

2023

Runtrack Le réseau



Jordan Reinaldo
Bachelor
20/10/2023

Job 01

Cisco Packet Tracer a été installé.

Job 02

Qu'est-ce qu'un réseau et à quoi sert un réseau informatique ?

Un réseau est un système d'appareils interconnectés permettant la communication et le partage d'informations, qu'il s'agisse de petits réseaux locaux ou de vastes réseaux mondiaux comme internet.

Ils permettent par exemple de partager des données, l'accès à internet, la diffusion de médias, la transmission de courriels, la gestion de bases de données, la collaboration en ligne etc.

Les réseaux informatiques sont essentiels pour connecter des appareils et permettre la transmission d'informations à l'échelle locale, nationale et internationale.

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

Ordinateurs et appareils clients : Ce sont les dispositifs qui se connectent au réseau pour accéder aux ressources et communiquer. Ils peuvent être des ordinateurs personnels, des smartphones, des tablettes, des imprimantes, etc.

Serveurs : Les serveurs sont des ordinateurs dédiés qui stockent des données, des applications ou des services accessibles aux clients du réseau. Ils peuvent inclure des serveurs de fichiers, des serveurs web, des serveurs de messagerie, etc.

Routeurs : Les routeurs dirigent le trafic réseau entre différents réseaux, y compris entre le réseau local (LAN) et Internet. Ils utilisent des tables de routage pour déterminer la meilleure façon de transférer les données.

Commutateurs (Switches) : Les commutateurs relient plusieurs dispositifs au sein d'un réseau local (LAN). Ils apprennent les adresses MAC des appareils connectés et dirigent le trafic uniquement vers les destinataires appropriés, améliorant ainsi l'efficacité du réseau.

Câbles et connexions : Les câbles Ethernet, les câbles de fibre optique et les connexions sans fil (Wi-Fi) assurent la liaison physique entre les appareils. Les câbles Ethernet sont couramment utilisés pour les connexions filaires.

Firewalls : Les pare-feu sont des dispositifs matériels ou logiciels qui sécurisent le réseau en filtrant le trafic entrant et sortant, empêchant ainsi les menaces potentielles.

Points d'accès sans fil : Les points d'accès sans fil permettent la connectivité Wi-Fi, permettant aux appareils de se connecter sans fil au réseau. Ils sont souvent utilisés dans les réseaux locaux pour fournir une connectivité sans fil.

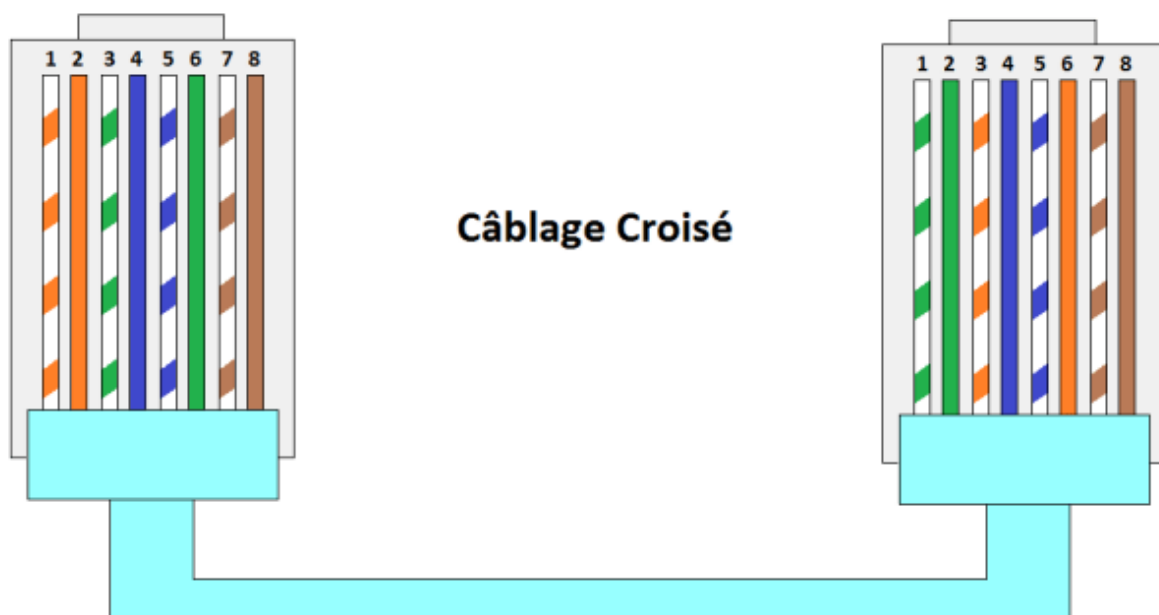
Modems : Les modems convertissent les signaux numériques des ordinateurs en signaux analogiques pour l'accès à Internet via des lignes téléphoniques, câble, fibre optique ou autres technologies.

Job 03

**Quels câbles avez-vous choisis pour relier les deux ordinateurs ?
Expliquez votre choix.**

J'ai choisi le câble croisé ou Copper cross over sur Cisco.

Le câblage interne des câbles croisés Ethernet inverse les signaux de transmission et de réception. Il est le plus souvent utilisé pour connecter deux périphériques du même type : comme deux ordinateurs (via le contrôleur d'interface réseau) ou deux commutateurs l'un à l'autre. Du fait, qu'ici nous avons deux appareils du même type, j'ai donc choisi un câble croisé.





Job 04

Qu'est-ce qu'une adresse IP et à quoi sert un IP?

Une adresse IP (Internet Protocol address) est une série de numéros qui identifie de manière unique un périphérique sur un réseau informatique utilisant le protocole Internet (IP). Les adresses IP sont essentielles pour permettre la communication entre les différents appareils connectés à Internet ou à un réseau local.

Elle sert à identifier et à acheminer les données entre les appareils. C'est essentiel pour la communication et le fonctionnement des réseaux informatiques.

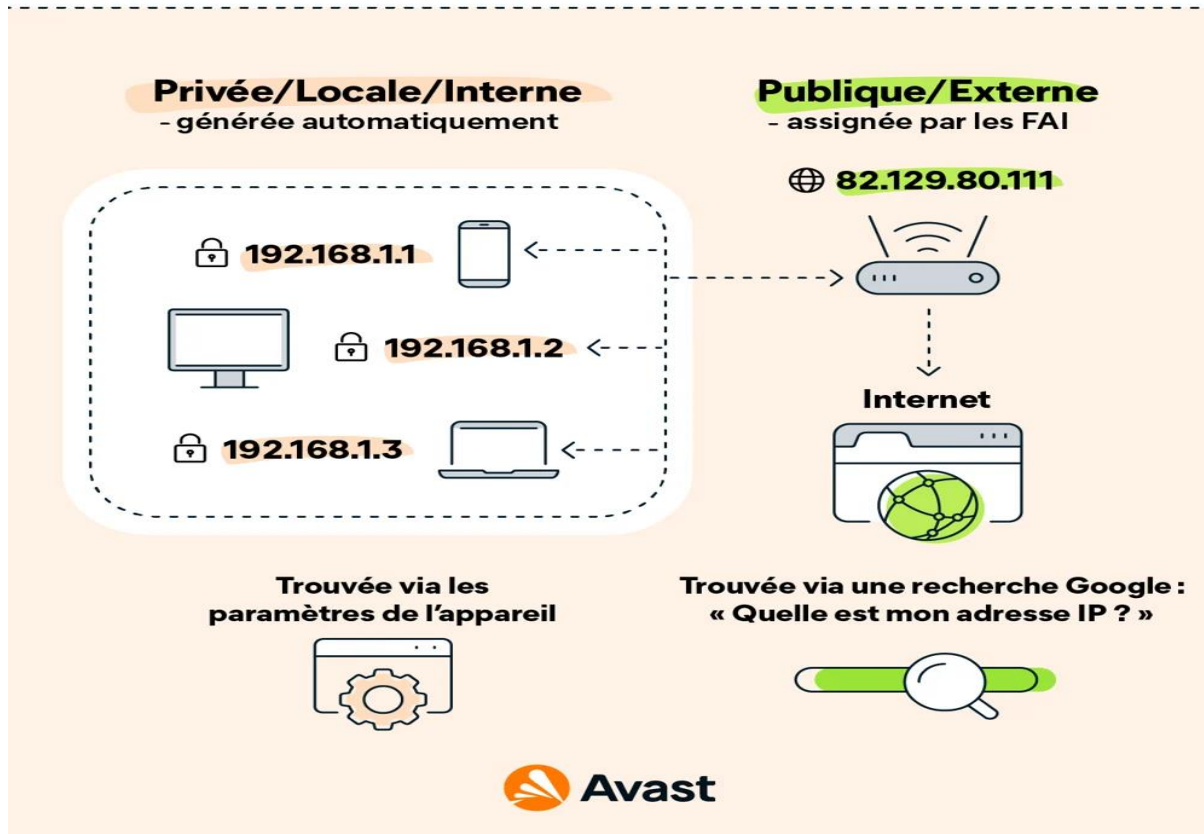
Qu'est-ce qu'une adresse MAC ?

Une adresse MAC, parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. Elle est unique au monde. Toutes les cartes réseau ont une adresse MAC, même celles contenues dans les PC et autres appareils connectés. Dans l'adresse Mac, nous avons une partie pour le constructeur et une partie pour la carte réseau.

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

La principale différence entre les adresses IP publiques et privées se situe au niveau de leur portée et du réseau auquel elles sont connectées. Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

Adresses IP publiques vs privées



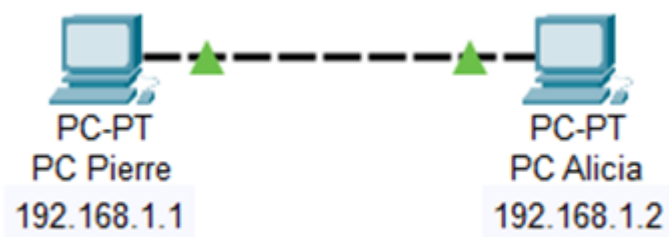
Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau correspond au masque de sous réseau :

Subnet Mask

255.255.255.0

Le réseau actuel est représenté ci-dessous :

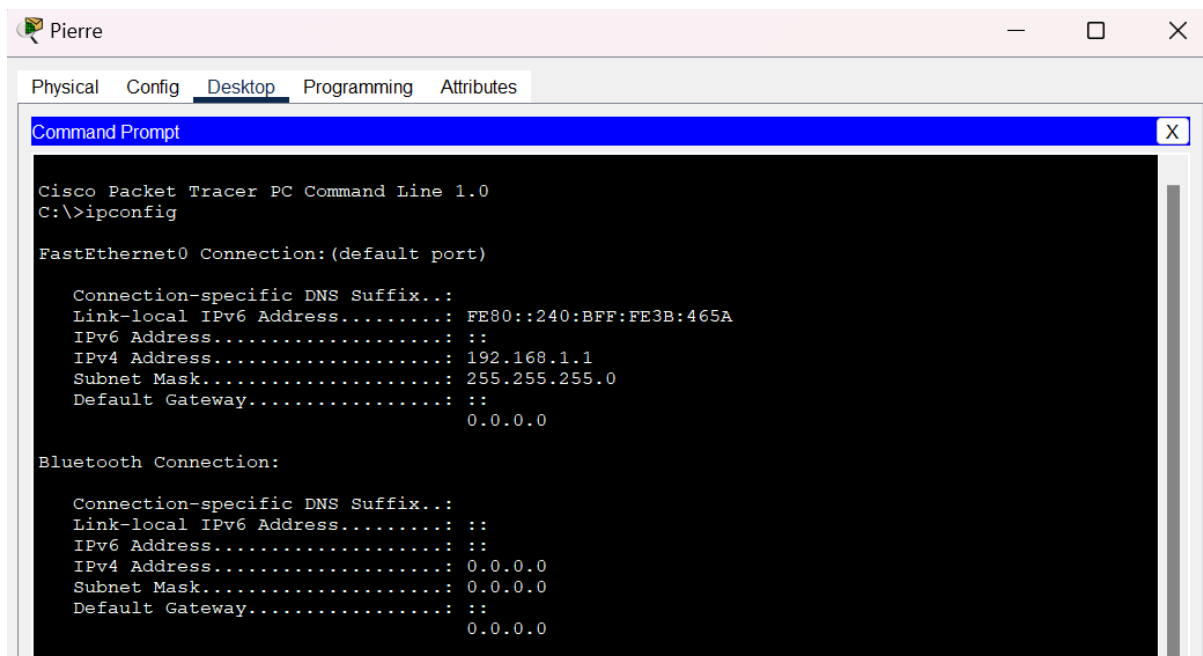


Job 05

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

ipconfig

Terminal de Pierre



The screenshot shows a terminal window titled 'Pierre' with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig' command in Cisco Packet Tracer. It displays details for the FastEthernet0 and Bluetooth connections, including DNS suffix, IPv6 and IPv4 addresses, subnet masks, and default gateways.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

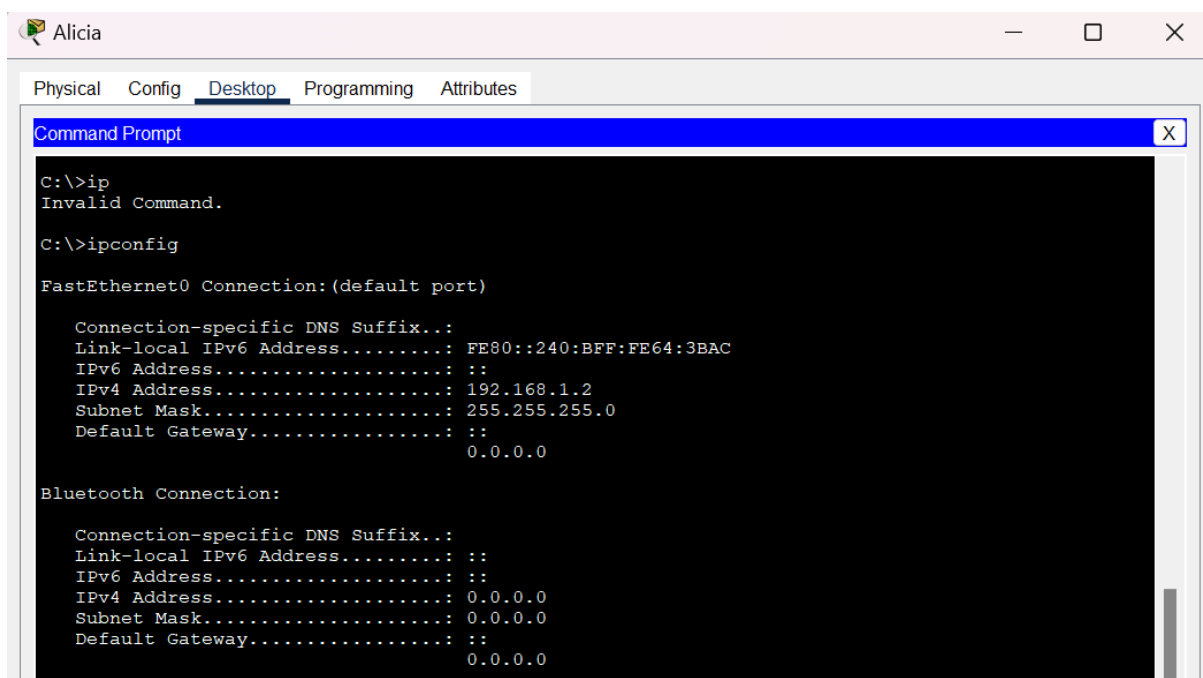
FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::240:BFF:FE3B:465A
    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
```

Terminal de Alicia



The screenshot shows a terminal window titled 'Alicia' with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a 'Command Prompt' window. The command prompt shows the output of the 'ipconfig' command in Cisco Packet Tracer. It displays details for the FastEthernet0 and Bluetooth connections, including DNS suffix, IPv6 and IPv4 addresses, subnet masks, and default gateways. The IPv4 address for FastEthernet0 is 192.168.1.2.

```
C:\>ip
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix.:
    Link-local IPv6 Address.....: FE80::240:BFF:FE64:3BAC
    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
```

Job 06

Quelle est la commande permettant de Ping entre des PC ?

ping "adresse ip de l'ordinateur que l'on veut ping"

Ping depuis le pc de Pierre

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

Ping depuis le pc de Alicia

```
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
```

Job 07

Ping depuis le pc de Alicia vers Pierre alors que le pc de dernier est éteint.

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
```

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

Non le le pc de Pierre n'a évidemment pas reçu les paquets envoyés par Alicia car il est hors tension. Dans cet état, il ne peut ni recevoir ni répondre aux paquets de données envoyés par Alicia.



Job 08

Quelle est la différence entre un hub et un switch ?

Un hub est un appareil réseau qui diffuse les données à toutes les connexions sans distinction, tandis qu'un switch intelligent dirige les données spécifiquement vers la connexion cible, cela permet d'améliorer la sécurité du réseau et d'éviter qu'il soit embouteillé !

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

Un hub fonctionne en transmettant toutes les données reçues à toutes les connexions. Il agit comme un simple répéteur de signal, sans prise de décision intelligente. Il a pour avantage d'être facile à configurer et moins coûteux cependant il a pour défaut d'être inefficace, il provoque du trafic inutile et est peu sécurisé.

Quels sont les avantages et inconvénients d'un switch ?

Le switch gère efficacement le trafic, améliore les performances, offre une sécurité accrue, minimise les collisions, cependant il est plus coûteux et plus complexe à configurer.

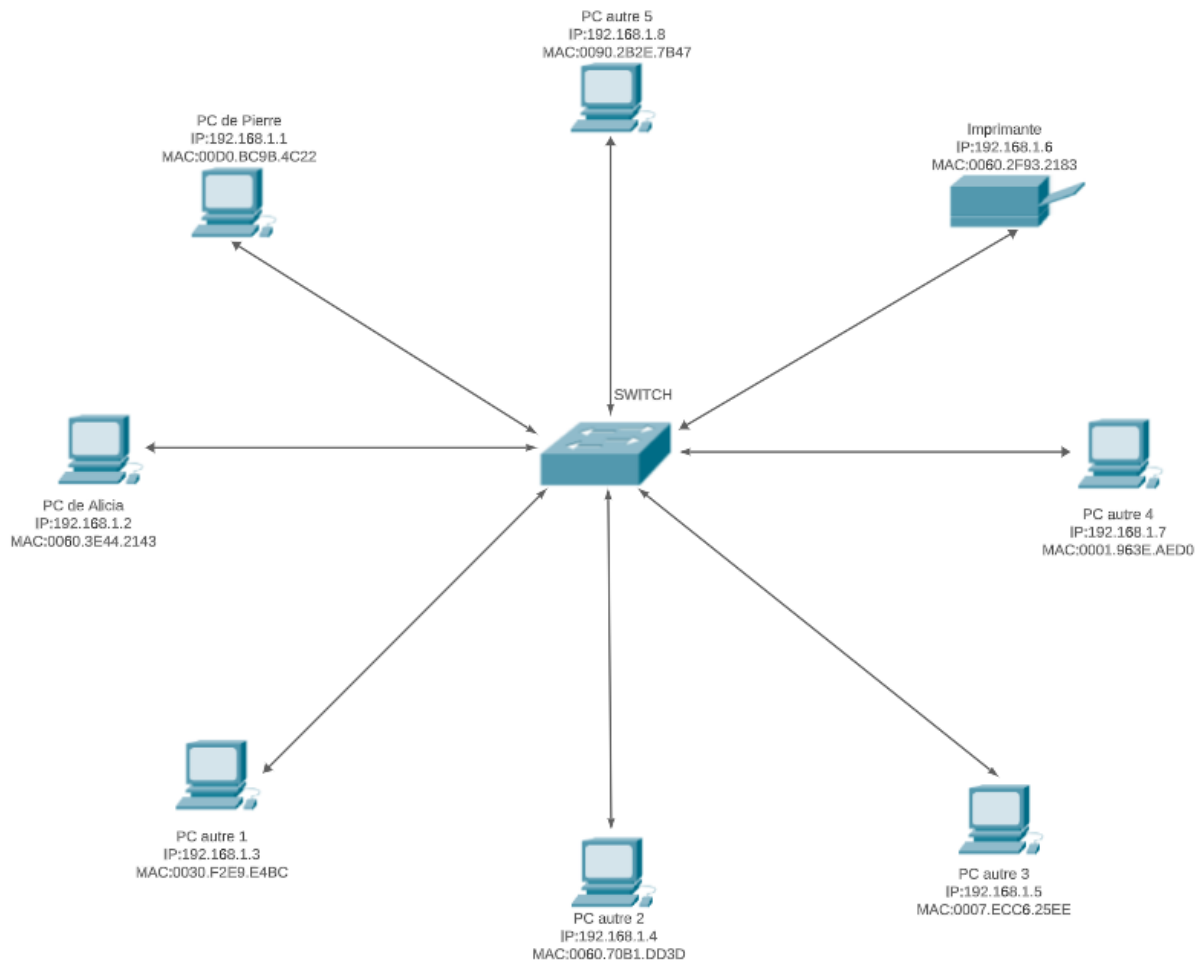
Comment un switch gère-t-il le trafic réseau ?

Un switch utilise des tables de correspondance MAC pour diriger les données uniquement vers le port où se trouve la destination, évitant ainsi la diffusion inutile et améliorant les performances et la sécurité du réseau.

Job 09

J'ai ajouté l'imprimante, je lui ai donné une IP et je l'ai ping avec le pc de pierre, tout fonctionnait.

Voici le schéma avec la topologie étoile que j'ai réalisé concernant le réseau que nous avons fait jusqu'ici:

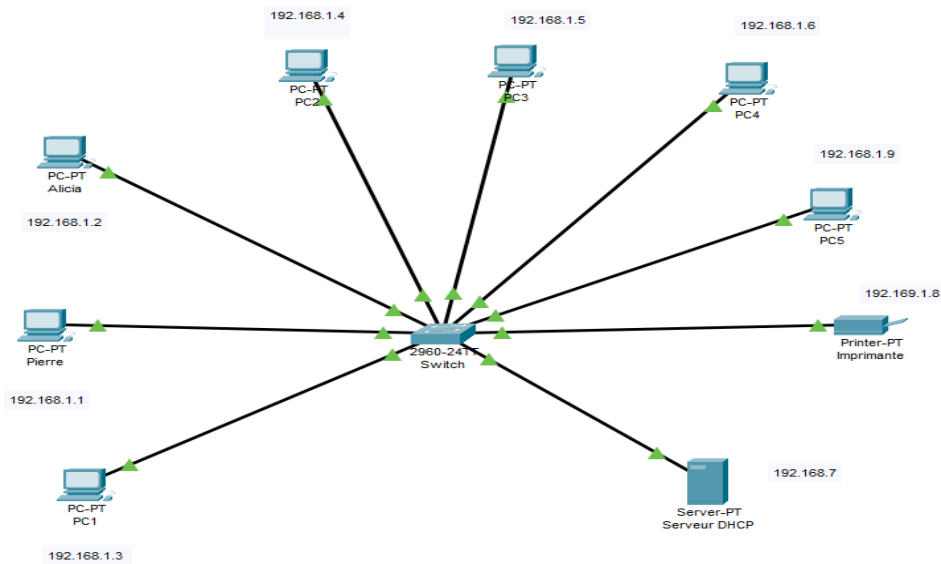


Il existe différents avantages pour l'utilisation de schéma dans le cadre du réseau, en voici 3 :

- Il permet de planifier et de prévoir l'expansion future du réseau. Vous pouvez évaluer vos ressources actuelles facilement et rapidement grâce au schéma et en fonction de vos besoins, prévoir les ajouts que vous allez devoir faire.
- La communication, un schéma de réseau permet de communiquer facilement et rapidement la structure du réseau aux différentes équipes, aux fournisseurs de services et différentes parties prenantes.

- En cas de sinistre, en ayant une vue d'ensemble de la topologie du réseau, il est plus facile de planifier des mesures de sauvegarde et de reprise pour garantir la disponibilité des données en cas de catastrophe

Job 10



Seurver DHCP

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP**
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: reseau

Default Gateway: 192.168.1.1

DNS Server: 10.10.0.1

Start IP Address: 192 168 1 0

Subnet Mask: 255 255 255 0

Maximum Number of Users: 256

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
reseau	192.168.1.1	10.10.0.1	192.168.1.0	255.255.255.0	256	0.0.0.0	0.0.0.0

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 gérée dynamiquement par un serveur DHCP et peut changer à chaque connexion.

Job 11

Ci-dessous le tableau d'adressage réseau correspondant à la consigne avec les 16 sous réseaux demandés :

Adressage réseau						
Adresse réseau	Masque sous réseau	Cidr	Adresse sous réseau	Nombre hôte*	Plage adresse	Adresse broadcast
10.0.0.0	255.255.255.240	28	10.1.0.0	14	10.1.0.1 à 10.1.0.14	10.1.0.15
10.0.0.0	255.255.255.224	27	10.2.0.0	30	10.2.0.1 à 10.2.0.30	10.2.0.31
10.0.0.0	255.255.255.224	27	10.3.0.0	30	10.3.0.1 à 10.3.0.30	10.3.0.31
10.0.0.0	255.255.255.224	27	10.4.0.0	30	10.4.0.1 à 10.4.0.30	10.4.0.31
10.0.0.0	255.255.255.224	27	10.5.0.0	30	10.5.0.1 à 10.5.0.30	10.5.0.31
10.0.0.0	255.255.255.224	27	10.6.0.0	30	10.6.0.1 à 10.6.0.30	10.6.0.31
10.0.0.0	255.255.255.128	25	10.7.0.0	126	10.7.0.1 à 10.7.0.126	10.7.0.127
10.0.0.0	255.255.255.128	25	10.8.0.0	126	10.8.0.1 à 10.8.0.126	10.8.0.127
10.0.0.0	255.255.255.128	25	10.9.0.0	126	10.9.0.1 à 10.9.0.126	10.9.0.127
10.0.0.0	255.255.255.128	25	10.10.0.0	126	10.10.0.1 à 10.10.0.126	10.10.0.127
10.0.0.0	255.255.255.128	25	10.11.0.0	126	10.11.0.1 à 10.11.0.126	10.11.0.127
10.0.0.0	255.255.255.0	24	10.12.0.0	254	10.12.0.1 à 10.12.0.254	10.12.0.255
10.0.0.0	255.255.255.0	24	10.13.0.0	254	10.13.0.1 à 10.13.0.254	10.13.0.255
10.0.0.0	255.255.255.0	24	10.14.0.0	254	10.14.0.1 à 10.14.0.254	10.14.0.255
10.0.0.0	255.255.255.0	24	10.15.0.0	254	10.15.0.1 à 10.15.0.254	10.15.0.255
10.0.0.0	255.255.255.0	24	10.16.0.0	254	10.16.0.1 à 10.16.0.254	10.16.0.255

* Le nombre d'hôtes a déjà été calculé en ayant déjà enlevé l'adresse disponible pour le réseau et la diffusion par exemple pour le Cidr 28 $2^8 - 2 = 14$, nous avons donc 14 hôtes utilisables. Dans la consigne nous avons besoin de 12 places, donc cela fonctionne.

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

Le choix d'une plage d'adresses de classe A 10.0.0.0 pour un réseau privé offre une grande capacité d'hôtes, une flexibilité d'expansion future et simplifie la gestion des adresses IP.

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

La différence fondamentale entre les différents types d'adresses est le nombre d'octet qu'ils allouent au réseau et aux hôtes.

La classe A utilise un octet pour le réseau et trois octets pour les hôtes.

La classe B utilise deux octets pour le réseau et deux octets pour les hôtes.

La classe C utilise trois octets pour le réseau et un octet pour les hôtes.

Job 12

Couche	Description des rôles	Matériels, protocoles, technologies
7- Application	Interface utilisateur	FTP
6- Présentation	Traduction, compression, chiffrement	HTML, SSL/TLS
5- Session	Gestion des sessions, synchronisation, récupère des données en cas de panne de connexions	PPTP
4- Transport	Transport fiable, segmentation des contrôles, contrôle des flux	TCP, UDP
3- Réseau	Détermine le parcours, et l'adressage logique : IP	ipv4, ipv6, routeur
2- liaison des données	Liaison point à point, adressage physique	Ethernet, MAC, WIFI,
1- Physique	Transmission brute sur le support physique, binaire, numérique ou analogique	Fibre optique, câble RJ45



Job 13

Quelle est l'architecture de ce réseau ?

Ce réseau a une architecture en étoile, tous les éléments sont connectés à un switch et uniquement à ce dernier.

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 ?

Nous avons un masque de sous réseau 255.255.255.0, c'est un réseau de classe C. Il y a donc 8 bits alloués aux hôtes. $2^8=256$. On retire à ces 256 adresses IP disponibles l'adresse du réseau et l'adresse de diffusion, on a donc 254 machines qui peuvent être connectées brancher sur ce réseau.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion du réseau est la dernière de la plage, 192.168.10.255.



Job 14

145.32.59.24

En binaire cela donne :

10010001.00100000.00111011.00011000

200.42.129.16

En binaire cela donne :

11001000.00101010.10000001.00010000

14.82.19.54

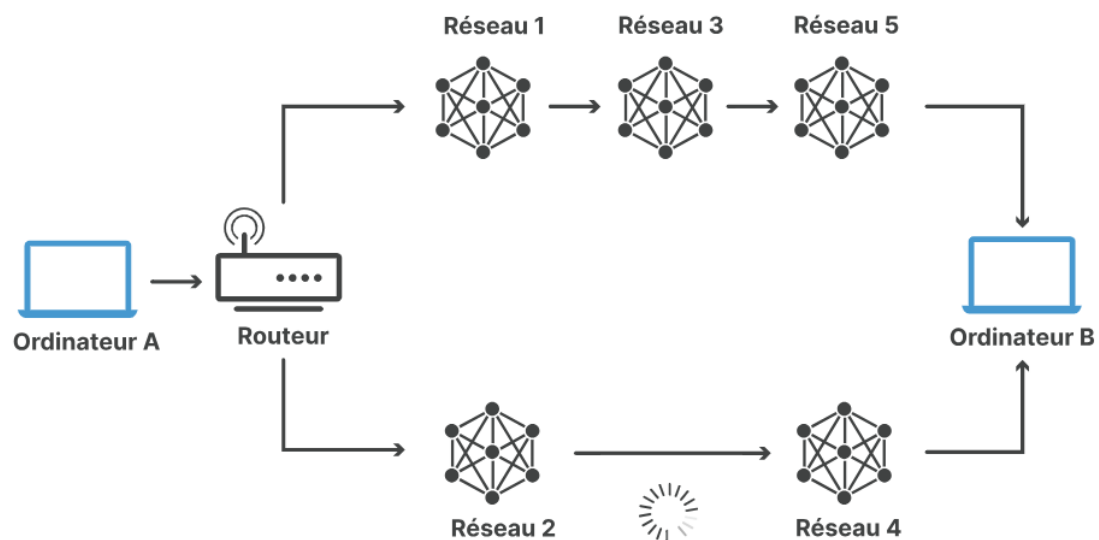
En binaire cela donne :

00001110. 01010010.00010011.00110110

Job 15

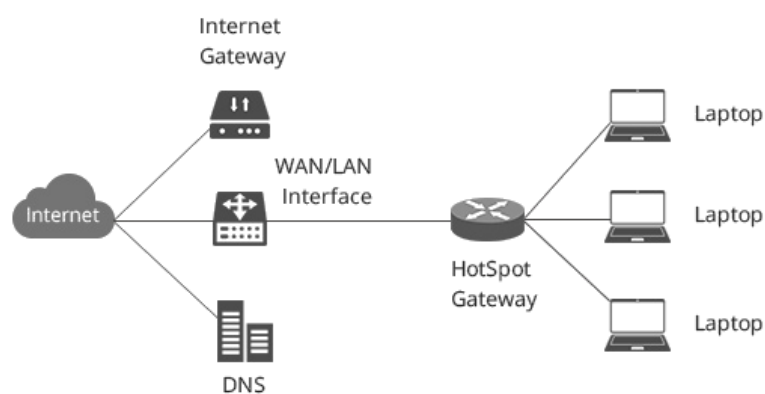
Qu'est-ce que le routage ?

Le routage consiste à déterminer le chemin optimal pour transmettre des données d'un point à un autre à travers un réseau.



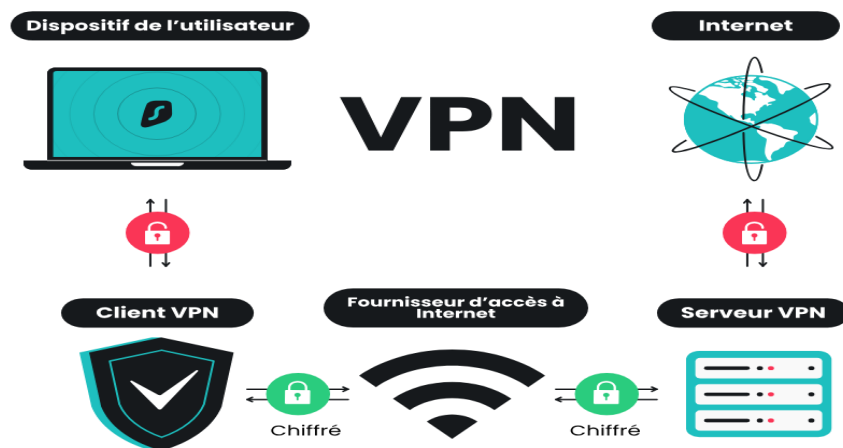
Qu'est-ce qu'un Gateway ?

Un Gateway est un point d'entrée/sortie qui relie deux réseaux différents, facilitant la communication entre eux.



Qu'est-ce qu'un VPN ?

Un VPN est un moyen de sécuriser et de chiffrer les communications sur Internet, en créant un tunnel privé entre un appareil et un serveur distant.



Qu'est-ce qu'un DNS ?

Le DNS convertit les noms de domaine en adresses IP pour faciliter l'accès aux sites web en utilisant des noms compréhensibles au lieu de numéros IP.

