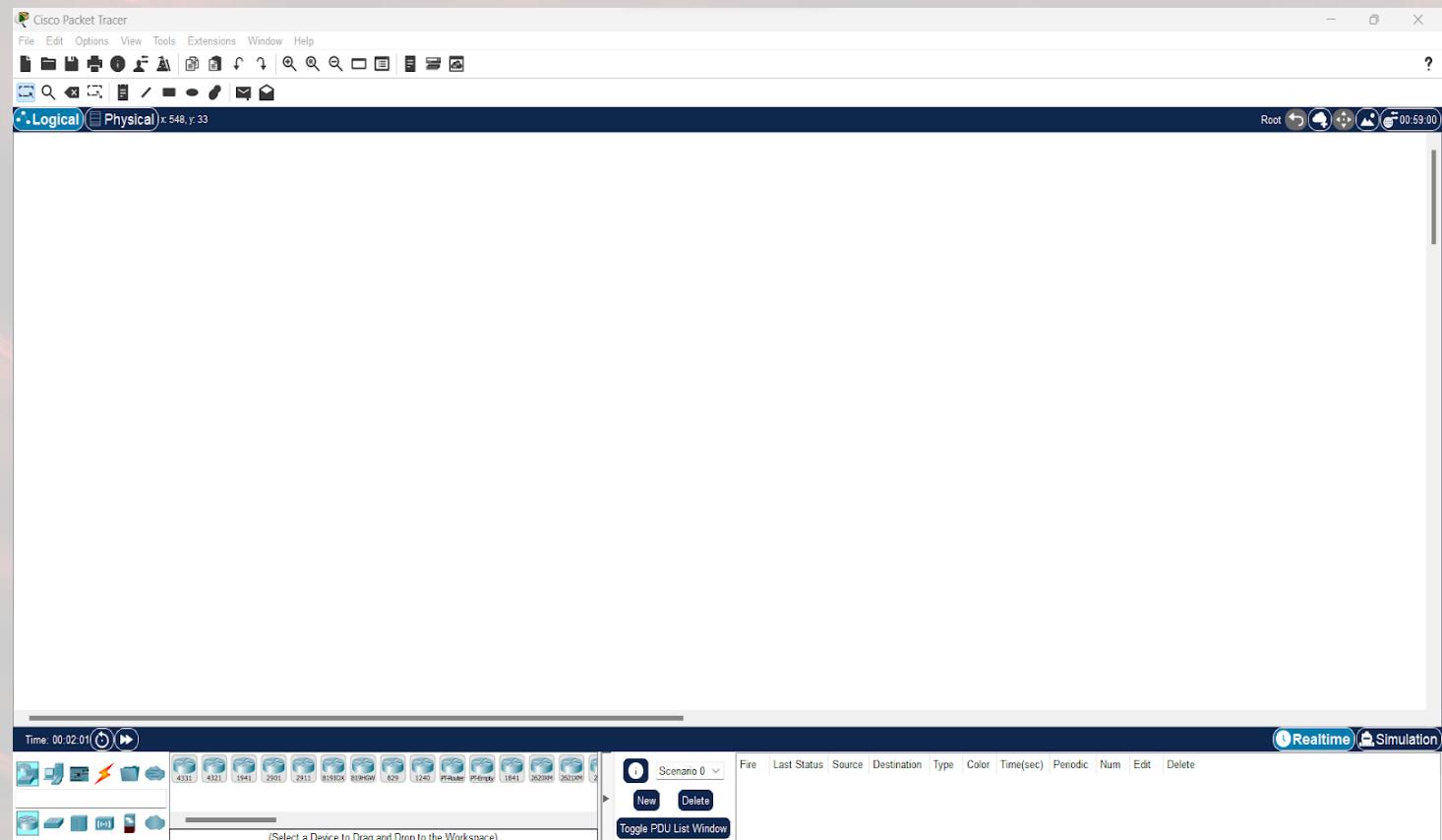


# RunTrack Réseau

Dossier préparé par Olivier DURAND

JOB 1

# Installation de Cisco Packet Tracer



## JOB 2

# FAQ Réseau

## ■ Qu'est-ce qu'un réseau ?

Un réseau informatique (data communication network ou DCN) est un ensemble d'équipements reliés entre eux pour échanger des informations.

Par analogie avec un filet (un réseau est un « petit rets », c'est-à-dire un petit filet), on appelle nœud l'extrémité d'une connexion, qui peut être une intersection de plusieurs connexions ou équipements (un ordinateur, un routeur, un concentrateur, un commutateur).

Indépendamment de la technologie sous-jacente, on porte généralement une vue matricielle sur ce qu'est un réseau.

De façon horizontale, un réseau est une strate de trois couches : les infrastructures, les fonctions de contrôle et de commande, les services rendus à l'utilisateur.

De façon verticale, on utilise souvent un découpage géographique : réseau local, réseau d'accès et réseau d'interconnexion.

## ■ À quoi sert un réseau informatique ?

Un réseau informatique est un outil fondamental pour la communication, le partage de ressources, la collaboration, la gestion des données et l'accès à l'Internet, ce qui en fait un élément essentiel de la technologie moderne et de l'informatique.

Les réseaux informatiques ont de nombreuses utilisations et offrent de nombreux avantages, notamment :

**Partage de ressources** : Les réseaux permettent le partage de ressources telles que des imprimantes, des fichiers, des applications et des périphériques, ce qui peut réduire les coûts et améliorer l'efficacité au sein d'une organisation.

**Communication** : Les réseaux permettent la communication entre les utilisateurs, que ce soit via la messagerie électronique, la messagerie instantanée, la visioconférence, ou d'autres moyens de communication en ligne.

**Accès à l'Internet** : Les réseaux fournissent un accès à l'Internet, offrant aux utilisateurs la possibilité de naviguer sur le web, de rechercher des informations, de consulter leurs courriels et de réaliser diverses activités en ligne.

**Stockage centralisé** : Les réseaux permettent le stockage centralisé des données, ce qui facilite la sauvegarde et la gestion des informations au sein d'une organisation.

**Collaborations** : Les réseaux permettent la collaboration en ligne, que ce soit pour travailler sur des projets partagés, partager des documents, ou collaborer à distance.

**Automatisation des processus** : Les réseaux sont utilisés pour l'automatisation de processus commerciaux et industriels, ce qui peut augmenter l'efficacité et réduire les erreurs humaines.

**Sécurité** : Les réseaux permettent la mise en place de mesures de sécurité informatique pour protéger les données et les systèmes contre les menaces en ligne.

**Mobilité** : Les réseaux sans fil, tels que les réseaux Wi-Fi, offrent la mobilité, permettant aux utilisateurs de se connecter à partir de divers endroits.

**Gestion à distance** : Les réseaux permettent la gestion à distance des systèmes informatiques, ce qui est essentiel pour la maintenance et le dépannage à distance.

# ■ Quel matériel avons-nous besoin pour construire un réseau ?

## Détails des fonctions de chaque pièce

### Matériel

#### Carte réseau

### Fonctions des pièces

La carte réseau est l'interface entre l'ordinateur et le réseau. Elle reçoit les données émises par l'ordinateur et les transfère vers un autre appareil présent sur le réseau, contrôle l'ensemble de ces données et les flux échangés.

#### Concentrateur (hub)

Le Hub a pour unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports. Tout comme le répéteur, le concentrateur opère au niveau 1 du modèle OSI, c'est la raison pour laquelle il est parfois appelé répéteur multiports.

#### Commutateur (switch)

Le Switch est un équipement qui relie plusieurs segments dans un réseau informatique et de télécommunication et qui permet de créer des circuits virtuels. La commutation est un des deux modes de transport de trame au sein des réseaux informatiques et de communication, l'autre étant le routage.

#### Routeur

Un routeur est un appareil permettant de créer un réseau Wi-Fi. Il doit pour cela être relié à un modem. Il envoie les informations provenant d'Internet à vos appareils personnels (ordinateurs, téléphones et tablettes).

#### Répéteur

Le répéteur fonctionne comme une seconde box, et va ainsi reproduire le signal wifi à l'identique. Un répéteur wifi permet de conserver le même nom de réseau wifi que celui de votre box. Pensez à placer votre répéteur wifi dans une zone bien couverte par votre routeur.

## JOB 3

# Installation de mon 1er réseau

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

Pour relier les deux ordinateurs nous avons opté pour les câbles croisés. Le câble croisé est utilisé pour connecter deux ou plusieurs appareils informatiques. Le câblage interne des câbles croisés inverse les signaux de transmission et de réception (le signal envoyé sur le câble TX depuis l'ordinateur 1 peut être reçu sur le câble RX de l'ordinateur 2). Il est largement utilisé pour connecter deux appareils du même type : par exemple deux ordinateurs ou deux commutateurs entre eux.

## JOB 4

IP

### ■ Qu'est-ce qu'une adresse IP ?

Une adresse IP est un numéro d'identification unique attribué de façon permanente ou provisoire à chaque périphérique faisant partie d'un même réseau informatique utilisant l'Internet Protocol. L'adresse IP est à l'origine du système d'acheminement des paquets de données sur Internet.

### ■ À quoi sert un IP ?

Le but d'une adresse IP est de gérer la connexion entre un appareil et un site de destination. L'adresse IP identifie de manière unique chaque appareil sur Internet. Sans elle, il n'y a aucun moyen de les contacter. Les adresses IP permettent aux appareils informatiques (tels que les PC et les tablettes) de communiquer avec des destinations telles que les sites Web et les services de streaming, et ils permettent aux sites Web de savoir qui se connecte. Une adresse IP sert également d'adresse de retour, au même sens qu'une adresse de retour sur courrier postal. Lorsque vous postez une lettre et qu'elle est livrée à la mauvaise adresse, vous récupérez la lettre si vous incluez une adresse de retour sur l'enveloppe. Il en va de même pour le courrier électronique. Lorsque vous écrivez à un destinataire non valide (par exemple, un correspondant qui a quitté son entreprise), votre adresse IP permet au serveur de messagerie de l'entreprise de vous envoyer un e-mail de renvoi indiquant que la destination est introuvable.

### ■ 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.

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

**Une adresse IP publique** est une adresse IPv4 accessible à partir d'Internet. Elle est attribuée à votre routeur réseau par votre fournisseur d'accès Internet (FAI). Votre appareil personnel possède également une adresse IP privée qui n'est pas divulguée lorsque vous vous connectez à Internet via l'adresse IP publique de votre routeur. Utiliser une adresse IP publique pour se connecter à Internet, c'est un peu comme utiliser une boîte postale pour le courrier postal plutôt que communiquer l'adresse de votre domicile. C'est un peu plus sûr, mais beaucoup plus visible.

Une adresse IP privée ce sont toutes les adresses IP qui ne sont pas utilisables sur internet, par exemple le réseau de votre entreprise ou le réseau domestique. Un réseau privé est un réseau qui utilise les plages d'adresses IP non accessibles depuis Internet.

Elles permettent de communiquer localement avec vos différents périphériques..

Les adresses IP privées se trouvent dans les classes A, B et C.

Voici les plages d'adresse IP privé selon les classes :

- Les adresses privées de la classe A : 10.0.0.0 à 10.255.255.255 (comprend 16 millions d'adresses)
- Les adresses privées de la classe B : 172.16.0.0 à 172.31.255.255 (comprend 65535 adresses)
- Les adresses privées de la classe C : 192.168.0.0 à 192.168.255.255 (comprend 256 adresses)

## ■ Quelle est l'adresse de ce réseau ?

L'adresse du réseau est 192.168.1

JOB 5

# ID des machines

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

Je suis allé sur le terminal Command Prompt sur le PC Pierre et ensuite sur le PC Alicia et j'ai utilisé la commande Ipconfig

```
C:\>ipconfig

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

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2E0:8FFF:FE4D:39DD
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::2E0:8FFF:FE4D:39DD
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:\>clean
Invalid Command.

C:\>clear
Invalid Command.

C:\>
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::201:C7FF:FE98:E347
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 6

# Ping

## ■ Quelle est la commande permettant de Ping entre des PC ?

La commande permettant le ping entre les PC est **ping adresse ip** (du pc recherché)

Par exemple, depuis le PC de Pierre je cherche à faire un ping avec le PC Alicia donc la commande permettant le Ping sera “ping 192.168.1.2” (adresse ip d'Alicia).

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix.:
Link-local IPv6 Address..... FE80::2E0:8FFF:FE4D:39DD
IPv6 Address..... :: 192.168.1.1
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..... :: 192.168.1.1
IPv6 Address..... :: 0.0.0.0
IPv4 Address..... :: 0.0.0.0
Subnet Mask..... 0.0.0.0
Default Gateway..... :: 0.0.0.0

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<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:\>
```

```
Default Gateway..... :: 0.0.0.0

Bluetooth Connection:

Connection-specific DNS Suffix.:
Link-local IPv6 Address..... :: 192.168.1.1
IPv6 Address..... :: 0.0.0.0
IPv4 Address..... :: 0.0.0.0
Subnet Mask..... 0.0.0.0
Default Gateway..... :: 0.0.0.0

C:\>ping

Cisco Packet Tracer PC Ping

Usage: ping [-n count | -v TOS | -t ] target

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

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 192.168.1.1

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),
C:\>
```

## JOB 7

# Echange de paquets par le ping

## ■ Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ?

Le PC de Pierre n'a pas réceptionné les paquets envoyés par Alicia car 4 paquets ont été envoyés et ces mêmes 4 paquets ont été perdus donc le PC de Pierre en a reçu 0.

## ■ Expliquez pourquoi ?

Les PC de Pierre et d'Alicia n'ont pas pu communiquer entre eux car le PC de Pierre était éteint au moment d'effectuer le test de connectivité réseau entre deux ordinateurs.

## JOB 8

# Développer le réseau

## ■ Quelle est la différence entre un hub et un switch ?

Un Hub est un périphérique qui connecte plusieurs périphériques Ethernet sur un même réseau et les faire fonctionner ensemble en un seul réseau. Un Hub ne collecte pas d'informations.

Un switch est un périphérique réseau qui effectue le même travail que le Hub mais qui est considéré comme un **Hub plus intelligent car il collecte des informations sur les paquets de données qu'il reçoit et les transmet au seul réseau auquel il était destiné.**

Les Hubs et les Switchs sont des périphériques utilisés dans la mise en réseau de données sur Internet. Ces périphériques sont utilisés pour connecter deux ports réseau ou plus afin de transférer des données tout au long d'une connexion. Bien que la tâche principale des Hubs et des Switch soit la même pour transférer des données vers différents réseaux mais ils fonctionnent de différentes manières.

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

Un hub fonctionne sur la couche physique de la couche OSI.

On utilise 'Store and forwarding' lorsqu'il reçoit un paquet de données.

Un réseau local virtuel(VLAN) ne peut être créé avec un Hub.

Généralement il possède 4 à 12 ports.

Il transmet uniquement les signaux électriques ou les bits.

Le hub n'utilise aucun logiciel et ne dispose pas de mémoire pour la mémorisation des périphériques connectés au réseau.

Un Hub prend en charge le mode de transmission semi-duplex et n'a qu'un seul domaine de diffusion

Attention il est impossible d'apprendre les adresses MAC et aucun ne peut les transférer et de prendre en charge le protocole Spanning Tree

Les collisions de paquets se produisent généralement dans un hub

## ■ Quels sont les avantages et inconvénients d'un switch ?

### Avantages des Switchs :

1. Augmente la capacité – Ils augmentent la capacité de transfert de données accessible de l'organisation.
2. Réduit la charge – Ils aident à réduire la charge exceptionnelle sur les ordinateurs hôtes individuels.
3. Incrémenter la présentation – Ils incrémentent la présentation de l'organisation.
4. Moins d'impacts sur le boîtier – Les réseaux qui utilisent des commutateurs auront moins d'impacts sur le boîtier. Cela est dû à la façon dont les commutateurs créent des zones d'impact pour chaque association.
5. Simple – Les commutateurs peuvent être directement associés aux postes de travail.
6. Augmente la bande passante – Il augmente la bande passante disponible du réseau.
7. Moins de collisions de trames – Les réseaux qui utilisent des commutateurs auront moins de collisions de trames

8. Plus sécurisé – Étant donné que le commutateur est isolé, les données n'iront qu'à la destination.

#### Inconvénients des switchs :

1. Coûteux – Ils sont plus coûteux que les étendues de réseau.
2. Problèmes de disponibilité difficiles – Les problèmes de disponibilité du réseau sont difficiles à suivre via le changement d'organisation.
3. Problèmes de diffusion du trafic – Le trafic de diffusion peut être problématique.
4. Sans défense – Si les commutateurs sont en mode aveugle, ils sont sans défense contre les attaques de sécurité, par exemple la caricature d'adresse IP ou la capture de contours Ethernet.
5. Nécessité d'une planification appropriée – Une planification et un agencement appropriés sont nécessaires pour traiter les colis multidiffusion.
6. Les composants mécaniques peuvent s'user – Les composants mécaniques du commutateur peuvent s'user avec le temps.
7. Le contact physique est obligatoire – Doit avoir un contact physique avec l'objet à actionner.

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

Un switch (ou commutateur Ethernet) est un dispositif réseau dont le rôle principal est de gérer efficacement le trafic réseau en fonction des adresses MAC (Media Access Control) des dispositifs connectés à un réseau local.

Voici comment un switch gère le trafic réseau :

**Apprentissage des adresses MAC** : Lorsqu'un commutateur est mis en service, il commence par un tableau de commutation (table MAC) vide. Au fur et à mesure que des paquets de données passent par le switch, il enregistre les adresses MAC des dispositifs connectés aux ports. Il maintient une liste des adresses MAC associées à chaque port pour savoir où diriger le trafic.

**Filtrage et commutation** : Lorsqu'un commutateur reçoit un paquet de données, il examine l'adresse MAC de destination du paquet. Il consulte ensuite sa table MAC pour déterminer le port associé à cette adresse MAC. Si l'adresse MAC est déjà présente dans la table, le switch envoie le paquet uniquement vers le port approprié, limitant ainsi le trafic inutile.

**Broadcast et inconnus** : Lorsque le switch reçoit un paquet de diffusion (broadcast) ou un paquet avec une adresse MAC de destination inconnue, il le transmet à tous les ports du réseau local, à l'exception du port source. Cela garantit que les dispositifs reçoivent les paquets de diffusion (par exemple, ARP) et permet au switch d'apprendre de nouvelles adresses MAC.

**Éviter les collisions** : Contrairement à un hub, qui diffuse les données sur tous les ports, un switch ne crée pas de collision de paquets sur le réseau. Il envoie le trafic uniquement aux ports appropriés, ce qui améliore l'efficacité et la performance du réseau.

**Séparation des domaines de diffusion** : Un commutateur divise le réseau en segments isolés en termes de diffusion. Les paquets de diffusion sont transmis uniquement aux ports qui ont besoin de les recevoir, réduisant ainsi le trafic inutile et le bruit sur le réseau.

**Gestion de la bande passante** : Un switch peut attribuer la bande passante de manière égale entre les ports ou en fonction des besoins du trafic. Les commutateurs plus avancés offrent des fonctionnalités telles que la qualité de service (QoS) pour prioriser certains types de trafic.

**Redondance** : Les commutateurs modernes prennent souvent en charge la mise en place de liens redondants pour assurer la disponibilité du réseau. Cette fonctionnalité permet de basculer automatiquement vers un autre chemin en cas de défaillance d'un lien.

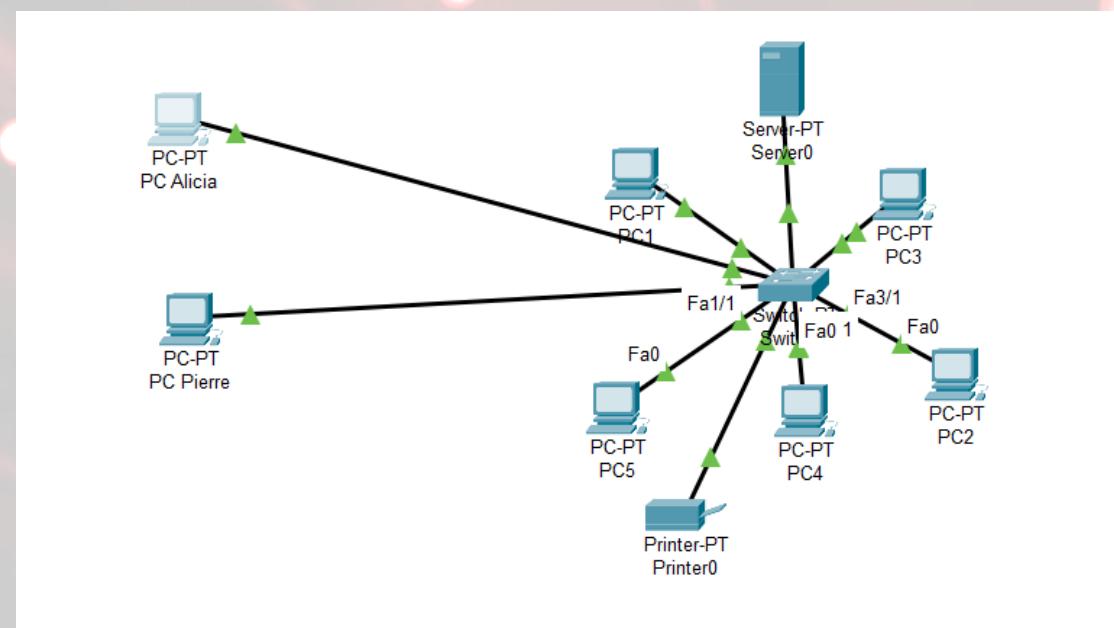
Un switch gère le trafic réseau en utilisant une table MAC pour diriger le trafic de manière efficace vers les dispositifs appropriés. Cela améliore les performances, réduit la congestion et permet une gestion plus intelligente du réseau.

# Schéma de mon réseau

## ■ 3 avantages importants d'avoir un schéma

1. Avoir une vue d'ensemble des composants et des périphériques utilisés et reliés entre eux
2. Déetecter les pannes directement pour faciliter le dépannage
3. Développement et déploiement de nouvelles solutions

## ■ Schéma de mon réseau



JOB 10

# Serveur DHCP

Server0

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: serverPool

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Start IP Address: 169 254 0 0

Subnet Mask: 0 0 0 0

Maximum Number of Users: 512

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
server1	0.0.0.0	192.168.1.10	192.168.1.15	255.255.2...	10	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	0.0.0.0	169.254.0.0	0.0.0.0	512	0.0.0.0	0.0.0.0

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

Ce qui distingue avant tout ces deux types d'adresses, c'est la fiabilité de connexion accrue qu'offrent les IP statiques.

Vos appareils personnels peuvent changer d'adresse IP dynamique chaque fois qu'ils se connectent à un réseau : cela n'a rien de problématique.

Ça l'est en revanche pour les sites commerciaux, tels Netflix et Facebook, qui ont besoin d'adresses IP statiques pour aider leurs clients à se connecter sans encombre à leurs plateformes.

En effet, les IP statiques maintiennent la qualité du débit ainsi que de la connexion. Dans le contexte des services de streaming, elles veillent par exemple à ce que les vidéos ne soient pas interrompues. Toutefois, malgré ces avantages, les adresses IP statiques coûtent généralement plus cher.

Il n'existe pas assez d'adresses IP uniques pour répondre aux besoins de tous les internautes dans le monde. Les adresses IP statiques requièrent une configuration manuelle assez complexe, tandis que les IP dynamiques sont gérées et attribuées automatiquement (ce qui est le cas de la connexion domestique que vous utilisez probablement en ce moment).

# Adressage du réseau

## ■ Plan d'adressage

Hôtes	12 hôtes	30 hôtes	120 hôtes	160 hôtes
Sous réseau(x)	1 sous réseau	5 sous réseaux	5 sous réseaux	5 sous réseaux
Adressage	10.1.0.0   10.1.0.14	10.2.0.0   10.2.0.32 10.3.0.0   10.3.0.32 10.4.0.0   10.4.0.32 10.5.0.0   10.5.0.32 10.6.0.0   10.6.0.32	10.7.0.0   10.7.0.122 10.8.0.0   10.8.0.122 10.9.0.0   10.9.0.122 10.10.0.0   10.10.0.122 10.11.0.0   10.11.0.122	10.12.0.0   10.12.0.162 10.13.0.0   10.13.0.162 10.14.0.0   10.14.0.162 10.15.0.0   10.15.0.162 10.16.0.0   10.16.0.162

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

La plage 10.0.0.0 est une option populaire pour les réseaux d'entreprise en raison de sa flexibilité et de sa compatibilité avec les meilleures pratiques en matière de gestion des adresses IP.

**Grande plage d'adresses :** La plage 10.0.0.0/8 offre une énorme plage d'adresses IP (plus de 16 millions d'adresses). Cela signifie que vous disposez d'une grande marge de manœuvre pour attribuer des adresses IP à tous les dispositifs de votre réseau, même dans le cadre d'une entreprise de grande taille.

**Gestion facile :** En utilisant une adresse de classe A privée, vous pouvez segmenter votre réseau en sous-réseaux plus petits (par exemple, 10.0.1.0/24, 10.0.2.0/24, etc.) pour organiser et gérer efficacement vos dispositifs. Cela facilite la gestion des adresses IP et la mise en place de stratégies de routage.

**Isolation du réseau :** En utilisant une plage d'adresses privées, vous isolez votre réseau local de l'Internet public, ce qui peut contribuer à renforcer la sécurité de votre réseau.

**Compatibilité avec les VPN :** De nombreuses entreprises utilisent la plage 10.0.0.0/8 pour configurer des réseaux privés virtuels (VPN) internes, car elle permet des connexions VPN sécurisées entre des sites distants tout en évitant les conflits d'adresses avec l'Internet public.

**Conformité avec les meilleures pratiques :** L'utilisation de plages d'adresses IP privées, comme 10.0.0.0/8, est conforme aux meilleures pratiques de gestion des adresses IP et réduit le risque de conflits d'adressage avec Internet.

**Simplicité de configuration :** Les adresses IP de la plage 10.0.0.0 sont faciles à configurer sur une grande variété d'équipements réseau, y compris les routeurs, les commutateurs et les serveurs DHCP.

**Évite les conflits :** En choisissant une plage d'adresses IP privées bien connue, vous réduisez les risques de conflits d'adressage avec d'autres réseaux locaux ou avec Internet public.

**Scalabilité :** La plage 10.0.0.0/8 offre suffisamment d'adresses IP pour prendre en charge la croissance future de votre réseau sans nécessiter un changement d'adresse IP.

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

La différence principale entre ces types d'adresses réside dans leur utilisation, leur portée et leur capacité à être routées sur Internet. Les **adresses IP publiques sont routables et permettent la communication sur Internet**, tandis que les **adresses IP privées, statiques, dynamiques, multicast, de bouclage, réservées et spéciales ont des rôles spécifiques dans des contextes particuliers, tels que les réseaux locaux, la gestion réseau, la diffusion, les tests et plus encore.**

Les principales adresses IP utilisés sont :

**Adresse IP publique** : Une adresse IP publique est utilisée pour identifier un dispositif sur Internet. Elle est généralement attribuée par l'organisme de réglementation Internet à un **fournisseur de services Internet (FAI)** ou à une organisation, et elle permet aux dispositifs de communiquer sur Internet. **Les adresses IP publiques sont limitées en nombre et sont uniques à l'échelle mondiale.**

**Adresse IP privée** : Une adresse IP privée est utilisée à l'intérieur d'un réseau local (LAN) et n'est pas routable sur Internet. Elle est généralement **attribuée à un dispositif par un routeur ou un serveur DHCP (Dynamic Host Configuration Protocol) à l'intérieur du réseau local**. Les adresses IP privées sont définies dans des plages spécifiques réservées pour un usage local, comme 192.168.0.0/16, 172.16.0.0/12, et 10.0.0.0/8.

**Adresse IP statique** : Une adresse IP statique est une adresse qui ne change pas et est attribuée manuellement à un dispositif. Elle est généralement utilisée pour les serveurs et les dispositifs nécessitant une adresse IP permanente.

**Adresse IP dynamique** : Une adresse IP dynamique est attribuée automatiquement à un dispositif par un serveur DHCP. Cette adresse peut changer chaque fois que le dispositif se connecte au réseau. Les adresses IP dynamiques sont couramment utilisées pour les ordinateurs de bureau et les dispositifs grand public.

**Adresse IP réservée** : Certaines adresses IP sont réservées à des utilisations spécifiques. Par exemple, l'adresse IP 127.0.0.1 est réservée pour la boucle locale (localhost), tandis que l'adresse IP 0.0.0.0 est utilisée pour signifier toutes les adresses possibles dans un contexte particulier.

**Adresse IP multicast** : Une adresse IP multicast est utilisée pour acheminer des paquets de données à un groupe de dispositifs spécifiques. Les adresses multicast permettent la diffusion de données à un ensemble de dispositifs intéressés.

**Adresse IP de bouclage (Loopback)** : L'adresse IP de bouclage (généralement 127.0.0.1) est utilisée pour tester la pile TCP/IP du dispositif lui-même. Les paquets envoyés à cette adresse ne quittent pas le dispositif et sont renvoyés immédiatement.

**Adresse IP réservée pour les adresses spéciales** : Il existe des adresses IP réservées pour des fonctions spécifiques, comme la configuration automatique d'IPv4 (169.254.0.0/16) ou l'adresse IP de passerelle par défaut (généralement utilisée pour représenter la passerelle de sortie du réseau).

JOB 12

# 7 couches du modèle OSI

Catégorie de couches	Unités de données	Couches	Matériels ou Protocoles
Couches hautes	Donnée	<b>7   Application</b> Point d'accès aux services réseau	FTP
	Donnée	<b>6   Présentation</b> Conversion et chiffrement des données	HTML
	Donnée	<b>5   Session</b> Communication Interhost	
	Segment	<b>4   Transport</b> Connexion de bout en bout et contrôle de flux (TCP)	TCP   SSL/TLS   UDP
Couches matérielles	Paquet	<b>3   Réseau</b> Détermine le parcours et l'adressage logique (IP)	PPTP   IPv4   IPv6 Routeur
	Tram	<b>2   Liaison</b> Adressage physique (MAC et LLC)	Ethernet   MAC   PPTP Wi-Fi
	Bit	<b>1   Physique</b> Transmission binaire numérique ou analogique	Fibre optique   Câble RJ45

JOB 13

# Architecture du réseau

## Calculateur de Masque IPv4 et IPv6

192.168.10.6/24	<input type="button" value="Envoyer"/>	
192.168.10.6	255.255.255.0	<input type="button" value="Envoyer"/>
<input checked="" type="radio"/> Direct <input type="radio"/> Inverse (Wildcard)		

### Adresse IPv4

CIDR : 24

Masque de réseau : 255.255.255.0

Masque inverse : 0.0.0.255

### En mode réseau :

Adresse de réseau : 192.168.10.0

Première adresse : 192.168.10.1

Dernière adresse : 192.168.10.254

Adresse de broadcast : 192.168.10.255

Nombre d'adresses IP disponibles : 254

### En mode filtre :

Première adresse : 192.168.10.0

Dernière adresse : 192.168.10.255

Nombre d'adresses IP disponibles : 256

## ■ Quelle est l'architecture de ce réseau ?

L'architecture du réseau pour les 4 PC de "L'école La Plateforme" est en MAN car les ordinateurs sont reliés entre eux sur un même lieu.

## ■ Indiquer quelle est l'adresse IP du réseau ?

L'adresse du réseau est 192.168.10.0

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

On peut brancher 254 machines sur ce réseau car il faut en réserver une pour le DHCP et une pour le Gateway .

## ■ Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion de ce réseau est 192.168.10.11111111 ou 192.168.10.255

## JOB 14

# Conversion des IP en binaire

■ Convertir les adresses IP suivantes en binaires :

- **145.32.59.24**

10010001.100000.111011.11000

- **200.42.129.16**

11001000.101010.10000001.10000

- **14.82.19.54**

1110.1010010.10011.110110

## ■ Qu'est-ce que le routage ?

Le routage réseau est le **processus de sélection d'un chemin à travers un ou plusieurs réseaux**. Les principes de routage peuvent s'appliquer à tous les types de réseaux, des réseaux téléphoniques aux transports publics. Dans les réseaux à commutation de paquets, comme Internet, le routage sélectionne les chemins que doivent emprunter les paquets IP (Internet Protocol) pour se rendre de leur origine à leur destination. Ces décisions de routage Internet sont prises par des périphériques réseau spécialisés appelés routeurs.

## ■ Qu'est-ce qu'un gateway ?

La Gateway est le **dispositif par lequel deux réseaux informatiques ou deux réseaux de télécommunication de nature différente sont reliés**. Le dispositif permet de vérifier la sécurité du réseau qui cherche à se connecter à l'autre. La Gateway est aussi appelée passerelle applicative. Le réseau que vous cherchez à connecter à un autre réseau doit respecter les conditions fixées par l'administrateur de ce nouveau réseau.

La plupart du temps, l'opération consiste à relier un réseau local à Internet. Parmi les Gateways, la plus connue est la box Internet, ou passerelle domestique. Il s'agit du boîtier qui sert de lien entre un fournisseur d'accès Internet et un abonné au haut débit. Parmi les types de passerelle, mentionnons le routeur, le répéteur et le pont.

## ■ Qu'est-ce qu'un VPN ?

Un VPN ou réseau privé virtuel crée **une connexion réseau privée entre des appareils via Internet**. Les VPN servent à transmettre des données de manière sûre et anonyme sur des réseaux publics. Ils fonctionnent en masquant les adresses IP des utilisateurs et en chiffrant les données de manière à ce qu'elles soient illisibles pour toute personne non autorisée à les recevoir.

## ■ Qu'est-ce qu'un DNS ?

Le Domain Name System (Système de nom de domaine) ou DNS est un **service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP ou d'autres types d'enregistrements**. En fournissant dès les premières années d'Internet, autour de 1985, un service distribué de résolution de noms, le DNS est un composant essentiel du développement du réseau informatique.