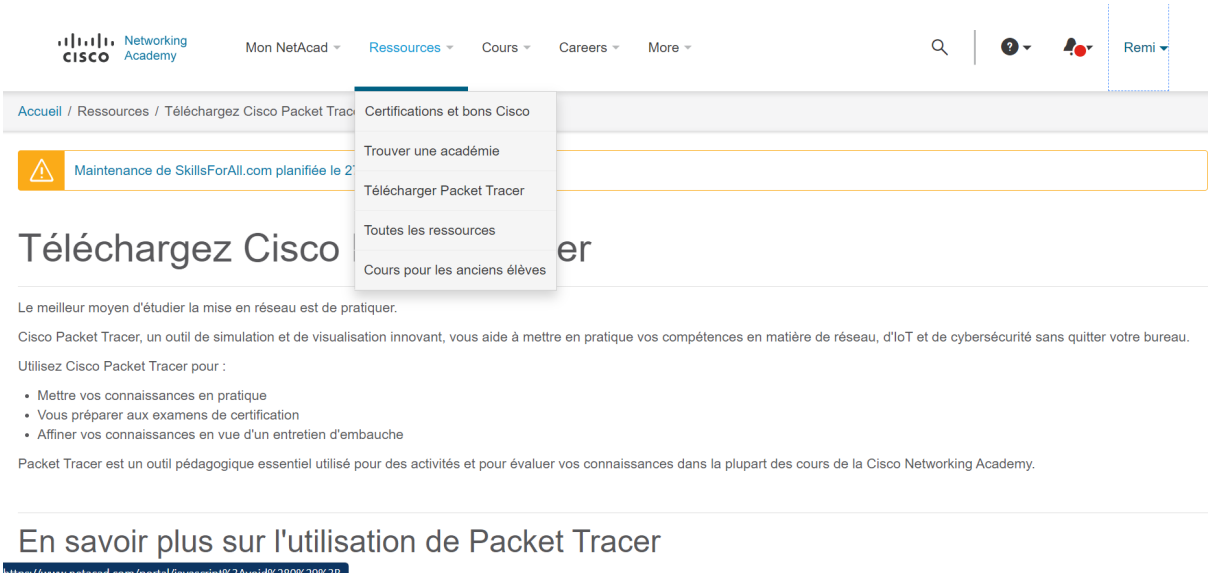
Runtrack Réseaux

Job 01

- Installer packet tracer en allant sur ce lien
- créer votre compte ainsi que votre mot de passe
- Aller sur ressources puis sur **télechargez Packet Tracer**



Job 02

- Un réseau est un ensemble de dispositifs interconnectés, tels que des ordinateurs, des serveurs, des commutateurs, des routeurs, des câbles, des antennes, etc. Ces dispositifs sont liés de manière à ce qu'ils puissent communiquer et partager des données. Il existe différents types de réseaux, notamment les réseaux locaux (LAN), les réseaux étendus (WAN), les réseaux sans fil (Wi-Fi), et les réseaux globaux (Internet).

  Un réseaux informatique sert a plusieurs choses ,notamment :

- Partage de ressources : Les utilisateurs peuvent partager des fichiers, des imprimantes, des bases de données, etc.
  Communication : Les réseaux permettent la communication instantanée par e-mail, messagerie instantanée, vidéoconférence, etc.

  Accès à Internet : La plupart des utilisateurs accèdent à Internet via un réseau.

  Centralisation des données : Les serveurs stockent et gèrent les données centralisées.

  Collaboration : Les équipes de travail peuvent collaborer sur des projets grâce aux réseaux partagés.

  Automatisation des processus : Les réseaux facilitent l'automatisation des tâches et des processus.

  Pour construire un réseau informatique de base, vous aurez besoin des éléments essentiels suivants, chacun ayant une fonction spécifique :

  Ordinateurs et périphériques clients : Ce sont les appareils utilisateurs du réseau. Ils se connectent au réseau pour accéder aux ressources partagées, telles que des fichiers, des imprimantes, des applications, etc.

  Commutateurs (Switches) : Les commutateurs sont des dispositifs qui relient plusieurs appareils au sein d'un réseau local (LAN). Leur fonction principale est de créer un réseau câblé local en interconnectant les ordinateurs, assurant ainsi la transmission efficace des données au sein du réseau.

  Routeur : Le routeur est un dispositif qui interconnecte votre réseau local (LAN) avec d'autres réseaux, tels qu'Internet. Il a pour rôle de diriger le trafic entre le réseau local et les réseaux externes en utilisant des adresses IP. Il offre également des fonctionnalités de sécurité en contrôlant les paquets de données entrants et sortants.

  Câbles Ethernet : Les câbles Ethernet sont utilisés pour connecter les ordinateurs, les commutateurs et le routeur au sein du réseau local. Ils assurent la transmission rapide et fiable des données.

  P**oints d'accès Wi-Fi (Access Points)** : Si vous souhaitez intégrer une connectivité sans fil à votre réseau, les points d'accès Wi-Fi sont nécessaires. Ils permettent aux appareils compatibles Wi-Fi de se connecter au réseau sans fil.

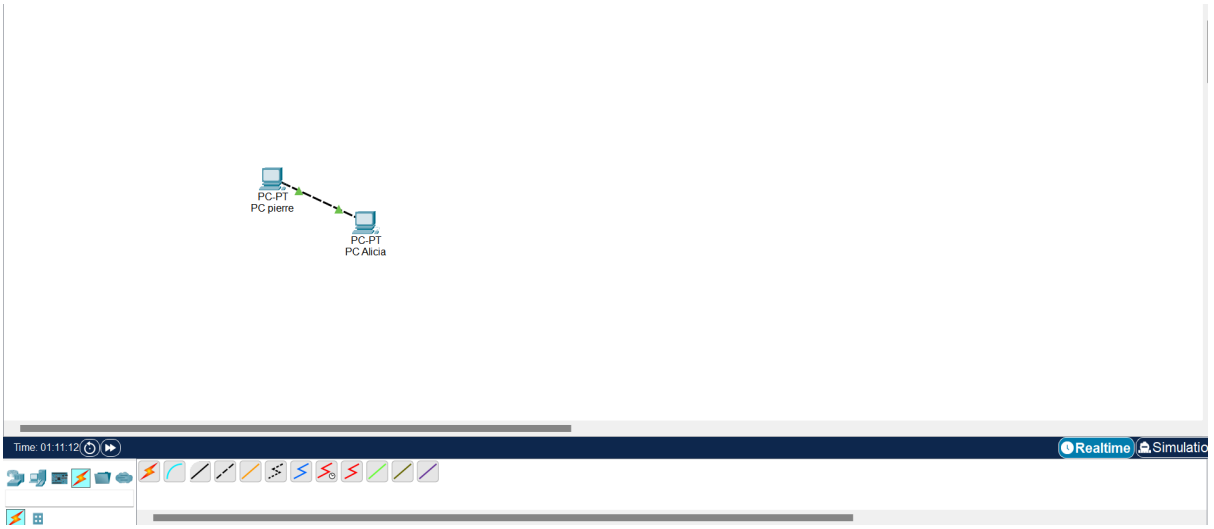
Firewall : Un pare-feu est un dispositif de sécurité qui protège le réseau contre les menaces en filtrant le trafic entrant et sortant. Il peut être matériel (un dispositif dédié) ou logiciel (exécuté sur un ordinateur ou un routeur).

Modem : Si vous souhaitez vous connecter à Internet, un modem est nécessaire. Il établit la connexion avec votre fournisseur de services Internet (FSI) et permet à votre réseau d'accéder à Internet.

Ces éléments constituent la base d'un réseau informatique. En fonction de la taille et de la complexité du réseau, nous pouvons également envisager d'autres composants tels que des serveurs, des imprimantes réseau, des câbles fibre optique, des routeurs plus avancés, des dispositifs de stockage en réseau (NAS), etc. Il est important de concevoir le réseau en fonction des besoins spécifiques en termes de taille, de performances et de sécurité.

Job 03

Dans ce Job nous devons mettre en place dans la zone de travail deux ordinateurs de bureau,reliés entre eux par un câble.



Pour relier les ordinateurs entre eux j'ai choisi un cable croisé car avec celui ci, les ordinateurs peuvent communiquer entre eux sans besoin d'avoir un dispositif intermédiaire pour gérer la connexion.

Job 04

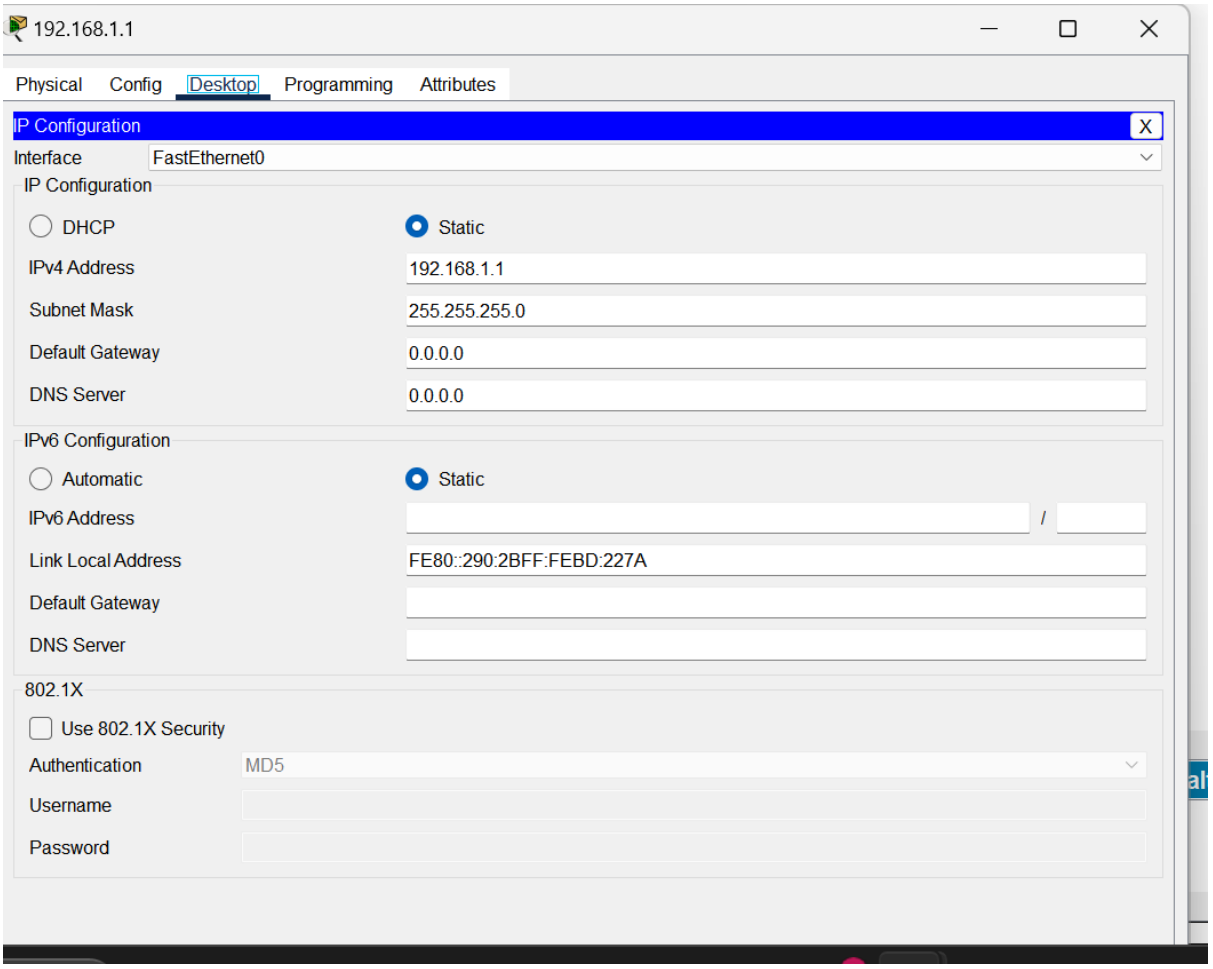
- Une adresse IP (Internet Protocol) est un identifiant numérique attribué à chaque périphérique connecté à un réseau informatique qui utilise le protocole Internet pour la communication. Les adresses IP sont essentielles pour le routage des données sur Internet et au sein des réseaux locaux. Elles sont généralement représentées sous la forme de quatre groupes de chiffres, tels que "192.168.1.7" pour les adresses IPv4 ou sous la forme de chaînes alphanumériques pour les adresses IPv6.

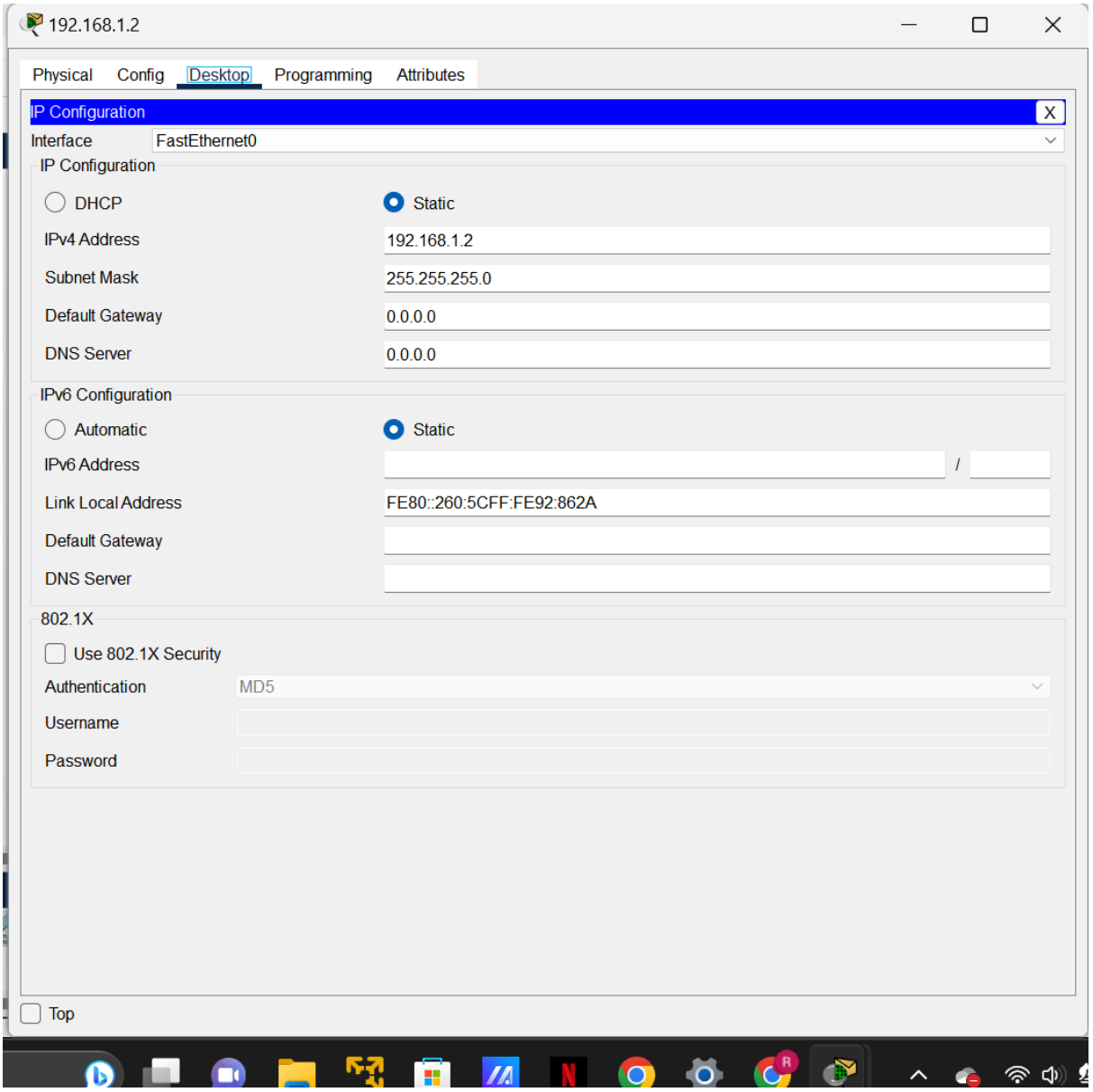
- Les adresses IP servent à identifier et localiser de manière unique chaque dispositif sur un réseau. Elles permettent aux données d'être acheminées vers le bon destinataire, que ce soit à l'échelle locale (dans un réseau domestique ou d'entreprise) ou sur Internet. Les adresses IP sont utilisées pour le partage de ressources, la communication, la navigation sur le web, la diffusion de données et bien d'autres applications réseau.

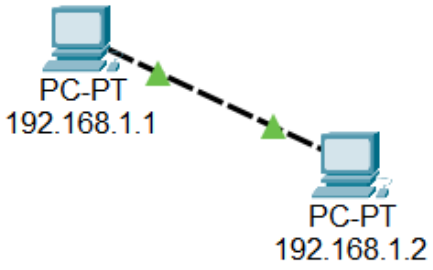
- Une adresse MAC (Media Access Control) est un identifiant physique unique attribué à chaque carte réseau (NIC) dans un dispositif, comme un ordinateur, un smartphone ou un commutateur réseau. Contrairement aux adresses IP, les adresses MAC sont généralement attribuées par le fabricant du matériel et sont permanentes. Elles sont représentées sous forme d'une série de chiffres et de lettres, par exemple, "00:1A:2B:3C:4D:5E".

- Adresse IP publique : Une adresse IP publique est utilisée pour identifier un dispositif sur Internet. C'est l'adresse IP attribuée par votre fournisseur de services Internet (FSI). Les adresses IP publiques sont uniques à l'échelle mondiale et permettent aux dispositifs de communiquer sur Internet. Vous partagez généralement une seule adresse IP publique avec tous les dispositifs de votre réseau domestique grâce à un routeur.
-
- Adresse IP privée : Une adresse IP privée est utilisée à l'intérieur d'un réseau local pour identifier les dispositifs. Ces adresses IP ne sont pas routées sur Internet et sont destinées à une utilisation locale au sein d'un réseau domestique ou d'une entreprise.Le routeur effectue la traduction d'adresse réseau (NAT) pour permettre aux dispositifs de partager une seule adresse IP publique pour accéder

- L'adresse de ce réseaux pour mon pc est 10.10.2.188




192.168.1.2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.2
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:FE92:862A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top



Job 05

- Pour vérifier si l'IP des deux pc est correcte nous utilisons la commande Ipconfig

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::290:2BFF:FEBD:227A
   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:\>
```

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:5CFF:FE92:862A
   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:\>
```

Job 06

- La commande permettant de ping entre le pc de pierre et le pc de Alicia est ping

```
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=4ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time=2ms 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 = 4ms, Average = 2ms

C:\>
```

```
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 = 1ms, Average = 0ms

C:\>
```

Job 07

Le pc de Pierre n'a malheureusement pas reçu les paquets de Alicia

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
```

Lorsque l'on effectue un ping vers un PC éteint, le PC ne reçoit pas les paquets de demande de ping. Par conséquent, il ne peut pas générer de réponse. Ont obtient généralement un message d'erreur indiquant "hôte inaccessible" ou "temps de réponse dépassé" en réponse au ping.Ces messages d'erreur sont totalement justifiée car si le pc est éteint sa carte réseau est aussi désactivée et ne peut pas être détectée, tout simplement

Job 08

- Un hub est un appareil réseau qui fonctionne au niveau de la couche physique du modèle OSI. Il répète simplement les signaux entrant sur un port vers tous les autres ports, ce qui signifie que toutes les données sont diffusées à tous les appareils connectés. Un hub ne prend pas en compte les adresses MAC.

  Un switch fonctionne au niveau de la couche de liaison de données du modèle OSI. Il examine les adresses MAC des appareils connectés pour déterminer à quel port acheminer les trames de données. Un switch isole le trafic, améliorant l'efficacité et la sécurité du réseau.

- Un hub est un appareil réseau qui fonctionne au niveau de la couche physique (couche 1) du modèle OSI. Il répète simplement les signaux entrants reçus sur un port vers tous les autres ports, diffusant ainsi les données à tous les appareils connectés, sans prendre en compte les adresses MAC.

  Les avantages d'un hub est qui sont généralement moins chers que les switches,il sont simple à configurer et à utiliser et ils peuvent être utilisés dans des situations où l'efficacité n'est pas critique, comme de petits réseaux.

  Les inconvénients sont qu'ils génèrent du trafic inutile en diffusant les données à tous les ports, ce qui peut provoquer une utilisation inefficace de la bande passante, ils ne fournissent pas aussi d'isolation du trafic, ce qui pose des problèmes de sécurité, car toutes les données sont accessibles à tous les appareils.

  Il y a beaucoup d'avantages pour les switches notamment :

  Efficacité : Les switches acheminent le trafic uniquement vers les ports nécessaires en fonction des adresses MAC, ce qui réduit le trafic inutile et améliore l'efficacité du réseau.

  Isolation du trafic : Les switches isolent le trafic entre les ports, améliorant la sécurité, car les données ne sont pas diffusées à tous les appareils connectés.

  Élimination des collisions : Les switches éliminent le risque de collisions de données, car ils acheminent les trames de données de manière séparée vers chaque port.

  Adaptabilité : Les switches sont appropriés pour des réseaux de taille moyenne à grande, offrant une évolutivité en fonction des besoins.

  Performances accrues : En raison de leur gestion intelligente du trafic, les switches permettent d'obtenir des performances réseau optimales.

  Ils comporte aussi des inconvénients comme le coût qui sont plus cher que les hubs en raison de leur fonctionnalité avancée, plus complexe et sa consommation électrique

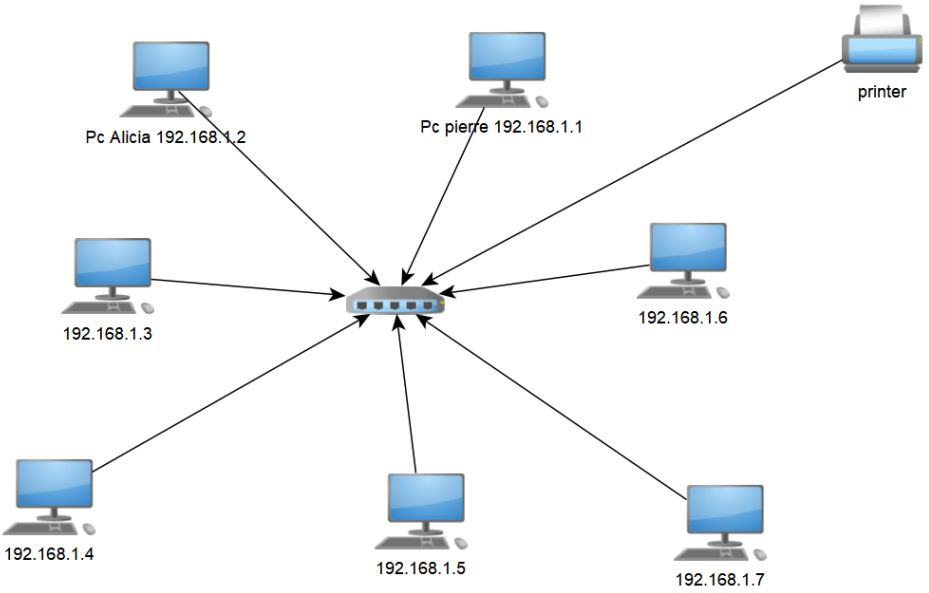
- Un switch gère le trafic réseau en utilisant une table d'adresses MAC pour diriger les trames de données vers les ports appropriés. Il apprend les adresses MAC des appareils connectés et achemine les données

uniquement vers le port auquel l'appareil de destination est connecté, améliorant ainsi l'efficacité, la sécurité et les performances du réseau.

Job09

Un schéma de réseau permet de visualiser et de comprendre facilement la structure et la configuration de votre réseau. Il sert de documentation visuelle précieuse, ce qui est utile pour les administrateurs réseau, les techniciens et les autres membres de l'équipe IT. Cela facilite la communication interne sur la configuration du réseau.
En cas de problèmes ou de pannes réseau, un schéma de réseau bien documenté permet d'identifier rapidement les points problématiques, de localiser les pannes et d'accélérer leur résolution. Les administrateurs peuvent utiliser le schéma pour suivre les connexions, les périphériques et les configurations pour diagnostiquer les problèmes plus efficacement.

Un schéma de réseau facilite la planification de l'expansion du réseau. Vous pouvez visualiser comment de nouveaux appareils, des modifications de topologie ou des mises à niveau matérielles affectent le réseau existant. Cela vous permet de prendre des décisions informées pour l'évolution de votre infrastructure.



Sur le schéma ci-dessus j'ai connecté en cable droits 7 Pc et une Imprimante dans un commutateur , 5 pc nommé avec leurs Adresse IP et 2 nommé Alicia et Pc Pierre. J'ai nommé les 7 pc avec leur adresse IP pour savoir ou j'ai donner les adresse ip fixe pour éviter de me tromper et de perdre du temps à savoir quel pc j'ai mis une adresse ip fixe, j'ai ensuite ajouté un commutateur pour interconnecter le réseaux.

Job 10

En résumé les la différence entre une adresse IP statique et une adresse IP attribuée par DHCP est que :

- Adresse IP statique : Configurée manuellement, ne change pas, adaptée aux dispositifs nécessitant une adresse IP constante.

- Adresse IP attribuée par DHCP : Assignée automatiquement, peut changer, adaptée aux dispositifs clients pour simplifier la gestion.

Job11

- Sous réseaux de 12 hôtes

Sous réseaux	Masque de sous réseau	Plage d'adresse IP Validées	Plage d'adresses Hôtes Valides
1	/28	10.0.0.1 - 10.0.0.15	10.0.0.2 - 10.0.0.14

- 5 sous réseaux de 30 hôtes

Sous réseaux	Masque de sous réseau	Plage d'adresse IP Validées	Plage d'adresses Hôtes Valides
1	/27	10.0.0.16 - 10.0.0.47	10.0.0.17 - 10.0.0.46
2	/27	10.0.0.48 - 10.0.0.79	10.0.0.49 - 10.0.0.78
3	/27	10.0.0.80 - 10.0.0.111	10.0.0.81 - 10.0.0.110
4	/27	10.0.0.112 - 10.0.0.143	10.0.0.113 - 10.0.0.142
5	/27	10.0.0.144 - 10.0.0.175	10.0.0.145 - 10.0.0.174

- 5 sous réseaux de 120 hôtes

Sous réseaux	Masque de sous réseaux	Plage d'adresse IP Validées	Plages d'adresses Hôtes Valides
1	/25	10.0.0.176 - 10.0.0.303	10.0.0.177 - 10.0.0.302
2	/25	10.0.0.304 - 10.0.0.431	10.0.0.305 - 10.0.0.430
3	/25	10.0.0.432- 10.0.0.559	10.0.0.433 - 10.0.0.558
4	/25	10.0.0.560 - 10.0.0.687	10.0.0.561 - 10.0.0.686
5	/25	10.0.0.688 - 10.0.0.815	10.0.0.689 - 10.0.0.814

- 5 sous réseaux de 160 hôtes

Sous réseaux	Masque de sous réseaux	Plages d'adresse IP Validées	Plages d'adresse Hôtes Valides
1	/25	10.0.0.816 - 10.0.0.983	10.0.0.817 - 10.0.0.982
2	/25	10.0.0.984 - 10.0.1.110	10.0.0.985 - 10.0.0.109
3	/25	10.0.1.111 - 10.0.1.238	10.0.1.112 -10.0.1.237
4	/25	10.0.1.239 - 10.0.1.365	10.0.1.240 - 10.0.1.364
5	/25	10.0.1.366 - 10.0.1.493	10.0.1.367 - 10.0.1.492

- On choisit généralement une adresse de classe A, comme 10.0.0.0, pour les réseaux privés et internes en raison de sa capacité à prendre en charge un grand nombre d'hôtes (jusqu'à 16 777 214) et de sa pertinence pour une organisation privée. L'adresse 10.0.0.0 offre également une plage d'adresses contiguë, ce qui facilite la gestion des réseaux privés.

- La différences entres les différents types d'adresses

Classe A :
Plage d'adresses : 1.0.0.0 à 126.0.0.0.
Structure : Un octet pour le réseau, trois octets pour les hôtes.
Utilisation : Convient aux grands réseaux, avec la capacité de prendre en charge un grand nombre d'hôtes. Souvent utilisé pour des réseaux privés internes.
Classe B :
Plage d'adresses : 128.0.0.0 à 191.255.0.0.
Structure : Deux octets pour le réseau, deux octets pour les hôtes.
Utilisation : Adapté aux réseaux de taille moyenne, prenant en charge un nombre modéré d'hôtes.

Classe C :

Plage d'adresses : 192.0.0.0 à 223.255.255.0.

Structure : Trois octets pour le réseau, un octet pour les hôtes.

Utilisation : Conçu pour de petits réseaux, avec une capacité limitée d'hôtes.

Classe D :

Plage d'adresses : 224.0.0.0 à 239.255.255.255.

Utilisation : Réservée pour les groupes multicast, utilisée pour la diffusion de données à plusieurs destinataires simultanément.

Classe E :

Plage d'adresses : 240.0.0.0 à 255.255.255.255.

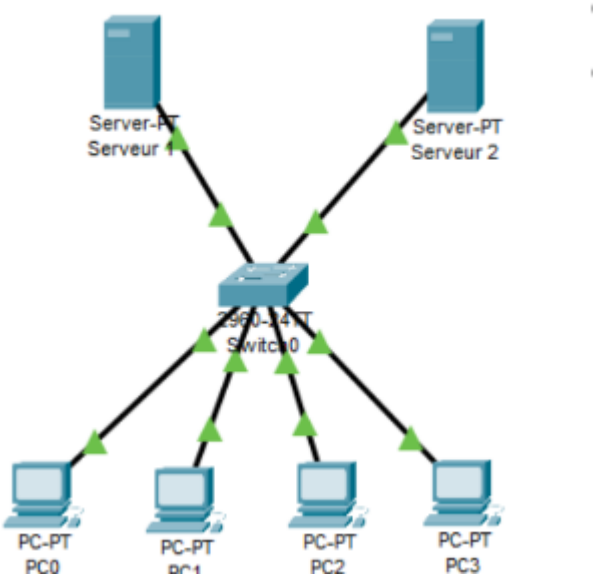
Utilisation : Réservée à des fins expérimentales et ne fait pas partie de l'adressage IP couramment utilisé.

Les différences majeures entre ces classes résident dans la structure des adresses, la plage d'adresses, la capacité en termes d'hôtes, et les usages spécifiques. Le choix de la classe d'adresse dépend des besoins de l'organisation et de la taille prévue du réseau. De nos jours, de nombreuses organisations utilisent des sous-réseaux pour optimiser l'utilisation des adresses IP et répondre aux besoins spécifiques de leur réseau..

JOB 12

Couche OSI	Rôle	Matériels/Protocoles
Couche 7 (Application)	Fournit des interfaces pour les applications utilisateur, telles que les navigateurs web, les clients de messagerie, etc.	HTML, FTP , SSL/TLS,PPTP
Couche 6 (Présentation)	Gère la traduction, la compression et le chiffrement des données. Elle s'occupe de la mise en forme des données pour la transmission.	SSL/TLS
Couche 5 (Session)	Établit, gère et termine les sessions de communication, telles que les sessions de chat ou les sessions vidéo.	
Couche 4 (Transport)	Fournit un contrôle de bout en bout de la communication, gère le flux de données et assure la fiabilité de la transmission.	TCP, UDP
Couche 3 (Réseau)	Gère la transmission des données à travers un réseau. Elle effectue le routage, le transfert de paquets et la résolution d'adresses IP.	Ipv4, IPV6, routeur
Couche 2 (Liaison de données)	Gère l'accès au support de transmission (comme Ethernet ou Wi-Fi) et effectue la détection d'erreurs	Ethernet,MAC (adresse matérielle),Wi-FI
Couche 1 (Physique)	Gère la transmission brute des données sur le support physique, définissant les propriétés électriques, mécaniques et optiques.	Fibre optique, câble RJ45

JOB 13



- L'architecture de ce réseau est une **architecture en étoile (Star Topology)** car tous les appareils sont connectés à un commutateur (switch).
- L'adresse ip du réseaux et sans aucun doute 192.168.10.0

- Logiquement nous pouvons brancher 254 machines sur ce réseau, en utilisant des adresses IP allant de 192.168.10.1 à 192.168.10.254. Cela est dû au masque de sous-réseau 255.255.255.0, qui alloue 8 bits pour les hôtes, permettant ainsi 2^8 - 2 = 254 adresses IP disponibles pour les machines.
  (Le symbole '^' fait référence aux signes de puissance des math).

- Si L'adresse ip du réseaux est 192.168.10.0 l'adresse de diffusion est certainement 192.168.10.255

JOB 14

- 145.32.59.24 :

  145 en binaire : 10010001
  32 en binaire : 00100000
  59 en binaire : 00111011
  24 en binaire : 00011000
  L'adresse IP 145.32.59.24 en binaire est donc : 10010001.00100000.00111011.00011000.

  200.42.129.16 :

  200 en binaire : 11001000
  42 en binaire : 00101010
  129 en binaire : 10000001
  16 en binaire : 00010000
  L'adresse IP 200.42.129.16 en binaire est donc : 11001000.00101010.10000001.00010000.

  14.82.19.54 :

  14 en binaire : 00001110
  82 en binaire : 01010010
  19 en binaire : 00010011
  54 en binaire : 00110110
  L'adresse IP 14.82.19.54 en binaire est donc : 00001110.01010010.00010011.00110110.

JOB 15:

Le Routage : Le routage est le processus de transmission de données à travers un réseau en choisissant le meilleur chemin. Il permet de diriger les données du point source au point de destination en utilisant des routeurs pour prendre des décisions de transfert.

La Gateway (Passerelle) : Une passerelle est un dispositif ou un logiciel qui connecte deux réseaux distincts, permettant la communication entre eux. Elle sert de point d'entrée ou de sortie pour les données entre ces réseaux, souvent en effectuant la traduction des protocoles de communication.

Le VPN (Virtual Private Network) : Un VPN est un système qui crée une connexion sécurisée et cryptée entre un appareil et un réseau, généralement via Internet. Il est utilisé pour protéger la confidentialité des données, permettant un accès sécurisé à distance à des ressources réseau et masquant l'emplacement de l'utilisateur.

Le DNS (Domain Name System) : Le DNS est un système qui associe des noms de domaine conviviaux à des adresses IP numériques, permettant ainsi aux utilisateurs d'accéder à des sites Web en utilisant des noms faciles à retenir plutôt que des adresses IP. Il facilite la navigation sur Internet en traduisant les noms de domaine en adresses IP.