispositifs électroniques (ordinateurs, serveurs, téléphones...) afin de faciliter le transfert de données, le partage des ressources, l'accès à internet, la sauvegarde et la récupération de données..).

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

.Un ordinateur et autre dispositifs : l'ordinateur pc (disposant de carte réseau ethernet ou Wifi), téléphones, tablettes...

.Commutateur (switches) : Les commutateurs permettent de relier plusieurs appareils au sein d'un réseau local (LAN), il s'agit souvent d'un boîtier avec plusieurs ports ethernet.

.Câbles et connecteurs: Ils permettent de relier physiquement les appareils du réseau (câble ethernet, , prise RJ45...)

.Le Routeur : Le routeur sert de passerelle entre différents réseaux, comme votre réseau local et Internet. Il dirige les données entre ces réseaux, gère les adresses IP et offre des fonctions de sécurité.

.Le Modem : Un modem est un appareil qui convertit votre connexion entrante (câble coaxial, ligne téléphonique, fibre optique ou autre) en connexion Ethernet, qui permet à un routeur Wi-Fi de se connecter à Internet.

.Le Serveur : Un serveur est un ordinateur ou un programme informatique qui fournit des services ou des ressources à d'autres appareils ou programmes, appelés clients, au sein d'un réseau informatique. Sa fonction principale est de répondre aux requêtes des clients et de distribuer les informations demandées.

.Le fireWall ou pare-feux : Un pare-feu est un système de sécurité informatique qui contrôle et filtre le trafic réseau entre un réseau privé et un réseau public (comme Internet). Il agit comme une barrière pour empêcher l'accès non autorisé ou les menaces potentielles de pénétrer dans le réseau privé, tout en autorisant le trafic légitime à passer.

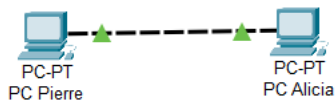
.Hub: Un hub Ethernet ou concentrateur Ethernet est un appareil informatique permettant de concentrer les transmissions Ethernet de plusieurs équipements sur un même support dans un réseau informatique local.

JOB 3 :

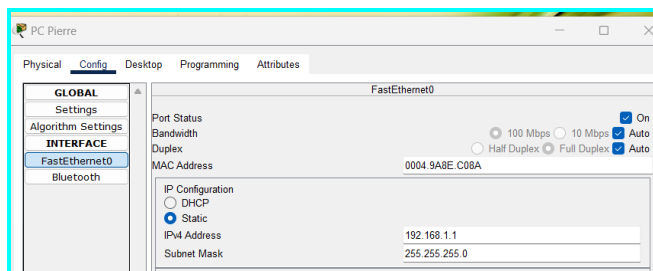
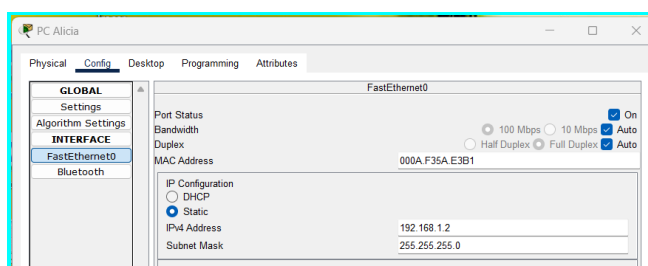
.Quels câbles avez-vous choisis pour relier les deux ordinateurs ?

Pour ce cas de figure, nous allons faire le choix du câble croisé, en effet un câble croisé connecte deux dispositifs du même type pour communiquer ensemble, comme un ordinateur à un autre ordinateur, ou un commutateur à un autre commutateur.

A la différence du câble droit qui lui connecte deux dispositifs différents l'un à l'autre, comme un ordinateur et un commutateur.



JOB 4 :



→ **Qu'est-ce qu'une adresse IP ?** Une adresse IP (Internet Protocol) est une série de chiffres qui identifie de manière unique un appareil sur un réseau IP.

→ **À quoi sert un IP ?** Une adresse IP permet de s'identifier et de localiser un appareil à un réseau. L'adresse IP permet également à deux machines de s'identifier et de dialoguer entre elles, en échangeant des données sur Internet.

→ **Qu'est-ce qu'une adresse MAC ?** Une adresse MAC (Media Access Control) est une adresse physique unique attribuée à chaque carte réseau d'un appareil. Contrairement à une adresse IP, une adresse MAC ne change pas et est spécifique à un appareil.

→ **Qu'est-ce qu'une IP publique et privée ?** Une adresse IP publique est l'adresse qui est visible sur Internet et utilisée pour identifier un appareil au niveau mondial. Chaque appareil connecté à Internet doit avoir une adresse IP publique unique.

Une adresse IP privée est utilisée à l'intérieur d'un réseau local (comme à la maison ou dans une entreprise). Les adresses IP privées sont souvent utilisées pour les appareils tels que les ordinateurs, smartphones... à l'intérieur d'un réseau local.

→ Quelle est l'adresse de ce réseau ? C'est l'adresse de sous réseau (subnet mask)
255.255.255.0

Subnet Mask	255.255.255.0
-------------	---------------

JOB 5 :

Pour cet exemple la commande pour vérifier l'adresse IP de Pierre est : *ipconfig* :
192.168.1.1

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::204:9AFF:FE8E:C08A
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

Pour cet exemple la commande pour vérifier l'adresse IP d'Alicia est : *ipconfig* :
192.168.1.2

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

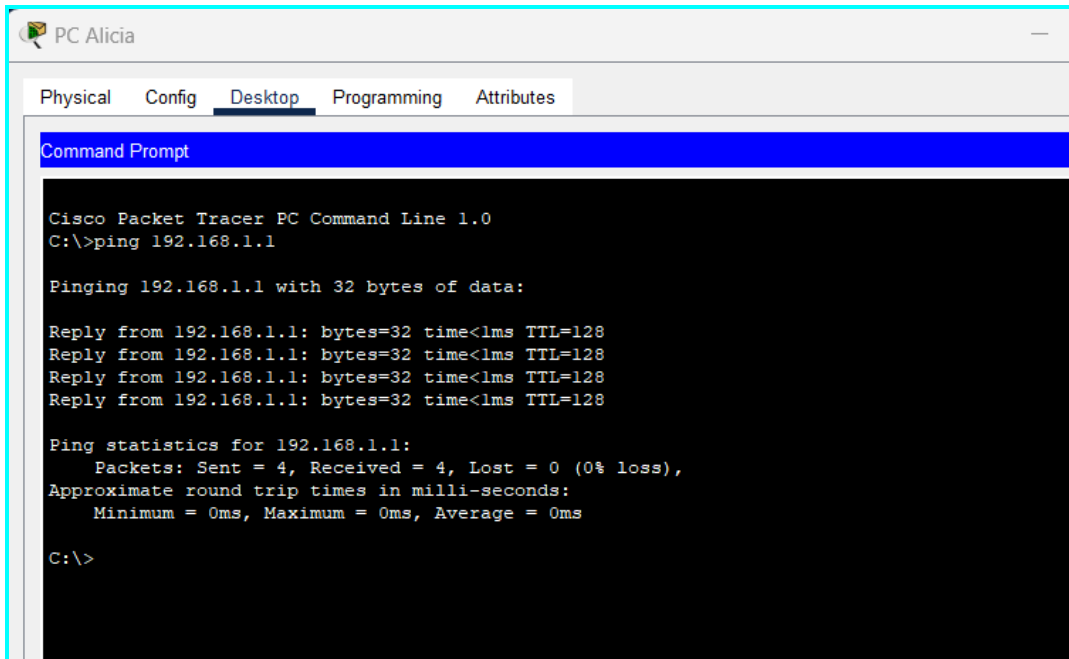
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::20A:F3FF:FE5A:E3B1
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0
```

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

ipconfig

JOB 6 :

Pour cet exemple (PC de Alicia) la commande sur le terminal est ping 192.168.1.1 (l'adresse IP de Pierre)



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

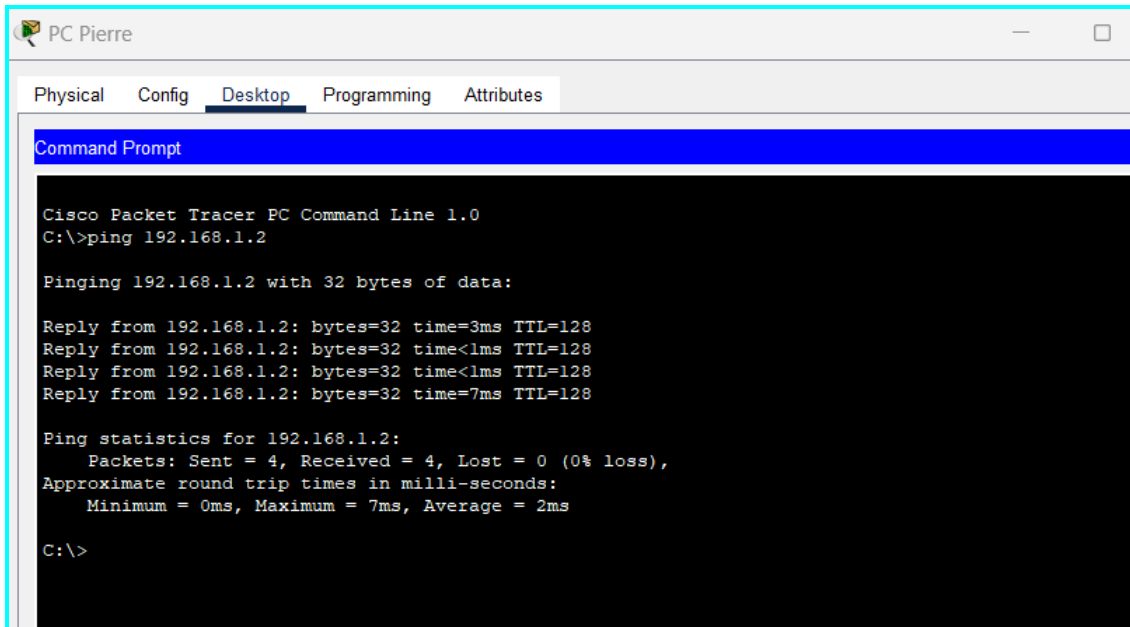
Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Pour cette exemple (PC de Pierre) la commande du terminal est ping 192.168.1.2 (l'adresse IP d'Alicia)



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=3ms 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=7ms 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 = 7ms, Average = 2ms

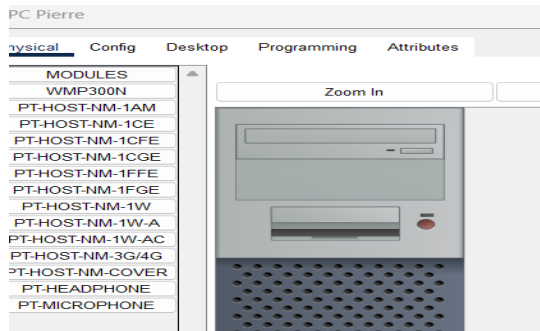
C:\>
```

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

PING (suivi de l'adresse ip de l'autre PC)

JOB 7 :

On va éteindre le pc de pierre “manuellement” (*bouton rouge*)



On va procéder à un ping du pc d'Alicia à celui de pierre

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

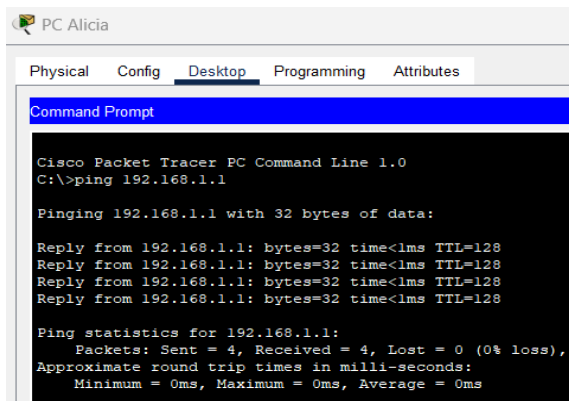
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

→ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ? Non, le ping envoie des paquets de données à une adresse ip, pour tester sa connectivité, donc si le pc est éteint il ne pas se connecté à un réseau et donc ne peut pas recevoir le Ping.

JOB 8 :

Nous avons effectué à partir du PC d'Alicia des ping aux autres pc , pour vérifier qu'ils sont bien connectés.



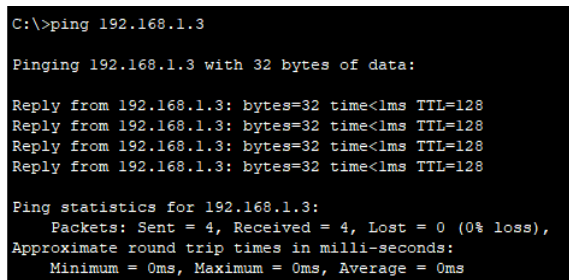
```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

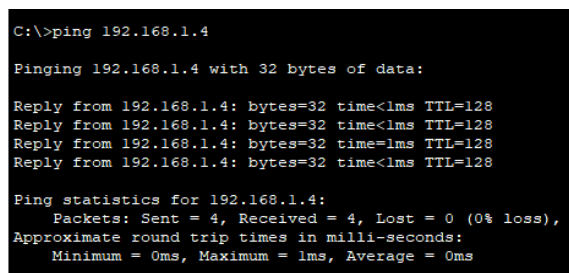


```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

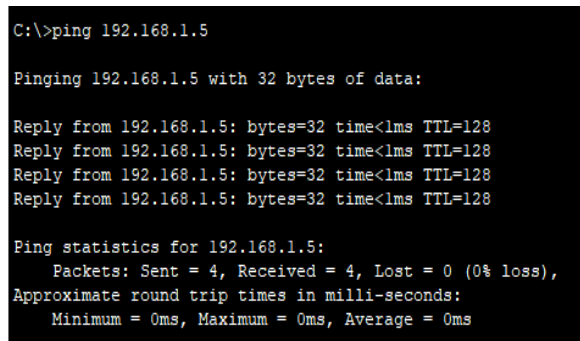


```
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128
Reply from 192.168.1.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```



```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

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

Les hubs répètent simplement les signaux à tous les ports, tandis que les switches analysent les adresses MAC et envoient le trafic uniquement là où il est nécessaire. De nos jours, les switches sont la norme pour la plupart des réseaux en raison de leur efficacité et de leur capacité à gérer de manière optimale le trafic.

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

Le Hub fonctionne principalement comme un répéteur : il prend un signal entrant et le répète à tous les autres ports.

Le principal avantage du hub est son prix.

Les inconvénients : Lorsqu'un hub reçoit des données sur un port, il les envoie à tous les autres ports, quelle que soit la destination. Cela signifie que tous les appareils connectés au hub voient le trafic réseau de tous les autres appareils. Les hubs sont rarement utilisés dans les réseaux modernes car ils génèrent beaucoup de trafic inutile et réduisent l'efficacité du réseau.

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

Un switch opère en examinant l'adresse MAC (Media Access Control) de chaque paquet de données et en les envoyant uniquement au port approprié.

Lorsqu'un switch reçoit des données, il examine l'adresse MAC du destinataire et envoie le paquet uniquement au port auquel l'appareil destinataire est connecté.

Cela permet d'optimiser le trafic et de réduire la congestion du réseau.

Les switches minimisent le trafic inutile et permettent une communication simultanée entre plusieurs paires d'appareils.

Les switches sont largement utilisés dans les réseaux modernes car ils améliorent considérablement la performance et la sécurité.

Son principal inconvénient (par rapport au Hub) c'est qu'il est plus onéreux.

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

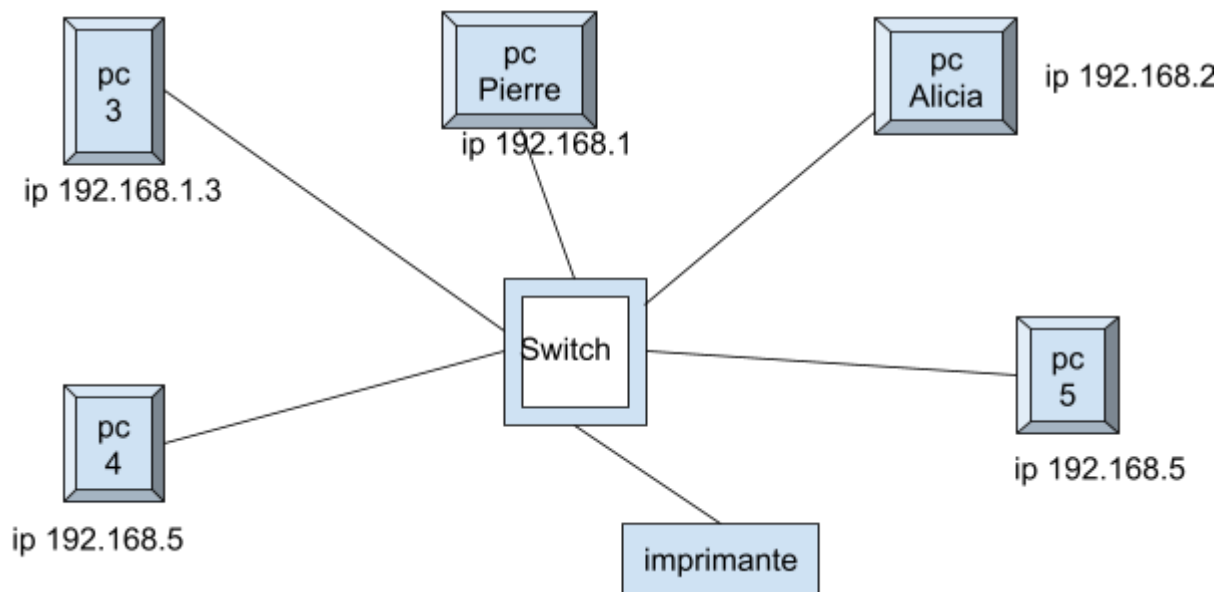
Un switch utilise une table d'adresses MAC pour diriger sélectivement les paquets de données vers les ports appropriés, ce qui permet un transfert de données plus efficace et réduit la congestion du réseau. Ce processus est dynamique et se répète chaque fois qu'un nouveau périphérique est connecté ou lorsqu'une adresse MAC change de port.

(NB: L'adresse MAC est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est sensée être unique au monde. On peut donc considérer qu'elle constitue une sorte de plaque d'immatriculation des appareils électroniques)

JOB 9 :

Configuration du Réseau:

1. Configuration des machines, on va ajouter une adresse IP aux 5 PC et à l'imprimante.
3. On va relier par des câbles droits les machines à la switch (analyse des adresses MAC)
2. On va tester la connectivité des machines entre elles , par la commande ping



Les avantages importants d'avoir un Schéma ?

1. Le schéma offre une clarté visuelle du réseau ce qui facilite sa compréhension
2. Le schéma permet une identification visuelle des différents éléments qui composent le réseau (PC, Switch...).
3. La visualisation du réseau par le schéma peut permettre une plus grande facilité en cas de problème, en facilitant la localisation du problème.
4. La conceptualisation d'un réseau peut être difficile à appréhender , une vue d'ensemble par un schéma, peut faciliter la compréhension du réseau dans son ensemble.

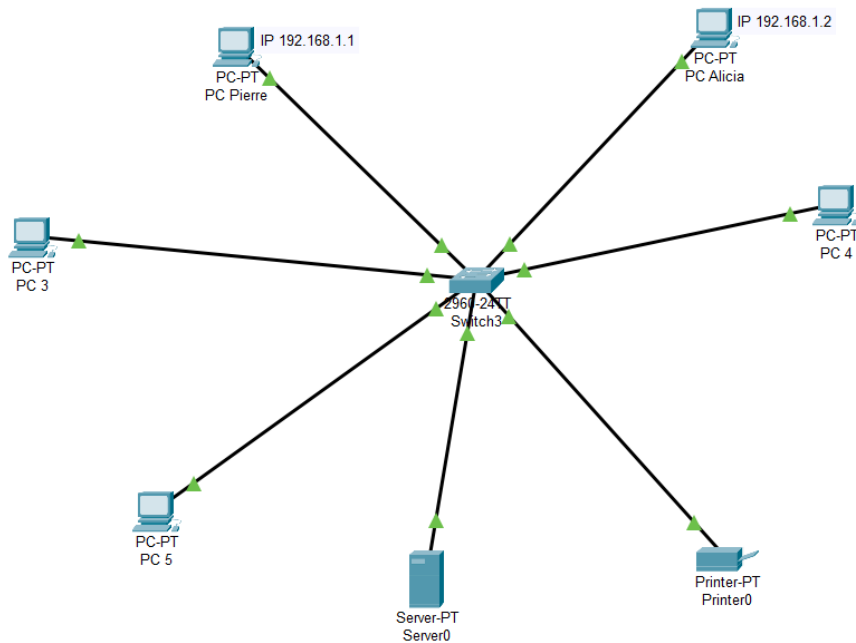
JOB 10 :

Mise en place d'un serveur DHCP, on va le paramétrer de sorte qu'il attribue une adresse ip aux PC (ceux en DHCP: PC3, PC4, PC5)

IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	169.254.172.115
Subnet Mask	255.255.0.0

IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	169.254.155.135
Subnet Mask	255.255.0.0

IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IPv4 Address	169.254.236.153



(ici on a gardé les PC de Pierre et alicia en statique et les PC3 PC4 PC5 seront DHCP)

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

Une adresse IP statique est configurée manuellement et reste la même, tandis qu'une adresse IP attribuée par DHCP est automatiquement attribuée par un serveur DHCP et peut changer dynamiquement au fil du temps.

JOB 11 :

	Getaway	Adresse IP	adresse diffusion	Sous-masque
12 hotes	10.0.0.0	10.0.0.1 à 10.0.0.14	10.0.0.15	255.255.255.240
30 hôtes	10.1.0.0	10.1.0.1 à 10.1.0.30	10.1.0.31	255.255.255.224
30 hôtes	10.2.0.0	10.2.0.1 à 10.2.0.30	10.2.0.31	255.255.255.224
30 hôtes	10.3.0.0	10.3.0.1 à 10.3.0.30	10.3.0.31	255.255.255.224
30 hôtes	10.4.0.0	10.4.0.1 à 10.4.0.30	10.4.0.31	255.255.255.224
30 hôtes	10.5.0.0	10.5.0.1 à 10.5.0.30	10.5.0.31	255.255.255.224
120 hôtes	10.6.0.0	10.6.0.1 à 10.6.0.126	10.6.0.127	255.255.255.128
120 hôtes	10.7.0.0	10.7.0.1 à 10.7.0.126	10.7.0.127	255.255.255.128
120 hôtes	10.8.0.0	10.8.0.1 à 10.8.0.126	10.8.0.127	255.255.255.128
120 hôtes	10.9.0.0	10.9.0.1 à 10.9.0.126	10.9.0.127	255.255.255.128
120 hôtes	10.10.0.0	10.10.0.1 à 10.10.0.126	10.10.0.127	255.255.255.128
160 hôtes	10.11.0.0	10.11.0.1 à 10.11.0.254	10.11.0.254	255.255.255.0
160 hôtes	10.12.0.0	10.12.0.1 à 10.12.0.254	10.12.0.255	255.255.255.0
160 hôtes	10.13.0.0	10.13.0.1 à 10.13.0.254	10.13.0.255	255.255.255.0
160 hôtes	10.14.0.0	10.13.0.1 à 10.12.0.254	10.14.0.255	255.255.255.0
160 hôtes	10.15.0.0	10.15.0.1 à 10.12.0.254	10.14.0.255	255.255.255.0

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

Le système de classe des adresses IP a pour fonction de gérer l'allocation des adresses IP sur Internet

Une adresse de classe A utilise le premier octet pour identifier le réseau, tandis que les trois octets restants sont pour les hôtes. Cela signifie qu'il y a potentiellement beaucoup d'adresses disponibles pour les hôtes dans un réseau de classe A.

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

Classe: A : Les adresses de classe A sont utilisées pour les réseaux très vastes. Le premier octet identifie le réseau, tandis que les trois octets restants sont pour les hôtes.

Classe: B : 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 sont pour les hôtes.

Classe: C : Les adresses de classe C sont utilisées pour les réseaux de petite taille. Les trois premiers octets identifient le réseau, tandis que le dernier est pour les hôtes.

(Classe: D : Les adresses de classe D sont réservées pour le multicast.)

Job 12 :

	Les 7 couches OSI	Description/Matériels/Protocoles associés
Couche 7	APPLICATION	Services applicatifs, au plus proche des utilisateurs. Fournit des interfaces pour les applications (navigateur, FTP , HTML ...)
couche 6	PRÉSENTATION	Encode, chiffre et compresse les données utiles. Gère la syntaxe et sémantique des données (compression, chiffrement des données SSL/TLS ...)
couche 5	SESSION	Établit des sessions entre des applications (protocoles de session, authentification...)
couche 4	TRANSPORT	Établit, maintient et termine des sessions entre des périphériques terminaux. Assure le transfert de bout en bout, gère de contrôle de flux et la fiabilité (TCP , UDP , PPTP ...)
couche 3	RÉSEAU	Adresse les interface globalement, et détermine les meilleurs chemins à travers un inter-réseau . Gère le routage des paquets à travers le réseau (IPv4 , IPv6 , Routeur ...)
couche 2	LIAISON DE DONNÉES	Adresse localement les interfaces, livre les informations localement méthode MAC Gère la communication entre les systèmes et la détection d'erreur (Ethernet , Wifi , Mac ..)
couche 1	PHYSIQUE	Encodage du signal, câblage et connecteurs, spécifications matérielles (câble, carte réseau , fibre optique , Cable RJ45 ...)

JOB 13:

→ Quelle est l'architecture de ce réseau ?

Ce réseau est composé de 4 PC liés à une Switch, qui elle même est reliée à 2 serveurs.

Le masque de sous réseau 255.255.255.0 indique qu'il s'agit d'un réseau de classe C.

Il s'agit ici d'un réseau LAN, ou tous les appareils appartiennent à un réseau local.

→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau est 192.168.10.0

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

On peut connecter 254 machines sur ce réseau.

Pour trouver ce chiffre: ici le masque de sous réseau est 255.255.255.0 , on a donc 24 bits consacrés à l'identification et 8 bits pour les adresses machines.

On va appliquer la Formule $2^n - 2$, donc ici $2^8 - 2 = 254$.

→ Quelle est l'adresse de diffusion de ce réseau ?

Ici l'adresse de diffusion de ce réseau est : 192.168.10.255

JOB 14

Convertissez les adresses IP suivantes en binaires :

- 145.32.59.24: 10010001.00100000.00111011.00011000
- 200.42.129.16: 11001000.00101010.10000001.00010000
- 14.82.19.54: 000001110.01010010.00010011.00110110

JOB 15 :

→ Qu'est-ce que le routage ?

Le routage informatique est un processus de sélection des chemins qui vont permettre de transmettre des paquets de données depuis un expéditeur jusqu'à un ou plusieurs destinataires. Les routeurs sont les principaux dispositifs qui effectuent le routage. Ils utilisent des tables de routage pour déterminer le chemin le plus efficace pour acheminer les paquets de données.

→ Qu'est-ce qu'un gateway ?

En informatique réseau, un gateway (en anglais) est un dispositif ou un logiciel qui agit comme un point d'entrée ou de sortie entre deux réseaux distincts, permettant ainsi la communication entre eux. Le Gateway est ainsi utilisé pour permettre la communication entre des réseaux qui utilisent des protocoles ou des architectures différentes.

Un routeur qui relie le réseau local à Internet, en permettant aux appareils du réseau local d'accéder à Internet, peut jouer le rôle d'un Gateway, dans certaines configurations.

→ Qu'est-ce qu'un VPN ?

VPN est l'abréviation de Virtual Private Network (réseau privé virtuel en français). Il s'agit d'un outil de cybersécurité qui permet de préserver la confidentialité en ligne en chiffrant la connexion entre l'appareil et Internet. Cette connexion sécurisée fournit un tunnel privé pour les données et communications lorsque sont utilisées sur des réseaux publics.

Il garantit ainsi la confidentialité et l'anonymat lorsque l'on effectue des achats ou des opérations bancaires en ligne.

→ Qu'est-ce qu'un DNS ?

Le DNS (Domain Name System) permet de faciliter la recherche sur internet, concrètement c'est un système de nom de domaine; il est le service assurant le lien entre le nom de domaine et l'adresse IP d'un serveur. Il permet à l'internaute de ne pas avoir à connaître l'adresse IP exacte d'un site web pour pouvoir y accéder.

