

Le Réseau

JOB 02:

Un réseau informatique est un ensemble de dispositifs électroniques interconnectés qui communiquent entre eux pour partager des ressources, des données et des services. Ces dispositifs peuvent inclure des ordinateurs, des serveurs, des routeurs, des imprimantes, etc..

Ce réseau informatique peut servir à plusieurs choses. Comme nous l'avons dit précédemment il peut servir à partager des ressources entre différents périphériques, mais pas que. Il nous permet aussi de communiquer, d'avoir accès à internet ou encore de mettre en place des mesures de sécurité pour protéger les données et les ressources contre les accès non autorisés.

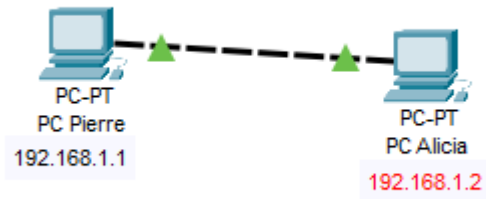
Si nous voulons à notre tour créer un réseau informatique, nous aurons besoin de plusieurs pièces et d'un matériel bien précis:

- un ordinateur
- des périphériques réseaux, tels qu'un **commutateur** (switches), un **routeur** et un **point d'accès sans fil**. Un **commutateur** permet de connecter plusieurs appareils au réseau en utilisant un câble Ethernet. Il dirige le trafic des données vers la destination appropriée. Un **routeur** est essentiel pour diriger le trafic entre le réseau local (LAN) et d'autres réseaux comme Internet. Il peut également inclure des fonctionnalités de sécurité, telles qu'un pare-feu. Enfin un **point d'accès sans fil** est nécessaire si l'on souhaite un réseau sans fil et laisser les dispositifs compatibles WI-FI se connecter.
- un **serveur** (si nous envisageons un réseau plus complexe, un serveur peut être nécessaire pour stocker des données, des applications ou des services centralisés.
- de **câblages**, plus spécifiquement de **câbles ethernet** pour connecter les appareils au réseau (par exemple Cat 5e, Cat 6 ou Cat 6a). Le câblage devra être plus structuré dans certaines situations, par exemple si nous créons un réseau plus vaste ou professionnel, il comprendra des armoires de brassage, des panneaux de brassage, des câbles, des prises murales.
- de **logiciels**, de **gestion réseau** ou **système d'exploitation** (obligatoire sur les ordinateurs/serveurs). Les logiciels de gestion réseau sont des logiciels de configuration, de surveillance et de gestion de réseau peuvent être utiles pour administrer le réseau.
- un **matériel de sécurité** tels qu'un **pare-feu** (qui surveille le trafic entrant et sortant et décide d'autoriser ou de bloquer une partie de ce trafic en fonction des règles de sécurité prédéfinies), un **antivirus** (qui a pour but principal de protéger notre système informatique des intrusions, virus et logiciels malveillants)
- d'outils et d'équipements tels que des tournevis, des pinces à sertir, des testeurs de câbles, des câbles patch pour l'installation et la maintenance du réseau.
- enfin d'une bonne source d'alimentation électrique qui nous permettra de fournir une alimentation électrique adéquate à tous nos dispositifs.

JOB 03:

Le câble que j'ai utilisé pour connecter le PC de Pierre avec celui d'Alicia est un câble ethernet.

JOB 04:



Une adresse IP (Internet Protocol Address) constitue la base du réseau internet. Il s'agit d'une étiquette numérique qui permet d'identifier un équipement tel qu'un ordinateur par exemple, en clair: tout ce qui est connecté sur le réseau est muni d'une adresse IP.

L'adresse IP sert principalement à identifier et localiser les appareils sur un réseau et à router les données entre eux. L'adresse IP peut acheminer les paquets de données d'un appareil source vers un appareil de destination sur un réseau (internet ou réseau local).

Une adresse MAC (Media Access Control) est une adresse physique unique permettant d'identifier un équipement réseau par rapport à un autre. Elles ne se changent généralement pas car elles sont fixées en usine par le constructeur.

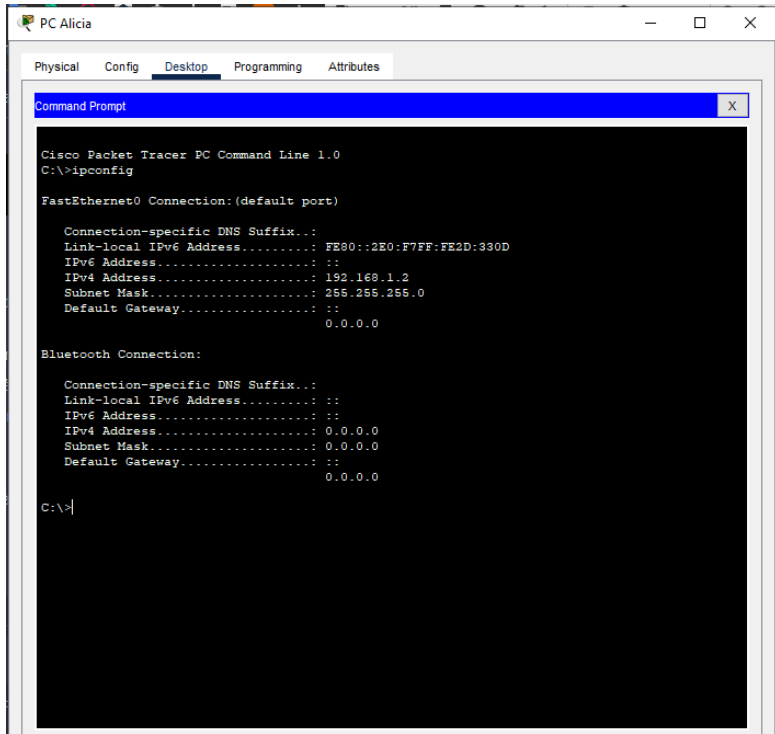
Une adresse IP publique est une adresse qui est utilisée pour identifier un appareil ou un réseau sur internet. Elle est accessible depuis internet et est généralement fournie par un fournisseur d'accès à internet.

Une adresse IP privée est utilisée pour identifier un appareil ou un réseau au sein d'un réseau local, comme un réseau domestique ou d'entreprise. Celles-ci ne sont pas directement accessibles depuis internet et sont généralement utilisées pour l'adressage interne.

JOB 05:

La commande que j'ai utilisé pour vérifier l'id des machines est la ligne de commande suivante:

ipconfig



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

FastEthernet0 Connection: (default port)

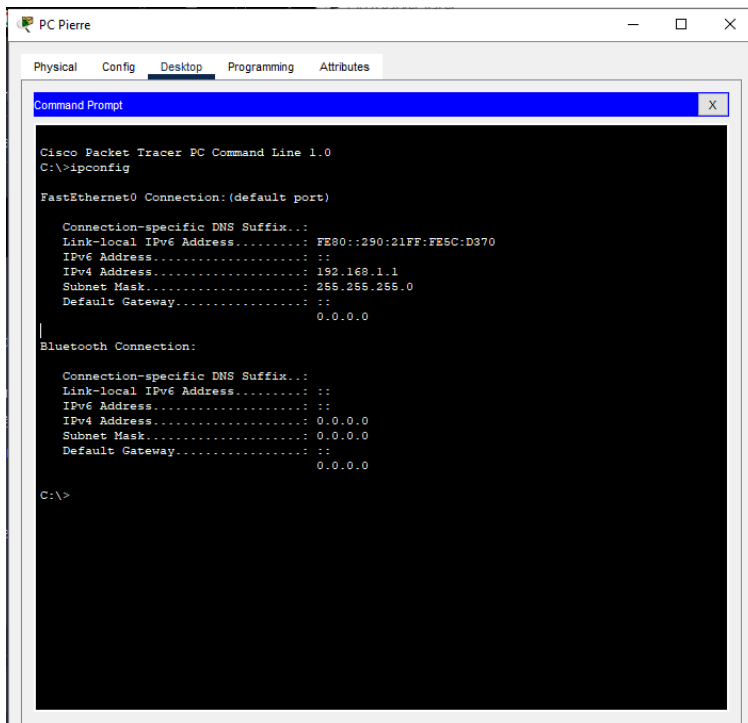
    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2E0:F7FF:FE2D:330D
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>
```

PC Pierre



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::290:21FF:FESC:D370
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .:
    IPv6 Address . . . . .:
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>
```

PC Alicia

JOB 06:

La commande permettant de Ping* entre des PC est:

ping <adresse IP>

```
8.1.1
8.1.1 with 32 bytes of data:
168.1.1: bytes=32 time<1ms TTL=128
168.1.1: bytes=32 time=4ms TTL=128
168.1.1: bytes=32 time=4ms TTL=128
168.1.1: bytes=32 time=3ms TTL=128

    for 192.168.1.1:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Round trip times in milli-seconds:
    0.00ms, Maximum = 4ms, Average = 2ms

8.1.2
8.1.2 with 32 bytes of data:
168.1.2: bytes=32 time<1ms TTL=128
168.1.2: bytes=32 time=4ms TTL=128
168.1.2: bytes=32 time<1ms TTL=128
168.1.2: bytes=32 time=1ms TTL=128

    for 192.168.1.2:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Round trip times in milli-seconds:
    0.00ms, Maximum = 4ms, Average = 1ms
```

Ping PC Pierre

```
8.1.2
8.1.2 with 32 bytes of data:
168.1.2: bytes=32 time=10ms TTL=128
168.1.2: bytes=32 time=6ms TTL=128
168.1.2: bytes=32 time=5ms TTL=128
168.1.2: bytes=32 time=5ms TTL=128

    for 192.168.1.2:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Round trip times in milli-seconds:
    0.00ms, Maximum = 10ms, Average = 6ms

8.1.1
8.1.1 with 32 bytes of data:
168.1.1: bytes=32 time<1ms TTL=128
168.1.1: bytes=32 time<1ms TTL=128
168.1.1: bytes=32 time=18ms TTL=128
168.1.1: bytes=32 time=1ms TTL=128

    for 192.168.1.1:
    Sent = 4, Received = 4, Lost = 0 (0% loss),
    Round trip times in milli-seconds:
    0.00ms, Maximum = 18ms, Average = 4ms
```

Ping PC Alicia

* Pour rappel, le Ping (Packet Internet Groper) permet de vérifier si un ordinateur est actif et connecté à un réseau, un peu comme un jeu de coucou électronique entre ordinateurs.

JOB 07:

Le PC de Pierre n'a pas reçu les paquets envoyés par Alicia car dans un premier temps celui-ci est éteint, ce qui le rend inactif sur le réseau donc il ne peut pas répondre aux demandes de ping.

```
>ping 192.168.1.1  
  
ping 192.168.1.1 with 32 bytes of data:  
  
request timed out.  
request timed out.  
request timed out.  
request timed out.  
  
ping statistics for 192.168.1.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

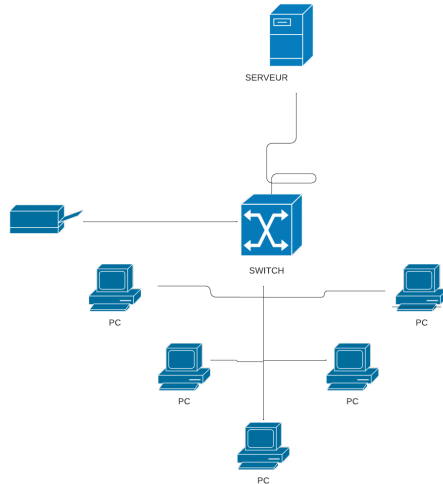
JOB 08:

Bien que qu'un hub et un switch soit deux dispositifs permettant de connecter plusieurs ordinateurs dans un réseau local, il existe cependant des différences entre les deux outils.

Un hub est une machine reliée à plusieurs machines en réseau qui permet de concentrer les données pour les transmettre par un unique canal. Il rediffuse les données reçues sur un port à tous les autres ports en même temps. Ses avantages sont qu'ils sont simples, faciles à utiliser, et peu coûteux. Ses inconvénients sont que si tous les appareils partagent la même bande passante cela entraînera une mauvaise performance, et son absence de sécurité.

Un switch est un boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier en réseau différents éléments du système informatique. Il apprend l'adresse MAC des appareils connectés à ses ports et achemine le trafic uniquement vers le port approprié en fonction de l'adresse MAC de destination. Ses avantages sont qu'il est plus intelligent qu'un hub et offre une meilleure performance en segmentant le trafic et en envoyant le trafic uniquement aux ports nécessaires, ils améliorent la sécurité en isolant le trafic entre les appareils. Ses inconvénients sont qu'un switch est plus coûteux que les hubs, leur configuration peut être plus complexe, les composants mécaniques peuvent s'user.

JOB 09:



Sur le schéma ci-dessus nous pouvons voir que les 5 ordinateurs et l'imprimante sont tous connectés à un **switch** qui est lui-même relié à un serveur.

Les trois avantages importants d'avoir un schéma sont qu'un schéma nous permet une meilleure clarté et visibilité du réseau. Le second avantage est que le schéma permet un dépannage plus rapide car nous saurons où se trouve le problème et nous pourrons le résoudre directement. Enfin le dernier avantage est qu'un schéma est pratique pour une planification à long terme.

JOB 10:

Un serveur DHCP (Dynamic Host Configuration Protocol) est un serveur qui délivre des adresses IP aux équipements qui se connectent au réseau.

La différence entre une adresse IP statique et une adresse IP attribuée par DHCP est que l'une est fixe et configurée manuellement (adresse IP statique) tant que l'autre est dynamique et gérée par un serveur DHCP (adresse IP par DHCP). Le choix des deux dépend des besoins spécifiques du réseau et du type d'appareils à connecter. Les adresses IP statiques sont utilisées pour les dispositifs nécessitant une adresse IP constante, tandis que le DHCP est largement utilisé pour simplifier la gestion des adresses IP pour un grand nombre d'appareils sur un réseau.

JOB 11:

Pourquoi avons-nous choisi une adresse 10.0.0.0 de classe A ?

Tout d'abord qu'est-ce qu'une adresse de classe A ? Une adresse de classe A correspond avant tout à l'adresse IP 10.0.0.0, qui a une grande plage d'adresse disponible pour les hôtes. Les adresses de classe A ont un octet de réseau suivi de trois octets pour les hôtes, ce qui permet d'avoir un grand nombre d'adresses individuelles dans le sous-réseau (16.777.214). Les adresses de classe A sont courantes pour les réseaux privés d'entreprises car elles offrent une grande flexibilité pour créer de nombreux sous-réseaux et permet une gestion efficace des adresses IP. Les adresses de classe A sont souvent utilisées dans des réseaux internes plus importants, tandis que les réseaux plus petits peuvent opter pour des adresses de classe B ou C.

Il existe cinq catégories principales de réseaux: A,B,C,D et E. Chacune de ces classes a un format spécifique qui détermine la taille du réseau et le nombre d'hôtes qu'elle peut prendre en charge.

Les classes A,B et C sont utilisées pour les réseaux de taille variable, tandis que les classes D et E sont réservées à des utilisations spéciales (multicast pour la classe D et expérimentale pour la classe E).

La classe A a un octet de réseau suivi de trois octets pour les hôtes, la classe B a deux octets de réseau et deux octets pour les hôtes, et la classe C a trois octets de réseau et un octet pour les hôtes. La taille du réseau diminue à mesure que vous avancez de la classe A à la classe C.

JOB 12:

<u>Couche OSI</u>	<u>Description et rôle</u>	<u>Matériels/Protocoles Associés</u>
Couche 1 (Physique)	Traite les signaux électriques, optiques, ou radiofréquences pour la transmission des données. S'occupe des câblages, des connecteurs et des médias de transmission.	Fibre optique, câble RJ45
Couche 2 (Liaisons de données)	Gère la communication entre les appareils connectés directement. Elle effectue la détection d'erreurs, la segmentation des données en trames, et la gestion des adresses MAC.	Ethernet, MAC, WI-FI, câble RJ45
Couche 3 (Réseau)	Dirige les paquets de données à travers un réseau. Elle gère la commutation, le routage et l'adressage IP.	IPv4, IPv6, routeur.
Couche 4 (Transport)	Assure la communication de bout en bout entre les applications. Elle est responsable du contrôle d'erreur, de la séparation des données en segments et de la gestion de flux.	TCP, UDP
Couche 5 (Session)	Gère l'établissement, la maintenance et la fin de sessions de communication. Elle synchronise les échanges de données entre les applications.	PPTP (gestion de sessions)
Couche 6 (Présentation)	Gère la syntaxe et la sémantique des données échangées entre les applications. Elle effectue la traduction, la compression et le chiffrement des données.	SSL/TLS (chiffrement), HTML (mise en forme)
Couche 7 (Application)	Responsable des services d'application pour les utilisateurs finaux. Elle	HTTP, FTP, PPTP, SSL/TLS, HTML

	permet aux applications de communiquer sur différents réseaux.	

JOB 13:

Ce réseau est une topologie de réseau simple où 4 PC sont connectés à un réseau local, il peut s'agir d'un réseau local d'une petite école, d'un bureau ou d'une installation similaire. Son adresse IP est 192.168.1.10. Nous pouvons y brancher 254 machines sur ce réseau. L'adresse de diffusion de ce réseau est utilisée pour envoyer des données à toutes les machines du réseau en même temps. Dans ce cas l'adresse de diffusion est 192.168.10.255.

JOB 14:

Conversion d'adresses IP en binaires:

145.32.59.24 : 10010001.00100000.00111011.00011000

200.42.129.16 : 11001000.00101010.10000001.00010000

14.82.19.54 : 00001110.01010010.00010011.00110110

JOB 15:

Un routage est un processus de transmission de données d'un réseau à un autre. Il consiste à prendre une décision sur la manière dont les données doivent être acheminées à partir de la source vers la destination. Les routeurs sont les appareils qui effectuent le routage en fonction des adresses IP des paquets de données. Le routage permet la communication entre des réseaux distincts, tels que internet en trouvant le meilleur chemin pour les données à travers un réseau complexe de dispositifs interconnectés.

Un gateway (passerelle) est un dispositif ou un logiciel qui agit comme une interface entre deux réseaux distincts. Les passerelles permettent la communication entre des réseaux qui utilisent des protocoles de communication différents. Elle peut relier un réseau local (LAN) à internet en traduisant les adresses IP privées du LAN en adresses IP publiques routables sur Internet.

Un VPN (Virtual Private Network) est un réseau privé virtuel qui permet de sécuriser et de crypter la communication sur un réseau public (comme internet). Il crée un tunnel de communication sécurisé entre un périphérique ou un réseau et un serveur VPN distant. Ils sont souvent utilisés pour garantir la confidentialité et la sécurité des données lors de la transmission sur des réseaux non sécurisés, pour accéder à des ressources réseau internes à distance.

Un DNS (Domain Name System) est un système de noms de domaine qui permet de traduire des noms de domaine conviviaux pour les humains en adresses IP compréhensibles pour les ordinateurs. Plutôt que de mémoriser des adresses IP numériques, les utilisateurs peuvent utiliser des noms de domaine pour accéder à des sites / ressources sur internet. Il joue un rôle important en associant les noms de domaine aux adresses IP correspondantes facilitant ainsi la résolution des noms.