

# La Plateforme

## Le Réseau

### Job 2

#### Qu'est ce qu'un réseau?

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux.

#### À quoi sert un réseau informatique ?

Un réseau informatique sert à connecter un ensemble d'ordinateurs et de périphériques électroniques pour permettre la communication, le partage de ressources et l'accès à l'information.

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

**Ordinateurs et dispositifs finaux** : Ils génèrent, reçoivent et manipulent les données

**Câbles réseau** : Les câbles réseau permettent la transmission des données entre les appareils connectés au réseau.

**Routeur** : Le routeur relie différents réseaux, tels qu'un réseau local (LAN) à Internet. Il gère le trafic réseau en acheminant les données entre les différents réseaux et en attribuant des adresses IP aux dispositifs du réseau local.

**Commutateur (Switch)** : Les commutateurs sont utilisés pour relier plusieurs appareils au sein d'un même réseau local (LAN). Ils fonctionnent au niveau de la couche de liaison de données pour diriger le trafic uniquement vers les appareils qui en ont besoin, améliorant ainsi l'efficacité du réseau.

**Modem** : Le modem est utilisé pour établir la connexion à Internet via un fournisseur de services Internet (FAI).

**Point d'accès sans fil (Access Point, AP)** : Les points d'accès sans fil permettent aux dispositifs sans fil tels que les ordinateurs portables, les smartphones et les tablettes de se connecter au réseau local via Wi-Fi.

**Serveur** : Un serveur peut fournir divers services au réseau, tels que le stockage de fichiers, la gestion des utilisateurs, la messagerie électronique, les applications web, etc. Il est conçu pour être accessible en permanence.

**Firewall** : Le pare-feu est un dispositif ou un logiciel qui sécurise le réseau en filtrant le trafic entrant et sortant. Il protège le réseau contre les menaces et les accès non autorisés.

**Périphériques de stockage en réseau (NAS)** : Les NAS sont utilisés pour le stockage de fichiers partagés sur le réseau. Ils permettent le stockage centralisé et la sauvegarde des données.

**Coffrets et armoires de câblage** : Ils abritent les composants matériels du réseau, tels que les commutateurs, les routeurs, les serveurs, les panneaux de brassage, et organisent les câbles pour une installation propre et bien gérée.

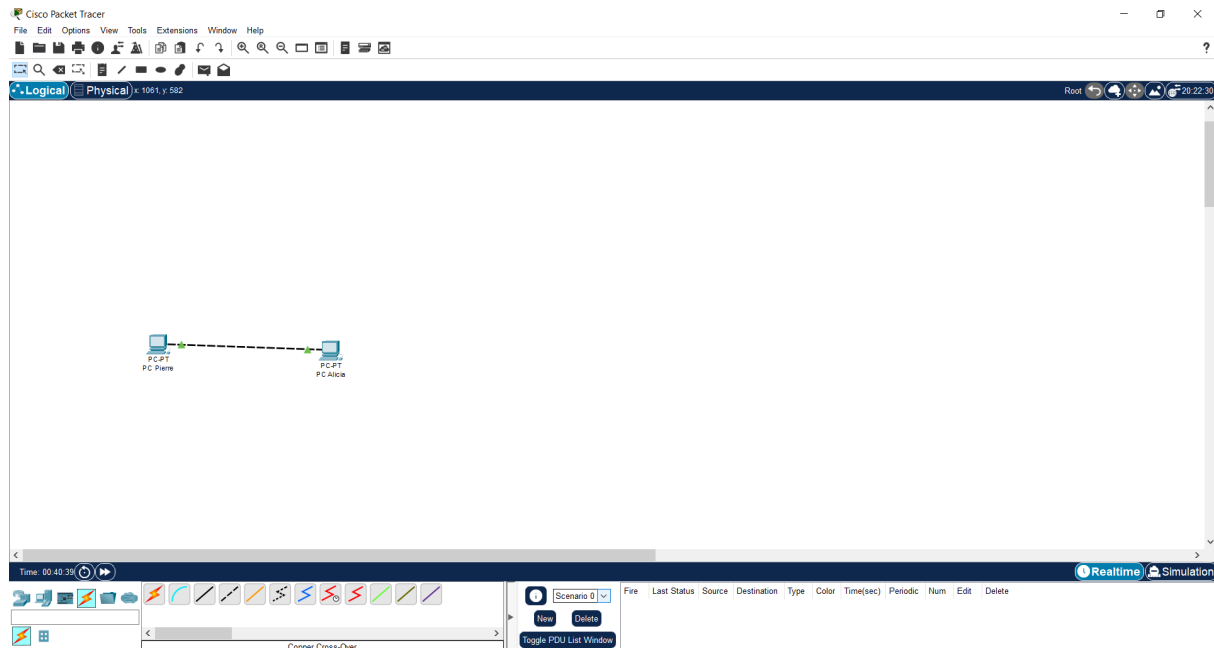
**Panneaux de brassage** : Les panneaux de brassage sont utilisés pour connecter les câbles réseau dans les coffrets de câblage.

**Câblage structuré** : Il s'agit de l'infrastructure physique qui connecte tous les composants du réseau.



## Job 3

Un "copper crossover cable" (câble de croisement en cuivre) est simplement un câble Ethernet torsadé croisé qui est fabriqué en utilisant des conducteurs en cuivre. Ce type de câble est utilisé pour relier directement deux dispositifs similaires, tels que deux ordinateurs, deux commutateurs (switches), ou deux routeurs, sans nécessiter un équipement intermédiaire, comme un commutateur ou un routeur.



## Job 4

**Qu'est-ce qu'une adresse IP ?**

Une adresse IP (Internet Protocol) est un identifiant unique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet pour communiquer.

**À quoi sert un IP ?**

Les adresses IP sont la base de la communication et de la connectivité sur les réseaux informatiques, qu'il s'agisse de réseaux locaux (LAN), de réseaux étendus (WAN) ou d'Internet. Elles permettent l'identification, la communication, le routage des données, la gestion des ressources et la sécurité sur les réseaux.

## Qu'est-ce qu'une adresse MAC ?

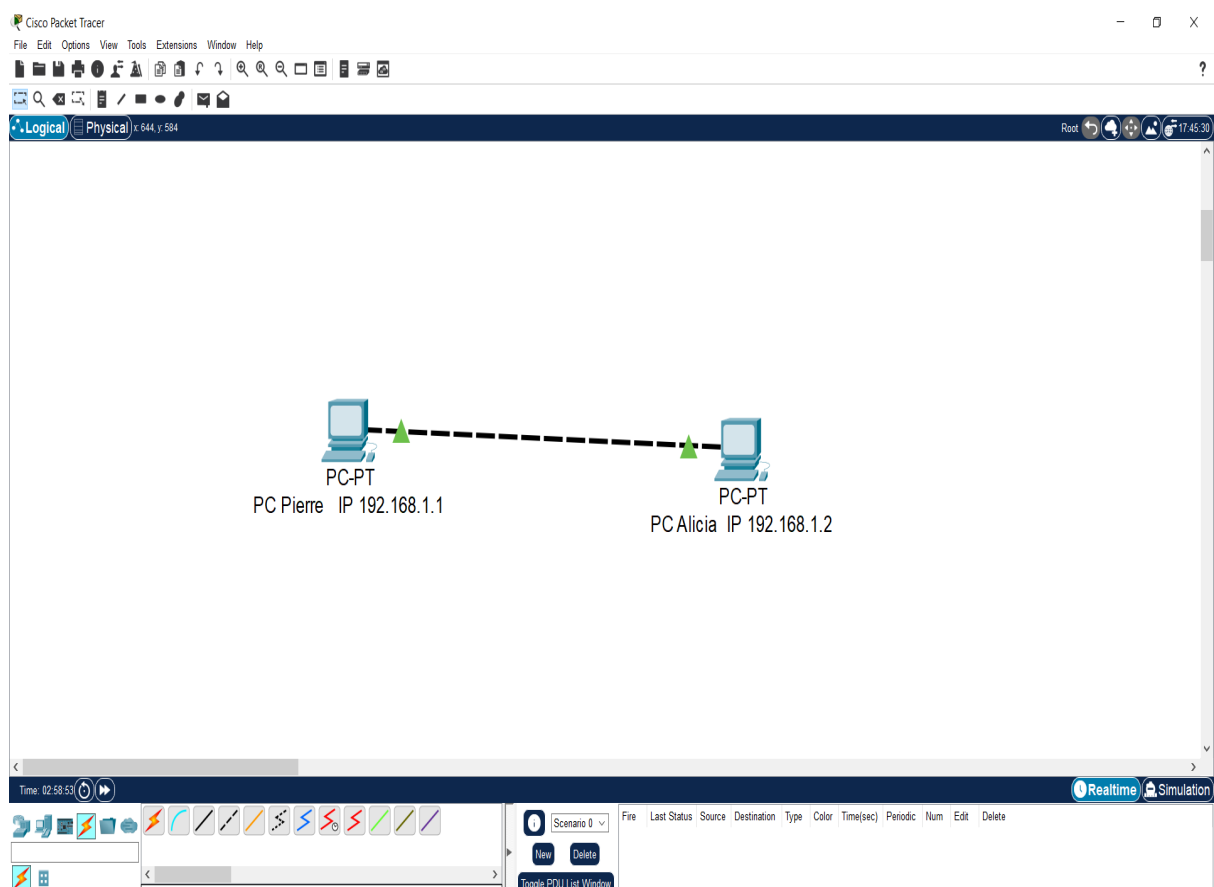
Une adresse MAC (Media Access Control), également connue sous le nom d'adresse physique, est un identifiant unique attribué à chaque carte réseau, adaptateur réseau ou périphérique réseau connecté à un réseau local (LAN) ou à un réseau étendu (WAN). Les adresses MAC sont des identifiants physiques et uniques gravés dans le matériel de chaque carte réseau.

## Adresse IP Publique :

Une adresse IP publique est une adresse unique attribuée à un dispositif ou à un réseau qui est directement accessible sur Internet. Elle permet d'identifier un dispositif de manière globale et unique sur Internet.

## Adresse IP Privée :

Une adresse IP privée est une adresse IP attribuée à un dispositif dans un réseau local (LAN) ou une organisation privée. Elle est conçue pour être utilisée à l'intérieur d'un réseau local et n'est pas directement routable sur Internet.



PC Pierre IP 192.168.1.1

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

Port Status

Bandwidth

Duplex

MAC Address: 00E0.B03B.4193

IP Configuration

☐ DHCP

☒ Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address:

Link Local Address: FE80::2E0:B0FF:FE3B:4193

100 Mbps 10 Mbps On

Half Duplex Full Duplex Auto

Top

## Réseau PC Pierre

PC Alicia

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

FastEthernet0

Bluetooth

Port Status

Bandwidth

Duplex

MAC Address: 0001.4241.5CA3

IP Configuration

☐ DHCP

☒ Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

IPv6 Configuration

☐ Automatic

☒ Static

IPv6 Address:

Link Local Address: FE80::201:42FF:FE41:5CA3

100 Mbps 10 Mbps On

Half Duplex Full Duplex Auto

## Réseau PC Alicia

## Job 5

PC Pierre IP 192.168.1.1

Physical Config **Desktop** Programming Attributes

Command Prompt

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

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 00E0.B03B.4193
    Link-local IPv6 Address.....: FE80::2E0:B0FF:FE3B:4193
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
    0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-8A-22-25-7A-00-E0-B0-3B-41-93
    DNS Servers.....: ::
    0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 00E0.F721.19E6
    Link-local IPv6 Address.....: ::
--More--
```

### PC Pierre

PC Alicia IP 192.168.1.2

Physical Config **Desktop** Programming Attributes

Command Prompt

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

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0001.4241.5CA3
    Link-local IPv6 Address.....: FE80::201:42FF:FE41:5CA3
    IPv6 Address.....: ::
    IPv4 Address.....: 192.168.1.2
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: ::
    0.0.0.0
    DHCP Servers.....: 0.0.0.0
    DHCPv6 IAID.....:
    DHCPv6 Client DUID.....: 00-01-00-01-2C-BA-28-16-00-01-42-41-5C-A3
    DNS Servers.....: ::
    0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Physical Address.....: 0002.4A8A.5AD0
    Link-local IPv6 Address.....: ::
--More--
```

### PC Alicia

La ligne de commande pour vérifier l'id des machines est : `ipconfig /all`

## Job 6

La ligne de commande pour faire un ping est: ping IP par exemple ping 192.168.1.1

```
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=14ms 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=3ms 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 = 14ms, Average = 4ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

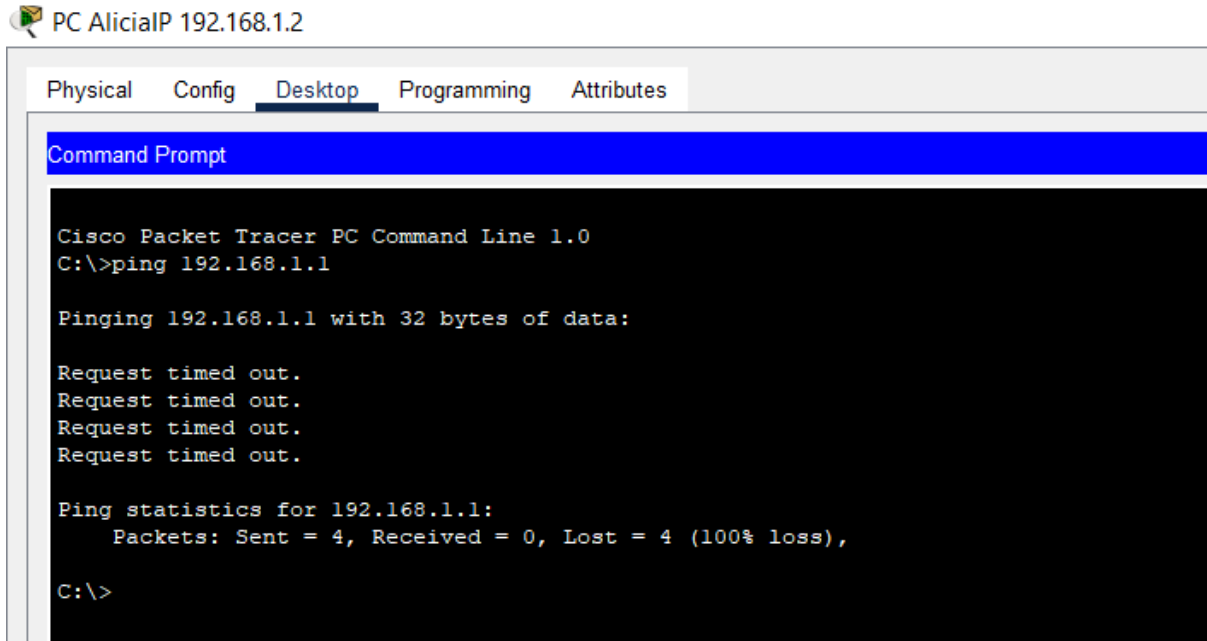
Reply from 192.168.1.1: bytes=32 time=9ms TTL=128
Reply from 192.168.1.1: bytes=32 time=27ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=23ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 27ms, Average = 15ms

C:\>rm
```

## Job 7

Si on éteint le PC de pierre et utilisé le terminal du pc de Alicia pour ping le pc de pierre on a le résultat suivant :



```
PC Alicia IP 192.168.1.2

Physical  Config  Desktop  Programming  Attributes

Command Prompt

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),

C:\>
```

**Le PC de Pierre a-t-il reçu les paquets envoyés par Alicia ? NON**

**Expliquez pourquoi.**

Si l'ordinateur de Pierre est éteint, il ne pourra pas recevoir les paquets envoyés par l'ordinateur d'Alicia. Le ping est une commande réseau qui envoie des paquets ICMP (Internet Control Message Protocol) d'un ordinateur à un autre pour vérifier la connectivité et mesurer le temps de réponse. Si l'ordinateur de Pierre est éteint, il ne sera pas en mesure de répondre aux paquets. Pour que l'ordinateur de Pierre puisse recevoir les paquets, il doit être allumé et connecté au réseau.

## Job 8

**Un hub et un switch** sont deux types de dispositifs utilisés pour connecter des appareils au sein d'un réseau local (LAN). Cependant, ils fonctionnent de manière très différente et ont des performances et des fonctionnalités distinctes.

La principale différence réside dans la manière dont ces dispositifs gèrent le trafic. Un hub est simple et répète le signal à tous les ports, tandis qu'un switch est plus avancé, examine les adresses MAC et transmet le trafic de manière sélective pour optimiser les performances et minimiser les collisions.



**Un hub,** est un dispositif matériel qui agit comme un concentrateur pour connecter plusieurs périphériques sur un réseau local (LAN)

Un hub reçoit les données de tous les périphériques connectés et les transmet à tous les autres périphériques. Il agit comme un amplificateur passif, répétant les signaux entrant à tous les ports. le hub ne prend pas de décision pour déterminer à quel port spécifique les données doivent être transmises. Il se contente de répéter les données à tous les ports.

**avantages :** Les hubs sont généralement moins chers que les commutateurs, ce qui les rend accessibles pour les petits réseaux. Ils sont simples à installer et à configurer, ce qui en fait un choix approprié pour les utilisateurs peu expérimentés en matière de réseaux.

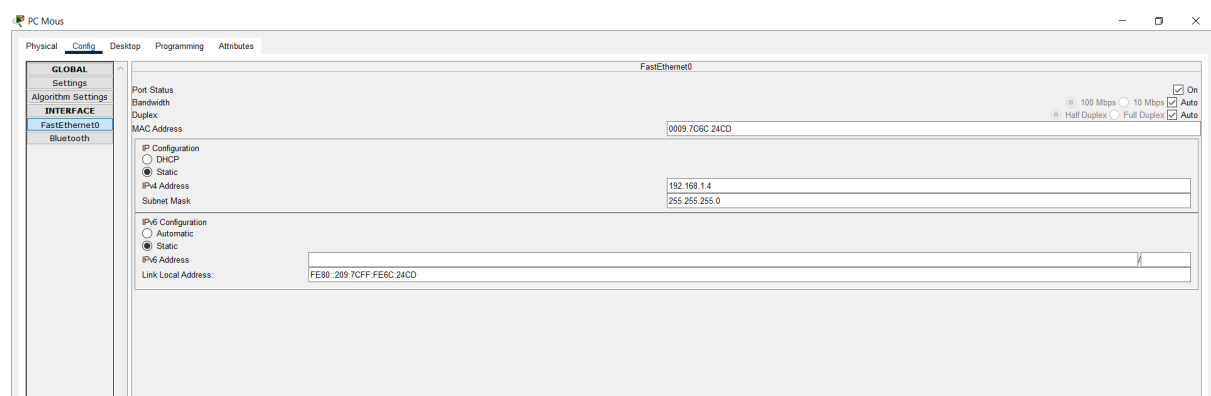
**Inconvénients:** L'un des principaux inconvénients est la diffusion de données à tous les ports. Cela signifie que toutes les données sont reçues par tous les périphériques connectés, même si elles ne sont pas destinées à un périphérique particulier.

**Dans les réseaux Ethernet traditionnels (non commutés), les hubs augmentent le risque de collisions de données,** car tous les périphériques partagent le même espace de communication. Les collisions réduisent les performances du réseau.

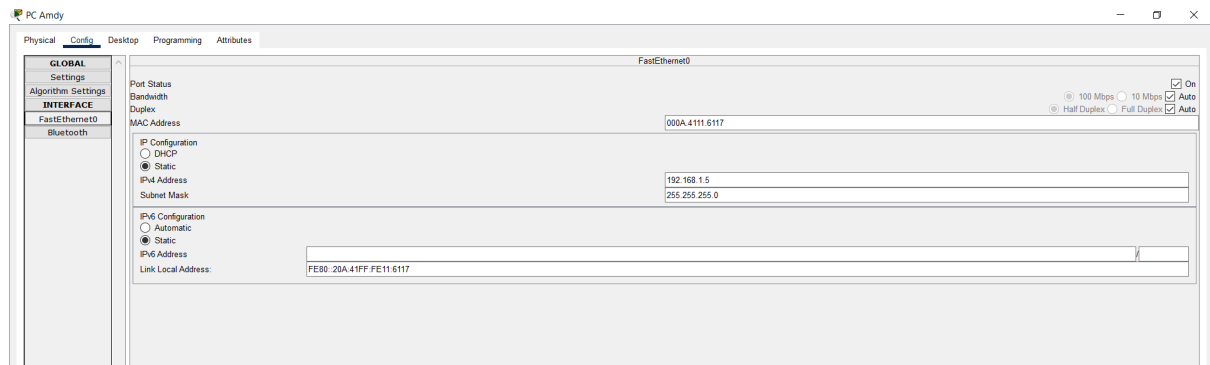
**La bande passante disponible** est partagée entre tous les périphériques connectés au hub. Si de nombreux périphériques sont actifs simultanément, cela peut entraîner des ralentissements et des goulots d'étranglement.

**Quels sont les avantages et inconvénients d'une switch ?**

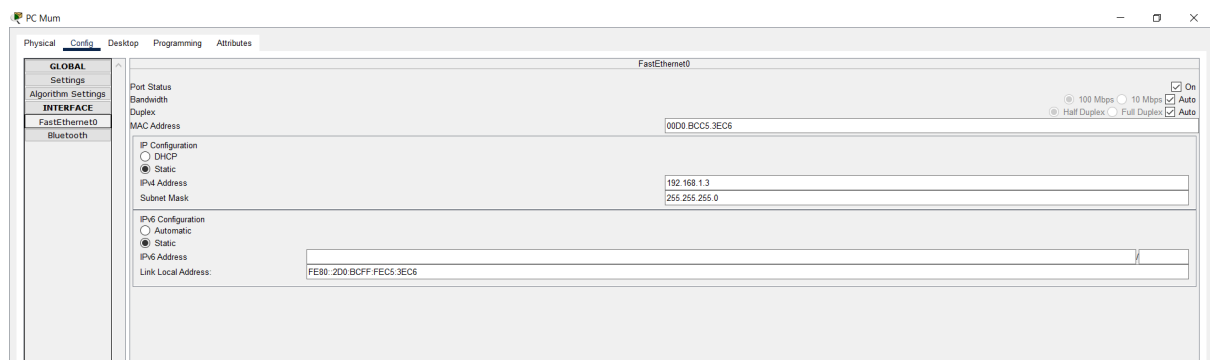
Les commutateurs offrent une performance et une efficacité supérieures par rapport aux hubs, mais ils peuvent être plus coûteux, nécessiter une configuration plus complexe, et avoir des points de défaillance potentiels. Cependant, pour la plupart des réseaux modernes, les avantages des commutateurs en matière de performance, de sécurité et de gestion du trafic l'emportent largement sur leurs inconvénients.



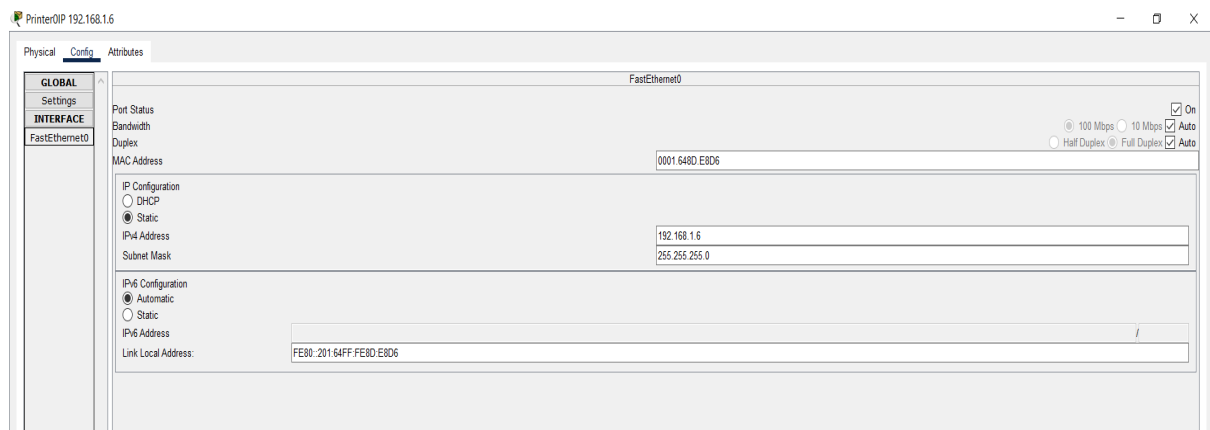
réseau pc Mous



réseau PC Andy



réseau PC Mum



printer

Si j'effectue un PING en utilisant le terminal prompt pour vérifier que les 5 PC soient tous bien connectés, j'obtiens les résultats suivants:

```
PC Alicia IP 192.168.1.2

Physical Config Desktop Programming Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.5

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=14ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 3ms

C:\>ping 192.168.1.4

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

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

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

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

## Job 9

Réalisez un schéma de votre réseau

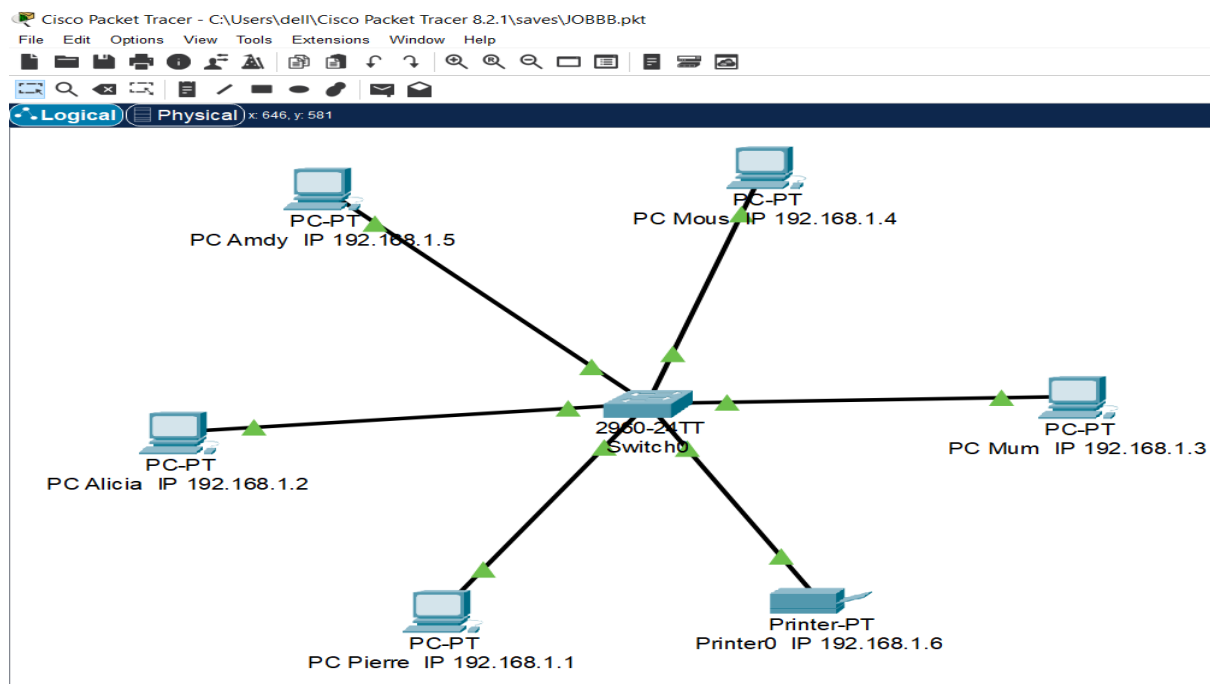


Schéma de réseau

Créer un schéma de réseau est une pratique courante dans l'administration et la gestion des réseaux, car il offre de nombreux avantages en termes de documentation, de maintenance et de sécurité.

**Un schéma de réseau sert de documentation visuelle du réseau**, ce qui facilite la compréhension de la structure et de la configuration du réseau pour les administrateurs et les techniciens.

**En cas de problème réseau**, un schéma de réseau bien documenté peut être un outil précieux pour diagnostiquer et résoudre les problèmes plus rapidement.

**Un schéma de réseau peut** aider à planifier l'expansion du réseau en identifiant les emplacements disponibles pour de nouveaux composants, les besoins en câblage, etc.

**Un schéma de réseau peut** servir de support visuel pour la communication au sein de l'équipe informatique et avec d'autres parties prenantes, facilitant ainsi la prise de décisions.

## Job 10

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

**Adresse IP Statique** est Fixe et manuellement configurer; Une adresse IP statique est attribuée manuellement à un périphérique par un administrateur réseau. L'administrateur configure l'adresse IP, le masque de sous-réseau, la passerelle par défaut et d'autres paramètres réseau directement sur le périphérique. Une fois configurée, une adresse IP statique reste la même tant que l'administrateur ne la modifie pas manuellement. Elle ne change pas automatiquement.

L'administrateur a un contrôle total sur la configuration des adresses IP statiques.

**Adresse IP attribuée par DHCP est attribuée automatiquement** : Une adresse IP attribuée par DHCP est allouée automatiquement par un serveur DHCP au moment où un périphérique se connecte au réseau. Le périphérique envoie une demande au serveur DHCP, qui attribue une adresse IP disponible.

Les adresses IP attribuées par DHCP sont temporaires et ont une durée de bail définie. Après expiration du bail, le périphérique doit renouveler son bail DHCP pour continuer à utiliser la même adresse IP

Le serveur DHCP gère la distribution des adresses IP, ainsi que d'autres paramètres réseau tels que la passerelle par défaut et les serveurs DNS. Cela simplifie la gestion des adresses IP sur un réseau avec de nombreux périphériques.

La principale différence réside dans la manière dont les adresses IP sont attribuées et gérées. Les adresses IP statiques sont configurées manuellement et restent constantes, tandis que les adresses IP attribuées par DHCP sont allouées automatiquement avec une certaine flexibilité et sont temporaires.

## **Job 11**

**Définissez le plan d'adressage.**

???

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

l'adresse 10.0.0.0 a été choisie comme point de départ pour créer des sous-réseaux en raison de sa nature de classe A, ce qui offre une grande flexibilité pour diviser l'espace d'adressage en sous-réseaux de différentes tailles tout en conservant un grand nombre d'adresses IP disponibles. Cette approche permet d'optimiser l'utilisation des adresses IP et de répondre aux besoins spécifiques de l'organisation tout en évitant le gaspillage d'adresses IP précieuses.

## Job 12

Créez un tableau dans lequel se trouvent les sept couches du modèle OSI, avec chaque couche une description des rôles.

COUCHES	RÔLES
1. Couche physique	Cette couche gère la transmission de données brutes sur un support physique, tel que des signaux électriques, optiques ou radiofréquences. Elle définit les spécifications matérielles, telles que les câbles, les connecteurs et les protocoles de transmission.
2. Couche liaison de données	La couche liaison de données est responsable de la communication entre des dispositifs directement connectés. Elle gère la détection et la correction d'erreurs, ainsi que le contrôle d'accès au support. Elle divise les données en trames (frames) et s'assure de leur transmission fiable.
3. Couche réseau	La couche réseau gère la transmission de données entre différents réseaux. Elle est responsable du routage des paquets de données, du maintien des tables de routage, et de la détermination du meilleur chemin pour les données à travers un réseau.
4.Couche transport	Cette couche gère la communication de bout en bout entre les applications. Elle assure un transfert de données fiable en découpant les données en segments, en gérant la séquence, le contrôle de flux et la retransmission en cas de perte de données.
5. Couche session	La couche session établit, gère et termine les sessions de communication entre les applications sur différentes machines. Elle gère également la synchronisation et la gestion des points de contrôle lors de la communication.
6. Couche présentation	La couche présentation s'occupe de la traduction, de la compression et du chiffrement des données pour assurer la compatibilité entre les systèmes hétérogènes. Elle garantit que les données sont présentées de manière cohérente pour les applications.
7. Couche application	La couche application est la couche la plus proche de l'utilisateur final. Elle gère la communication entre les applications et les services réseau. Cette couche comprend des protocoles tels que HTTP, FTP, SMTP et DNS, qui permettent aux applications de communiquer sur le réseau.

**Associez les différents matériels ou protocoles ci-dessous aux couches :**

<b>7. Couche application</b>	<b>HTML, FTP, PPTP, SSL/TLS</b>
<b>6. Couche présentation</b>	<b>SSL/TLS, HTML</b>
<b>5. Couche session</b>	<b>SSL/TLS, PPTP, FTP</b>
<b>4. Couche transport</b>	<b>TCP, UDP</b>
<b>3. Couche réseau</b>	<b>IPv4, IPv6, routeur</b>
<b>2. Couche liaison de données</b>	<b>Ethernet, MAC, câble RJ45, Wi-Fi</b>
<b>1. Couche physique</b>	<b>Fibre optique, câble RJ45</b>

### **Job 13**

**Quelle est l'architecture de ce réseau ?**

Tous les périphériques, y compris les PC (PC0, PC1, PC2, PC3) et les serveurs (Serveur 1, Serveur 2), font partie du même réseau, car ils partagent la même plage d'adresses IP (192.168.10.x) et le même masque de sous-réseau (255.255.255.0). Cela signifie que ces périphériques peuvent communiquer directement les uns avec les autres sans avoir besoin de routage, car ils sont tous dans le même sous-réseau local (LAN).

**Indiquer quelle est l'adresse IP du réseau ?**

L'adresse IP du réseau est : 192.168.10.0. en prenant les trois premiers octets de l'adresse IP de l'un des appareils de ce réseau.

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

Avec un masque de sous-réseau de 255.255.255.0; cela signifie qu'il y a 8 bits disponibles pour les adresses IP des machines dans ce réseau. Le nombre de machines que l'on peut brancher sur ce réseau est déterminé par  $2^{(\text{nombre de bits disponibles})} - 2$ , car l'adresse IP de réseau (tout à zéro) et l'adresse de diffusion (tout à un) sont réservées et ne peuvent pas être attribuées aux machines.

Dans ce cas, avec 8 bits disponibles, le nombre de machines possibles est  $2^8 - 2 = 256 - 2 = 254$ .

**Quelle est l'adresse de diffusion de ce réseau ?**

L'adresse de diffusion est calculée en prenant l'adresse réseau et en effectuant une opération OR (bitwise OR) avec l'inverse du masque de sous-réseau.

Adresse réseau : 192.168.10.0

Masque de sous-réseau : 255.255.255.0

Masque inverse : 0.0.0.255

J'effectue l'opération OR entre l'adresse réseau et le masque inverse :

$192.168.10.0 \text{ OR } 0.0.0.255 = 192.168.10.255$

Donc, l'adresse de diffusion pour ce réseau est 192.168.10.255

## **Job 14**

**Convertissez les adresses IP suivantes en binaires :**

Pour convertir l'adresse IP en binaire, vous devez convertir chaque partie de l'adresse IP (décimale) en sa représentation binaire. Chaque partie de l'adresse IP est un octet, composé de 8 bits. Voici la conversion en binaire :

145.32.59.24 en binaire = 10010001.00100000.00111011.00011000

200.42.129.16 en binaire = 11001000.00101010.10000001.00010000

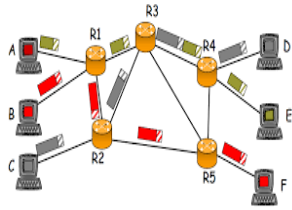
14.82.19.54 en binaire = 00001110.01010010.00010011.00110110

## **Job 15**

**Répondez attentivement aux questions suivantes :**

**Le routage** est le processus de transmission de données d'un réseau à un autre à travers un ensemble de dispositifs appelés routeurs. Le routage permet de diriger le trafic réseau de manière efficace en déterminant le chemin optimal pour que les données atteignent leur destination. C'est un élément fondamental des réseaux informatiques, en particulier sur Internet.





**Un gateway** (passerelle en français) est un dispositif matériel ou logiciel qui interconnecte deux réseaux informatiques ayant des protocoles différents, afin de permettre la communication et l'échange de données entre eux.

**Un VPN**, ou Réseau Privé Virtuel (Virtual Private Network en anglais), est un service qui permet de créer une connexion sécurisée et cryptée entre deux réseaux ou entre un utilisateur individuel et un réseau. Il est utilisé pour protéger la confidentialité et la sécurité des données lorsqu'elles sont transmises sur des réseaux publics, comme Internet.



**Les DNS** sont un élément fondamental de l'infrastructure d'Internet. Ils facilitent la navigation en traduisant les noms de domaine conviviaux en adresses IP numériques, permettant ainsi aux utilisateurs d'accéder aux sites web et aux services en ligne sans avoir à se souvenir des adresses IP.

