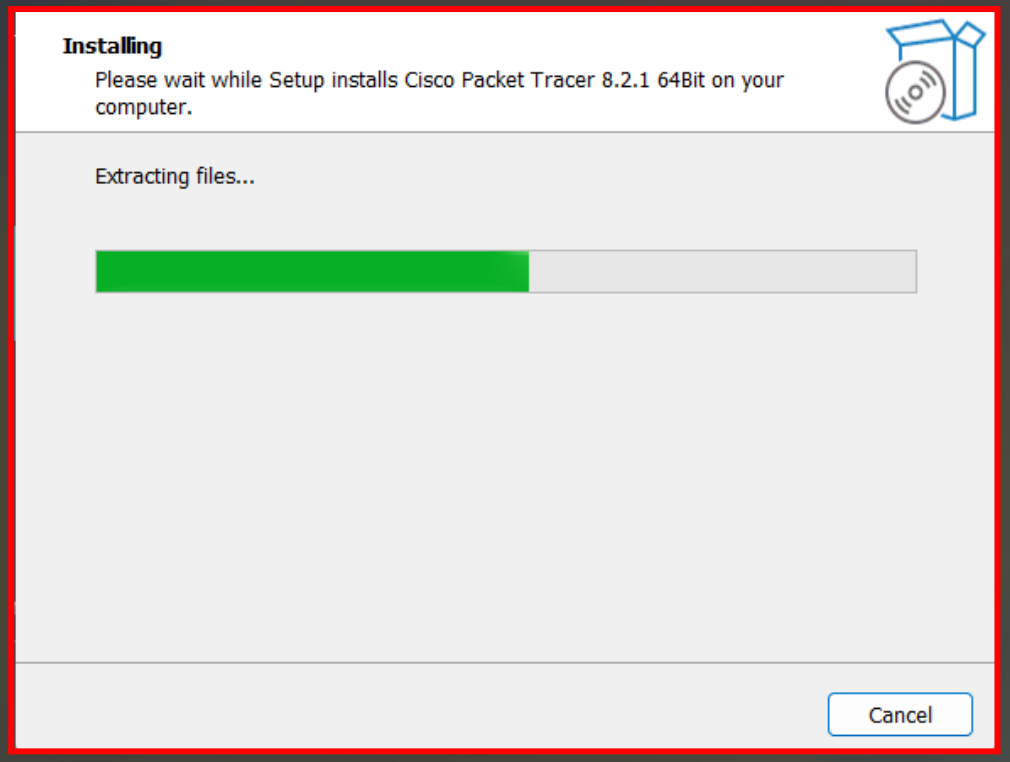

Installing
Please wait while Setup installs Cisco Packet Tracer 8.2.1 64Bit on your computer.
Extracting files...
Cancel

Qu'est-ce qu'un réseau ?

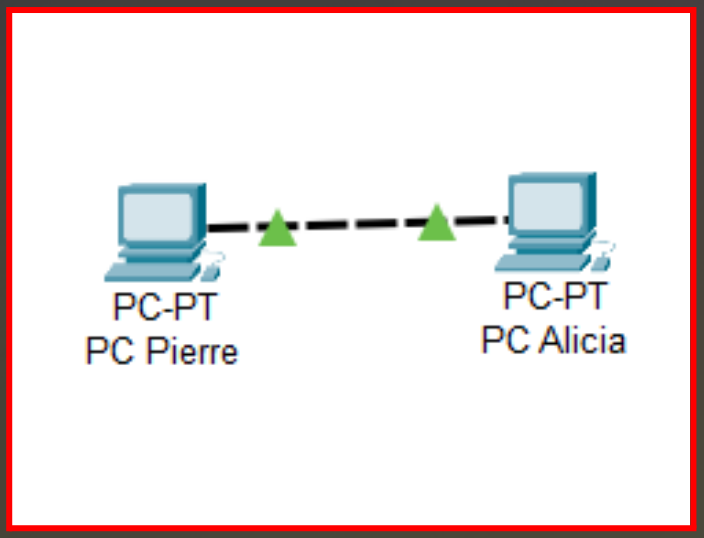
C'est un système qui relie des ordinateurs et des appareils électroniques. Ces réseaux peuvent être câblés ou sans fil.

À quoi sert un réseau informatique ?

Un réseau informatique facilite la communication et le partage de données entre appareils électroniques. Il permet de collaborer, d'accéder à Internet, de gérer des données de manière centralisée et d'automatiser divers dispositifs. Ces réseaux sont essentiels tant à un niveau personnel que professionnel pour simplifier la communication et l'accès à des services variés.

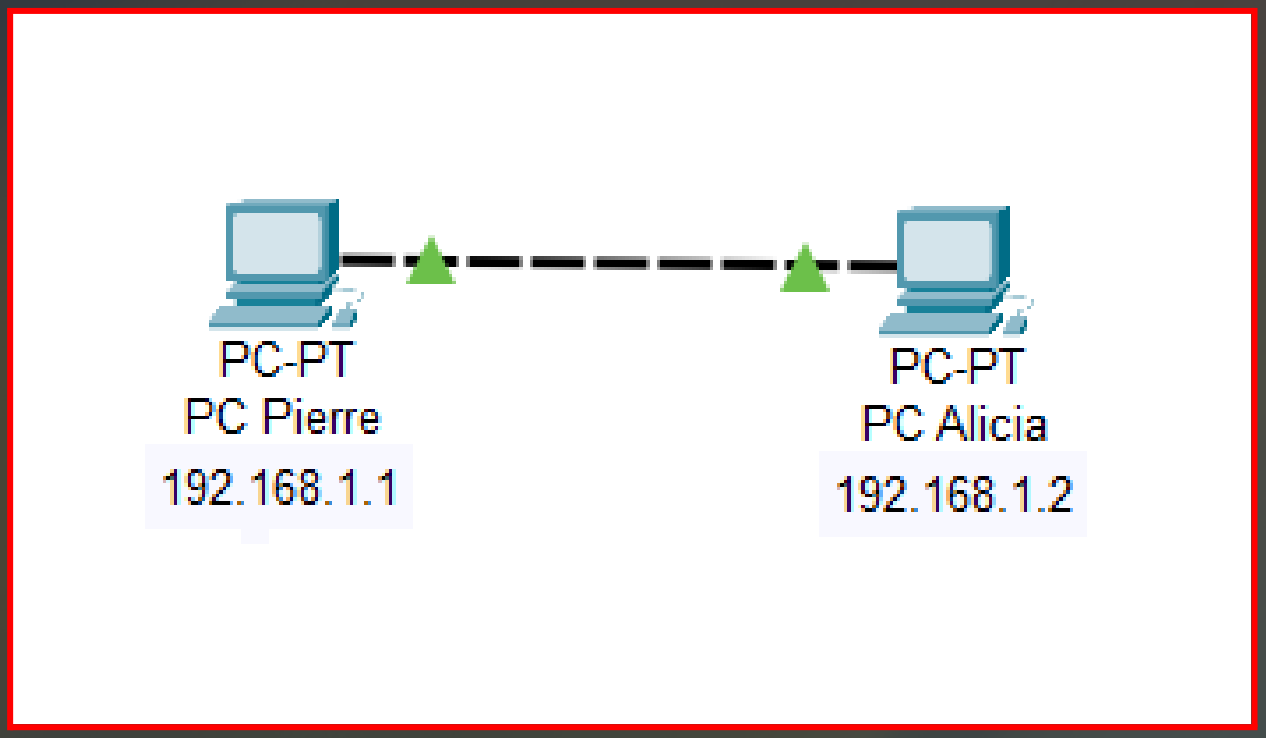
Quel matériel avons-nous besoin pour construire un réseau ?

Pour construire un réseau informatique, il vous faut des ordinateurs et des appareils réseau, des câbles ou une connectivité sans fil, un routeur pour relier votre réseau à Internet, des commutateurs pour connecter vos appareils localement, des points d'accès sans fil si vous souhaitez un réseau Wi-Fi, des serveurs si nécessaire, des logiciels réseau pour gérer et contrôler le trafic, un pare-feu pour la sécurité, un système d'adressage IP et des protocoles de communication, et enfin, du personnel compétent pour la configuration, la maintenance et la sécurité du réseau. L'ensemble de ces éléments constitue une infrastructure réseau solide pour répondre à vos besoins



CROSS-OVER

Un câble croisé est nécessaire pour connecter directement deux ordinateurs dans Packet Tracer. Cela évite les conflits de signaux en permettant une communication directe entre les deux PC, ce qui n'est pas possible avec un câble Ethernet standard conçu pour connecter des appareils différents. En résumé, le câble croisé assure une communication fluide entre deux ordinateurs sans l'interférence de signaux grâce à son agencement spécifique des fils.


PC-PT
PC Pierre
192.168.1.1
PC-PT
PC Alicia
192.168.1.2

Qu'est-ce qu'une adresse IP ?

Une adresse IP est une suite de chiffres assignée à chaque appareil connecté à un réseau informatique, permettant ainsi son identification unique sur ce réseau. Ces chiffres sont structurés selon un protocole spécifique, tel que IPv4 ou IPv6, et servent à acheminer les données vers l'appareil approprié.

À quoi sert une IP ?

Elle sert à identifier de manière unique et localiser un appareil ou un nœud sur un réseau informatique, lui permettant ainsi de communiquer avec d'autres appareils et de recevoir des données. Cela facilite le routage des informations sur Internet, assurant que les données parviennent à la destination correcte. En résumé, une adresse IP est essentielle pour l'acheminement des données à travers les réseaux informatique

Qu'est-ce qu'une adresse MAC ?

L'adresse MAC (Media Access Control) est essentiellement l'identifiant unique de la carte réseau de tout appareil connecté à un réseau. Imaginez-le comme le numéro de série qui distingue chaque appareil dans l'univers des réseaux informatiques. Contrairement à l'adresse IP, elle reste inchangée et joue un rôle vital dans la communication entre appareils au sein d'un réseau local.

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

Une adresse IP publique est attribuée à votre routeur par votre fournisseur d'accès Internet et permet aux appareils sur Internet de vous trouver. En revanche, une adresse IP privée est utilisée au sein de votre réseau local pour que vos appareils puissent se parler, créant ainsi une sorte de "réseau interne" tout en restant hors de vue depuis Internet, ce qui renforce la sécurité de vos données locales.

Quelle est l'adresse de ce réseau ?

L'adresse de ce réseau serait habituellement 192.168.1.0. Cependant, gardez à l'esprit que 192.168.1.0 est souvent utilisée pour désigner le réseau lui-même, tandis que 192.168.1.1 et 192.168.1.2 sont attribuées aux machines. En général, les adresses IP de 192.168.1.1 à 192.168.1.254 sont disponibles pour les dispositifs dans un réseau de classe C standard, avec 192.168.1.255 réservée pour les diffusions.

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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:17FF:FEAD:25DB
   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
```

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

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::250:FFF:FE51:D015
   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
```

La commande utilisé pour vérifier l'IP de la machine est **"ipconfig"**

JOB N°6

```
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
```

```
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
```

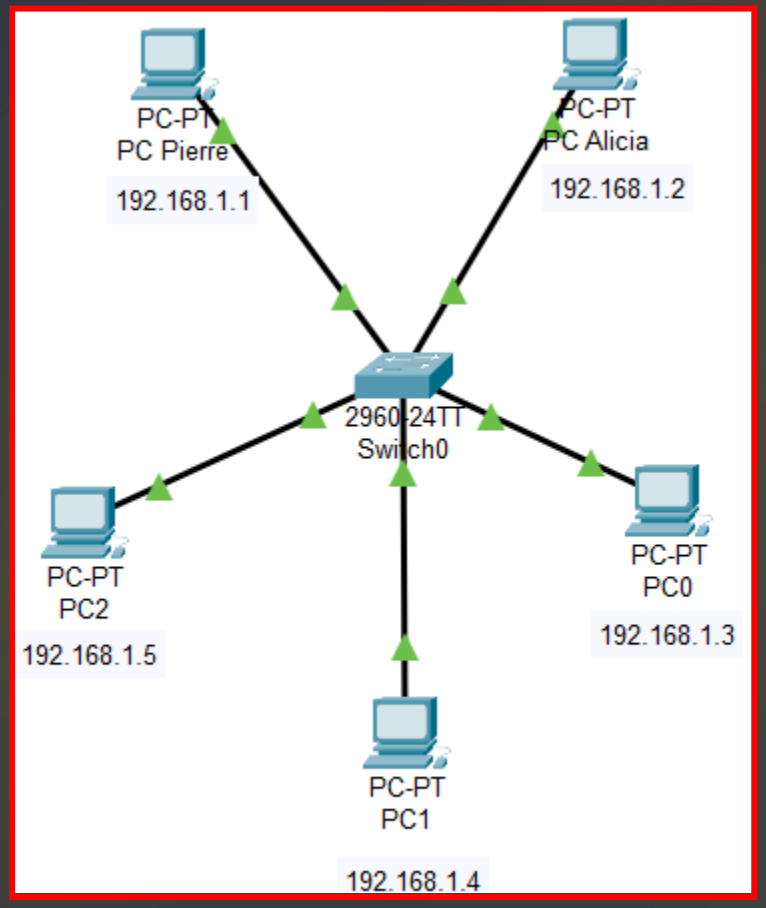
Pour ping une machine, il suffit juste de taper la commande **“ping”** suivit de l’IP de la machine.

JOB N°7

```
Cisco Packet Tracer PC Command Line 1.0
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 ping vers un ordinateur éteint ne fonctionne pas car le ping envoie des paquets de données pour demander une réponse de l'ordinateur cible. Lorsque l'ordinateur est éteint, il ne peut pas répondre, donc le ping ne reçoit aucune réponse. En résumé, le ping nécessite un ordinateur actif pour fonctionner.

JOB N°8




```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=16ms 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


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


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

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
```

Quelle est la différence entre un hub et un switch ?

Un hub fonctionne au niveau physique du réseau. Il reçoit des données d'un port et les transmet à tous les autres ports, ce qui signifie que toutes les données sont diffusées à tous les appareils connectés.

En revanche, un switch fonctionne au niveau de liaison de données. Il examine l'adresse MAC de chaque appareil connecté à ses ports et envoie les données uniquement au port où l'appareil de destination est connecté.

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

Un hub est un dispositif réseau qui transmet les données de chaque appareil à tous les autres, ce qui peut entraîner une utilisation inefficace de la bande passante et des problèmes de sécurité. Ils sont simples à utiliser et économiques, mais leur inefficacité a conduit à leur remplacement par des commutateurs plus performants dans la plupart des réseaux modernes.

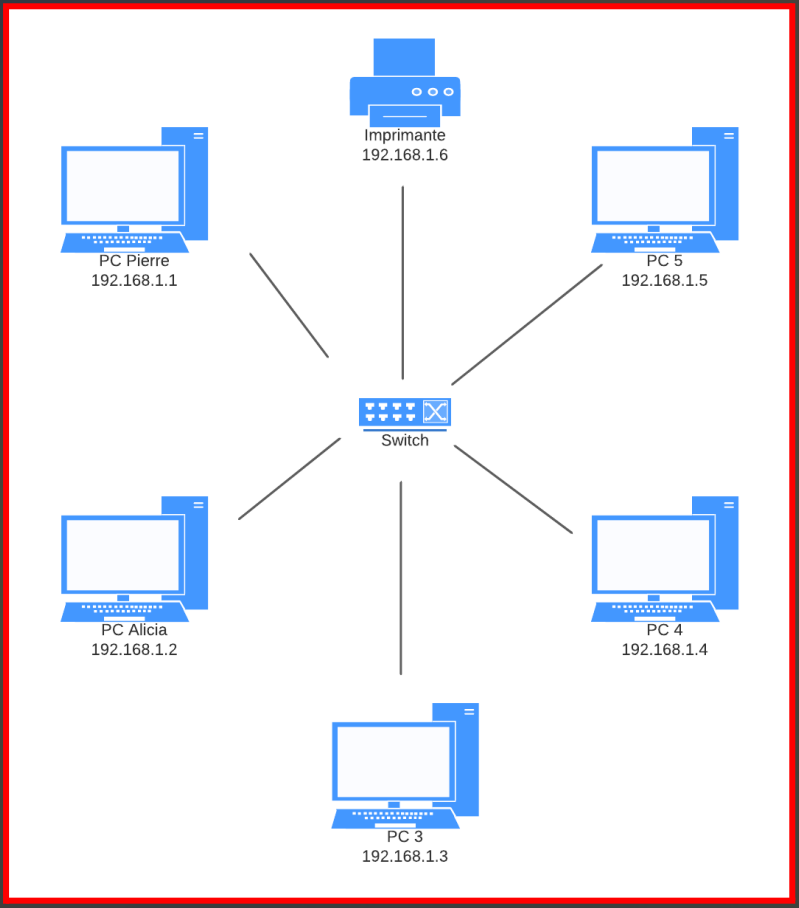
Quels sont les avantages et inconvénients d'un switch ?

Les avantages d'un switch incluent une meilleure efficacité de la bande passante, une sécurité accrue grâce à l'isolation des ports, et une gestion intelligente du trafic, réduisant les collisions. Cependant, les inconvénients potentiels résident dans leur coût plus élevé par rapport aux hubs, ainsi que dans la nécessité de configuration dans certains cas.

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

Un switch gère le trafic réseau en utilisant des tables de correspondance d'adresses MAC pour diriger les données vers le port approprié. Lorsqu'un appareil se connecte au switch, ce dernier apprend l'adresse MAC de l'appareil et la stocke dans sa table. Lorsqu'un appareil envoie des données, le switch examine l'adresse MAC de destination et la compare à sa table pour déterminer le port auquel envoyer les données. Cela permet au switch de diriger efficacement les données uniquement vers le port nécessaire, réduisant les collisions et améliorant les performances du réseau.

JOB N°9



Les avantages du schéma

Un schéma offre une clarté visuelle, rendant les informations complexes plus accessibles en présentant les éléments d'une manière facile à comprendre.

Il structure visuellement des idées ou des données, facilitant ainsi la visualisation de relations et de connexions.

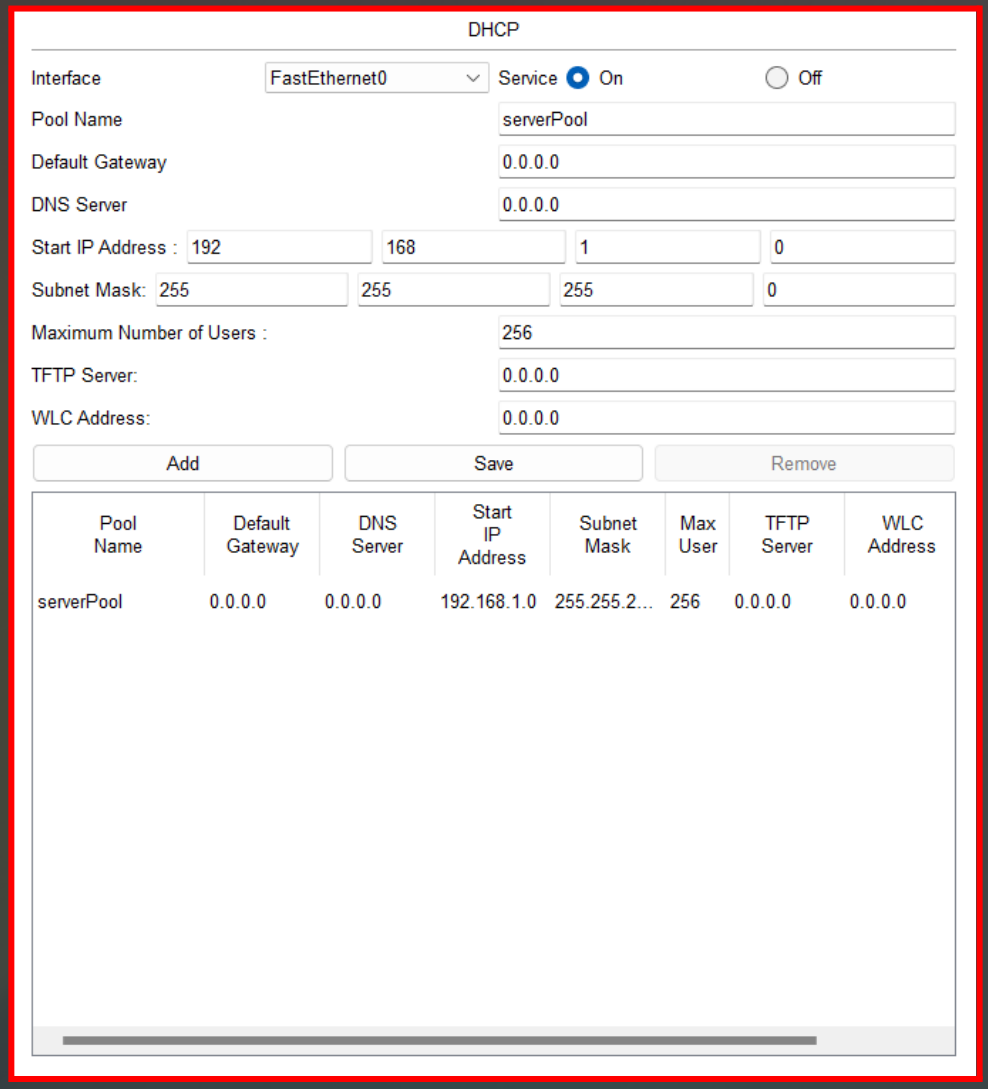
Lorsqu'il s'agit de résoudre des problèmes, un schéma permet de représenter graphiquement les composants en jeu, aidant à identifier les causes, les conséquences et à élaborer des solutions de manière plus systématique.

JOB N°10

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

Une adresse IP statique est une adresse fixe que vous définissez manuellement pour un appareil, tandis qu'une adresse IP attribuée par DHCP est automatiquement assignée par un serveur réseau et peut changer à chaque connexion.

Cela donne une certaine stabilité aux adresses statiques, tandis que les adresses DHCP sont plus flexibles et adaptées aux appareils qui se connectent de manière temporaire.



Sous-réseau	Adresse de réseau	Masque de sous-réseau	Plage d'adresses	Nombre d'hôtes
1	10.0.0.0	255.255.255.240	10.0.0.1 - 10.0.0.15	12
2	10.0.0.16	255.255.255.224	10.0.0.17 - 10.0.0.46	30
3	10.0.0.48	255.255.255.224	10.0.0.49 - 10.0.0.78	30
4	10.0.0.80	255.255.255.224	10.0.0.81 - 10.0.0.110	30
5	10.0.0.112	255.255.255.224	10.0.0.113 - 10.0.0.142	30
6	10.0.0.144	255.255.255.224	10.0.0.145 - 10.0.0.174	30
7	10.0.0.176	255.255.255.128	10.0.0.177 - 10.0.0.254	120
8	10.0.1.0	255.255.255.128	10.0.1.1 - 10.0.1.127	120
9	10.0.1.128	255.255.255.128	10.0.1.129 - 10.0.1.254	120
10	10.0.2.0	255.255.255.128	10.0.2.1 - 10.0.2.128	120

Sous-réseau	Adresse de réseau	Masque de sous-réseau	Plage d'adresses	Nombre d'hôtes
11	10.0.2.128	255.255.255.128	10.0.2.129 - 10.0.2.254	120
12	10.0.3.0	255.255.255.192	10.0.3.1 - 10.0.3.62	160
13	10.0.3.64	255.255.255.192	10.0.3.65 - 10.0.3.126	160
14	10.0.3.128	255.255.255.192	10.0.3.129 - 10.0.3.190	160
15	10.0.3.192	255.255.255.192	10.0.3.193 - 10.0.3.254	160
16	10.0.4.0	255.255.255.192	10.0.4.1 - 10.0.4.62	160
17-21	Non spécifié	Non spécifié	Non spécifié	Non spécifié

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

L'adresse 10.0.0.0 de classe A a été choisie pour créer des sous-réseaux en raison de sa capacité à prendre en charge un grand nombre d'adresses IP.

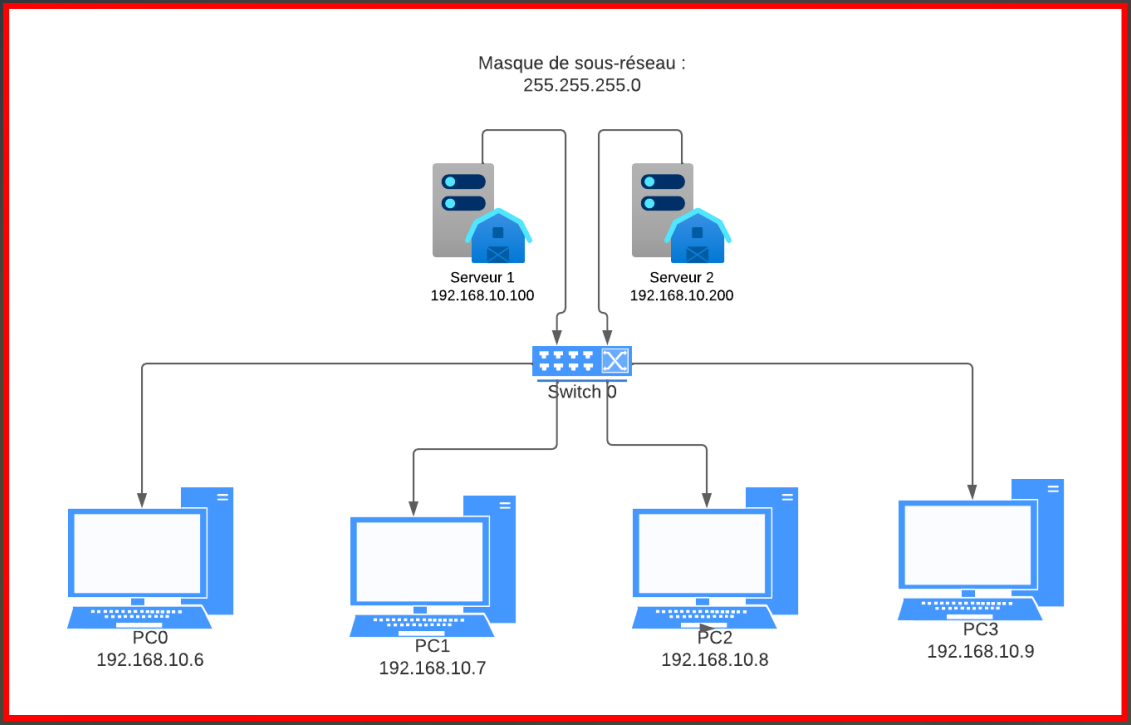
Quelle est la différence entre les différents types d'adresses ?

La différence entre les classes d'adresses réside principalement dans la plage d'adresses et le nombre d'hôtes qu'elles peuvent prendre en charge.
Les classes A, B, et C ont des plages et des capacités d'adressage différentes.

- **Classe A** : Couvre une vaste plage d'adresses de 1.0.0.0 à 126.255.255.255 et peut prendre en charge un grand nombre d'hôtes.
- **Classe B** : Couvre une plage d'adresses de 128.0.0.0 à 191.255.255.255 et prend en charge un nombre intermédiaire d'hôtes.
- **Classe C** : Couvre une plage d'adresses de 192.0.0.0 à 223.255.255.255 et est conçue pour un nombre limité d'hôtes.

Couche OSI	Composants/Protocoles	Description des rôles
Couche 7 - Application	FTP, HTML, SSL/TLS	Fournit des services d'application aux utilisateurs, gère l'interface utilisateur, et la communication applicative.
Couche 6 - Présentation	SSL/TLS	Gère la traduction, la compression, le cryptage des données pour l'application.
Couche 5 - Session	PPTP, FTP	Établit, gère et termine les sessions entre les applications sur différentes machines.
Couche 4 - Transport	TCP, UDP	Fournit un transport de bout en bout fiable (TCP) ou non fiable (UDP) pour les données.
Couche 3 - Réseau	IPv4, IPv6, routeur	Gère le routage des paquets de données à travers un réseau, identifie les machines via des adresses IP.
Couche 2 - Liaison de données	Ethernet, MAC, Wi-Fi	Gère la communication entre les machines au sein du même réseau local, contrôle l'accès au support partagé.
Couche 1 - Physique	Fibre optique, câble RJ45	Gère les signaux physiques qui transportent les données sur le support, détaille les spécifications matérielles.

JOB N°13


Masque de sous-réseau :
255.255.255.0
Serveur 1
192.168.10.100
Serveur 2
192.168.10.200
Switch 0
PC0
192.168.10.6
PC1
192.168.10.7
PC2
192.168.10.8
PC3
192.168.10.9

Quelle est l'architecture de ce réseau ?

L'architecture de ce réseau est une architecture en étoile. Dans une architecture en étoile, tous les appareils du réseau sont connectés à un point central, qui est généralement un commutateur ou un routeur.

Dans ce cas, le commutateur ou le routeur central gère la communication entre les quatre PC (PC0, PC1, PC2, PC3) et les deux serveurs (Serveur 1, Serveur 2).

Tous les appareils sont sur le même sous-réseau et sont connectés directement ou indirectement au commutateur ou au routeur central, ce qui facilite la communication au sein du réseau.

Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP du réseau, dans ce contexte, est 192.168.10.0. Cette adresse représente l'ensemble du réseau où se trouvent les PC et les serveurs.
C'est l'adresse qui identifie ce réseau spécifique au sein de la plage d'adresses IP 192.168.10.0/24.

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

Avec un masque de 255.255.255.0, on dispose de 8 bits pour les adresses des machines.

Et donc avec 8 bits, vous avez 2^8 combinaisons possibles, soit 256. Cependant, il y a deux adresses que vous ne pouvez pas utiliser, l'adresse réseau (192.168.10.0) et l'adresse de diffusion (192.168.10.255). Donc, le nombre d'adresses IP utilisables pour les machines est de 256 - 2, ce qui équivaut à 254.

En résumé, vous pouvez brancher jusqu'à 254 machines sur ce réseau sans souci d'adresses IP en double.

Quelle est l'adresse de diffusion de ce réseau ?

Comme j'ai noté ci dessus, l'adresse de diffusion est 192.168.10.255

145.32.59.24 en binaire est : 10010001.00100000.00111011.00011000

200.42.129.16 en binaire est : 11001000.00101010.10000001.00010000

14.82.19.54 en binaire est : 00001110.01010010.00010011.00110110

Qu'est-ce que le routage ?

Le routage est le processus fondamental de transmission de données au sein d'un réseau, qui implique la sélection du meilleur chemin pour acheminer les paquets de données de la source vers la destination. Il repose sur des protocoles spécifiques et des tables de routage pour déterminer l'itinéraire optimal, garantissant ainsi l'efficacité de la transmission des données.

Qu'est-ce qu'un gateway ?

Une gateway, ou passerelle, est un élément essentiel des réseaux informatiques. Elle agit comme une interface entre deux réseaux distincts, facilitant la communication entre eux. Les gateways assurent des fonctions telles que la traduction de protocoles, la sécurité, le filtrage du trafic et la gestion du flux de données entre les réseaux.

Qu'est-ce qu'un VPN ?

Un VPN est un système de communication sécurisé qui permet de créer un tunnel chiffré entre un périphérique et un serveur distant. Il est principalement utilisé pour sécuriser la communication sur des réseaux publics, garantissant la confidentialité et la sécurité des données. Les VPN masquent également l'adresse IP de l'utilisateur, préservant ainsi son anonymat.

Qu'est-ce qu'un DNS ?

Le DNS est un service de base qui assure la résolution des noms de domaine en adresses IP. Il agit comme un annuaire qui permet de traduire les noms de domaine conviviaux en adresses IP numériques, ce qui facilite la localisation des ressources sur Internet. Les serveurs DNS jouent un rôle crucial dans le fonctionnement du Web, en permettant aux utilisateurs d'accéder aux sites Web à l'aide de noms de domaine.