

RUNTRACK

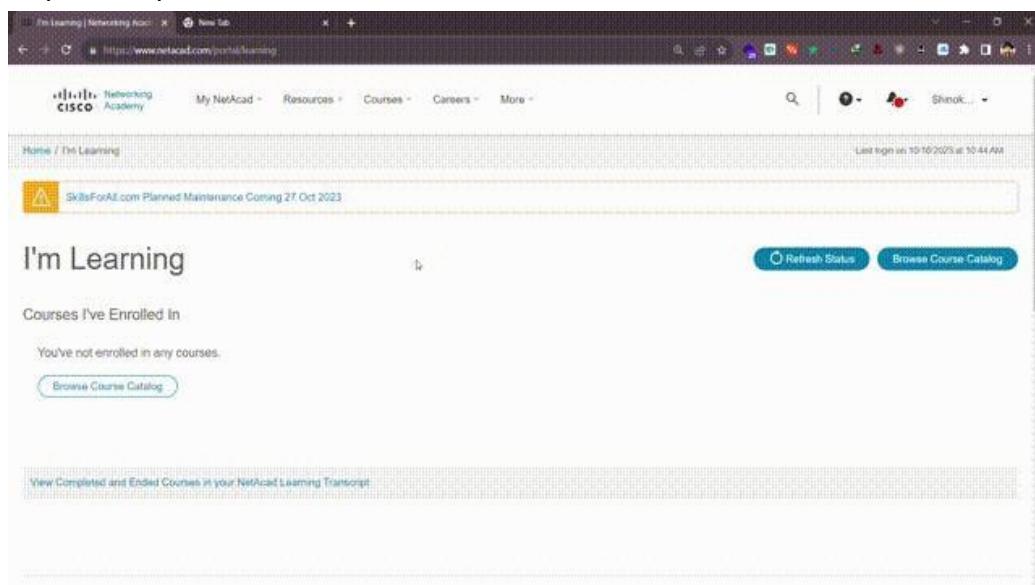
JOB 1 : Installer Packet Tracer

Etape 1 : On va se rendre sur le portail Netcad [ici](#)

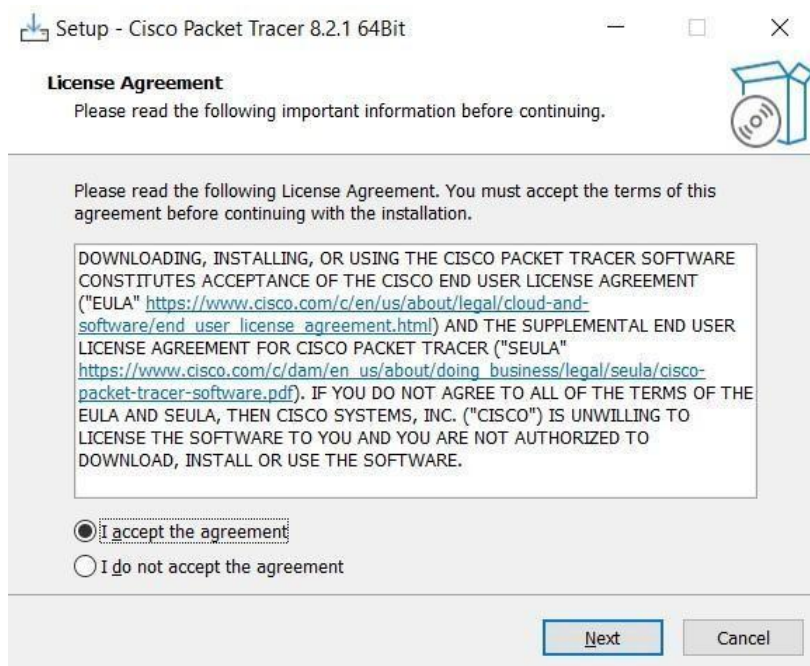
Ensuite on va nous demander de se connecter si on a un compte, sinon on s'inscrit.

The diagram illustrates the user flow on the Cisco Netcad portal. On the left, the 'Se connecter' (Login) page is shown with a 'S'inscrire' (Sign Up) link at the bottom. A red arrow points from this link to the 'Créer un compte' (Create Account) page on the right. The registration page includes fields for E-mail, Mot de passe (Password), Prénom (First Name), Nom (Last Name), and Pays ou région (Country or Region), along with a 'S'inscrire' button.

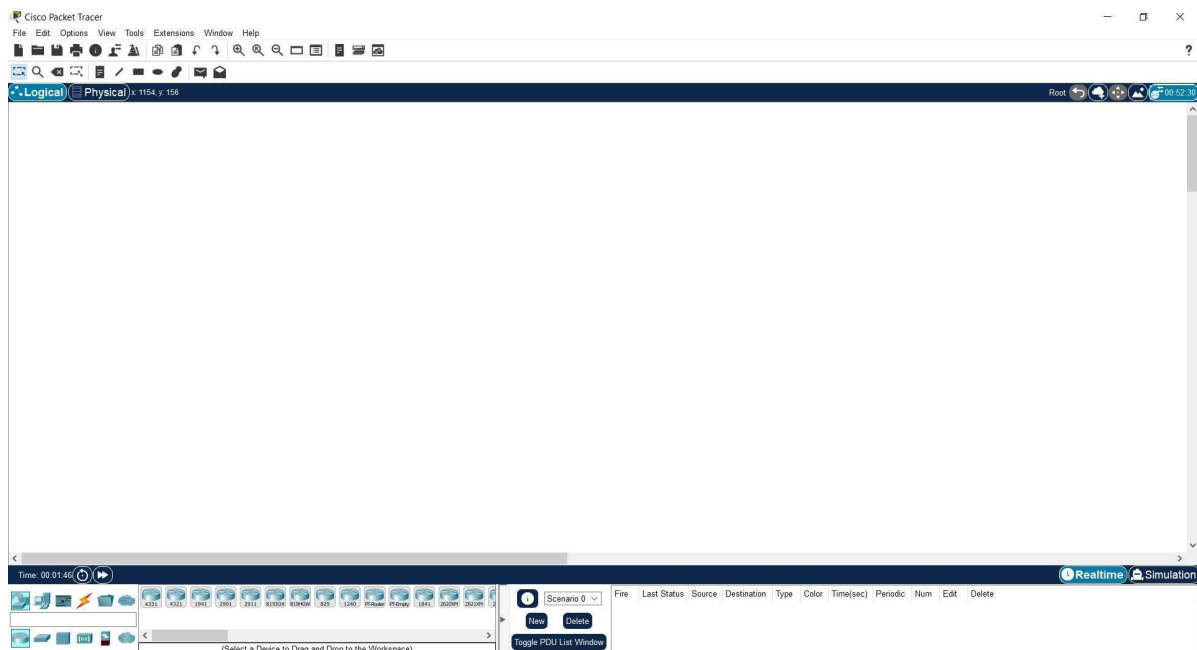
Après t'être inscrit tu arrivera sur cette page, pour telecharger Packet Tracer on suivra les étapes indiquées ci dessous



Execution du programme d'installation



Lancement de Cisco Packet Tracer



JOB 2 : Réponses au questions

Qu'est-ce qu'un réseau ?

=> Un réseau informatique, c'est un ensemble d'ordinateurs et de périphériques reliés entre eux qui permet de transporter de l'information d'un point à un autre pour :

- Partager des équipements ;
- Partager et échanger des informations et des fichiers ;
- Accéder à des services.

À quoi sert un réseau informatique ?

=> La fonction principale d'un réseau consiste à offrir aux participants une plateforme permettant l'échange de données et l'utilisation partagée des ressources. Cette mission revêt une importance cruciale, à tel point qu'imaginer notre quotidien et le monde professionnel actuel sans l'existence des réseaux serait difficile.

Illustrons cela avec un exemple concret : au sein d'un bureau, chaque poste de travail est équipé de son propre ordinateur. En l'absence de mise en réseau des ordinateurs, la collaboration au sein d'une équipe sur un projet deviendrait complexe. Il n'y aurait pas d'espace commun pour partager et déposer des documents et informations numériques, et les collaborateurs ne pourraient pas utiliser certains programmes de manière collaborative comme ils en ont l'habitude.

De plus, dans de nombreux bureaux, il n'y a qu'une ou quelques imprimantes destinées à l'usage de tous. Sans réseau, il serait nécessaire de connecter chaque ordinateur directement à l'imprimante, une tâche fastidieuse. Un réseau résout astucieusement ce problème en reliant tous les ordinateurs à l'imprimante via un nœud central.

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

Serveur : Un ordinateur dédié chargé d'organiser l'intégralité du réseau, gérant l'accès aux ressources, aux périphériques et les connexions des utilisateurs. L'accès au serveur nécessite une identification à l'aide d'un identifiant et d'un mot de passe.



Poste-client : Un ordinateur connecté au réseau par le biais d'une carte réseau, qu'elle soit filaire ou sans fil. Ce poste-client peut utiliser les ressources informatiques partagées sur le réseau.



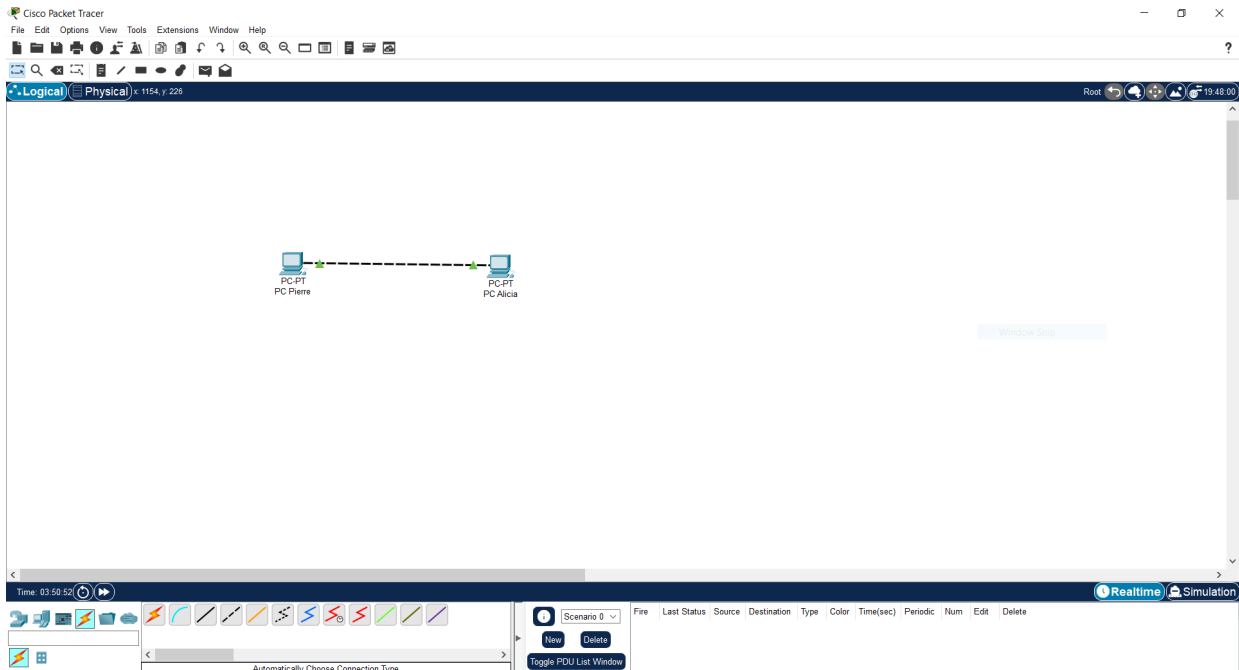
Commutateur ou Switch : Un dispositif permettant aux équipements du réseau de communiquer entre eux en facilitant le transfert des données.



Routeur/Modem : Un dispositif permettant la communication avec d'autres réseaux en acheminant des paquets d'informations découpées à travers les lignes téléphoniques.



JOB 3 : Création de notre premier réseau

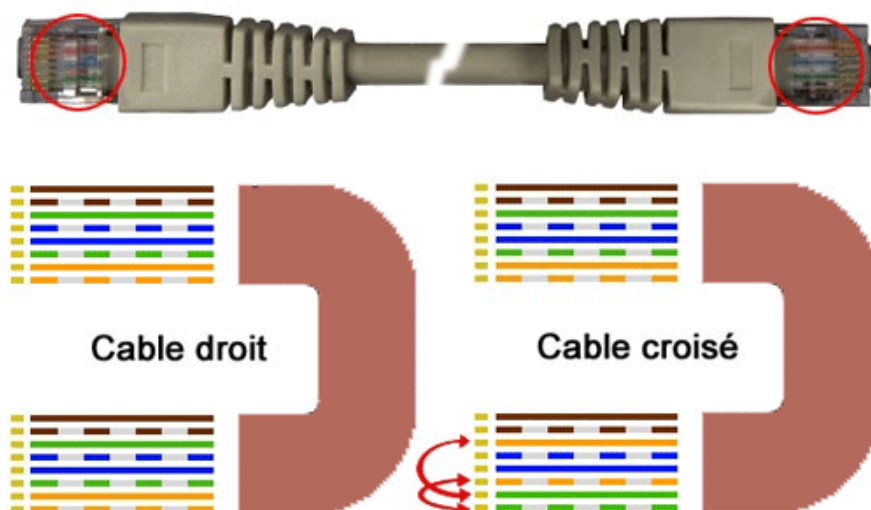


Quels câbles avez-vous choisis pour relier les deux ordinateurs ?

=> J'ai employé un **câble croisé** pour connecter les deux ordinateurs. Ce type de câble est spécialement conçu pour établir une liaison directe entre deux ordinateurs, facilitant ainsi l'échange bidirectionnel de données.

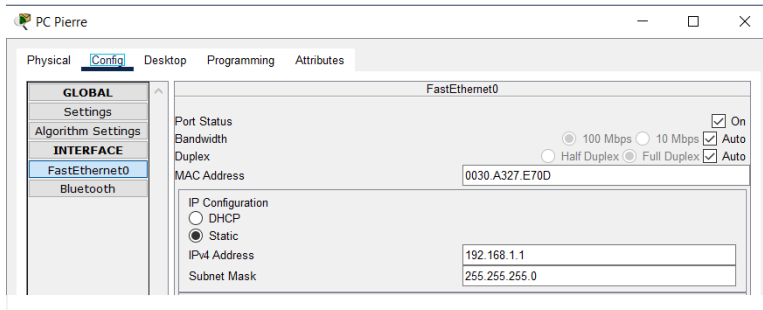
En croisant les fils du câble, on assure que la sortie de données d'un ordinateur correspond à l'entrée de données de l'autre, et réciproquement. Cette configuration permet une communication directe et bidirectionnelle efficace entre les deux ordinateurs.

Le **câble croisé** est utilisé pour relier deux ordinateurs entre eux ou pour connecter un ordinateur directement à un autre périphérique réseau, tandis que le **câble droit** est utilisé pour connecter un ordinateur à un équipement réseau.

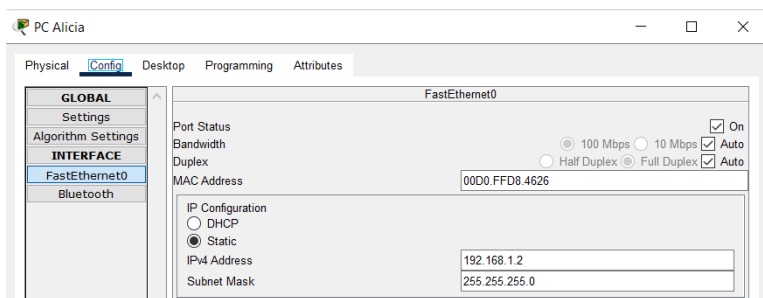


JOB 4 : Configuration de nos deux ordinateurs

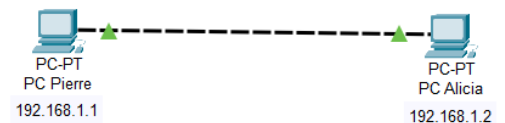
Adressage IP et masque de sous-réseau des deux ordinateurs (PC Pierre et PC Alicia)



PC Pierre



PC Alicia



Qu'est-ce qu'une adresse IP ?

=> Une adresse IP constitue une référence numérique assignée à un ordinateur qui est connecté à un réseau Internet.

En pratique, cette étiquette joue le rôle d'une carte d'identité en permettant l'identification des machines et en facilitant leur communication mutuelle par l'échange de données sur Internet.

Chaque ordinateur est pourvu d'une adresse IP, qui peut être **statique** (si l'ordinateur reste constamment allumé) ou **dynamique** (si l'ordinateur est régulièrement redémarré).

À quoi sert un IP ?

=> Les adresses IP assurent la **liaison** entre **vous** et les **sites web** que vous consultez, les e-mails que vous ouvrez, et les vidéos que vous visionnez.

Ces actions en ligne, regroupées sous le terme de "**demandes de données**", dépendent de l'utilisation d'une adresse IP. En **l'absence** d'une adresse IP, votre ordinateur et votre service Internet seraient **incapables de fonctionner**.

Qu'est-ce qu'une adresse MAC ?

=> L'adresse MAC (pour **Media Access Control**) est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est sensée être **unique** au monde. On peut donc considérer qu'elle constitue une sorte de plaque d'immatriculation des appareils électroniques.

À la différence de l'adresse IP qui peut changer si vous vous connectez à internet depuis un autre endroit, l'adresse MAC **reste constante** et permet d'identifier spécifiquement chaque périphérique réseau, surtout au sein d'un réseau local.

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

=> Une adresse IP publique est attribuée à un routeur ou à un serveur directement accessible depuis Internet.

Elle est utilisée pour identifier un réseau ou un dispositif sur l'internet mondial.

Les serveurs web, les routeurs principaux et d'autres dispositifs directement connectés à Internet ont des adresses IP publiques.

Ces adresses sont uniques dans le monde entier et sont routables sur Internet.

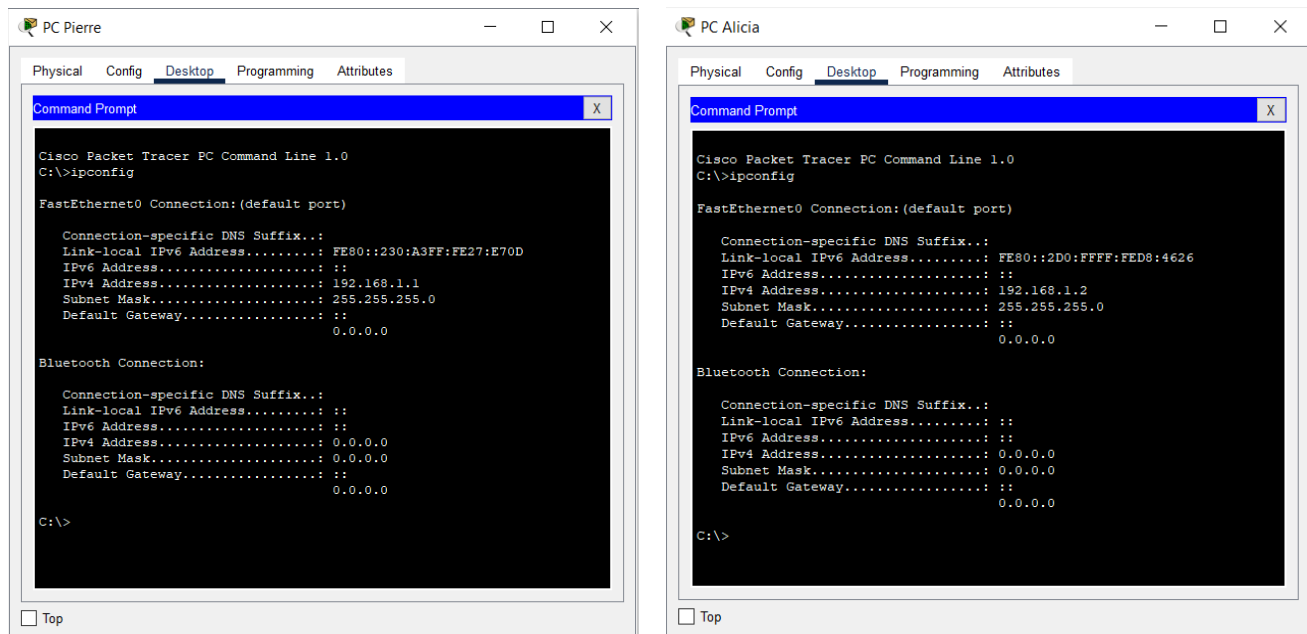
Une adresse IP privée est utilisée à l'intérieur d'un réseau local pour identifier les dispositifs connectés localement.

Ces adresses ne sont pas routables sur Internet et sont destinées à être utilisées en interne au sein d'un réseau privé.

Quelle est l'adresse de ce réseau ?

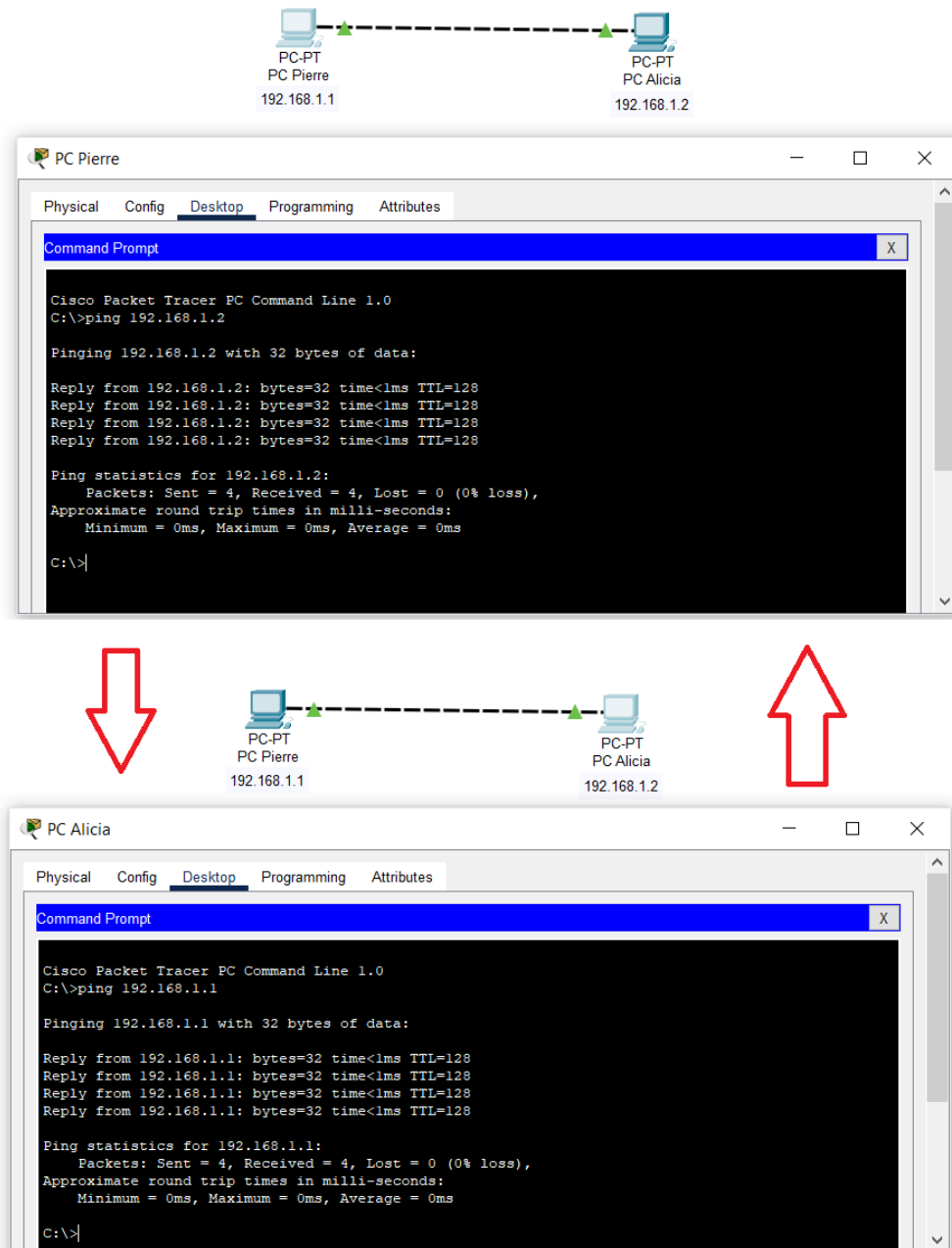
=> L'adresse du réseau est : 192.168.1.0

JOB 5 : Vérifier l'IP des deux ordinateurs à l'aide du Terminal



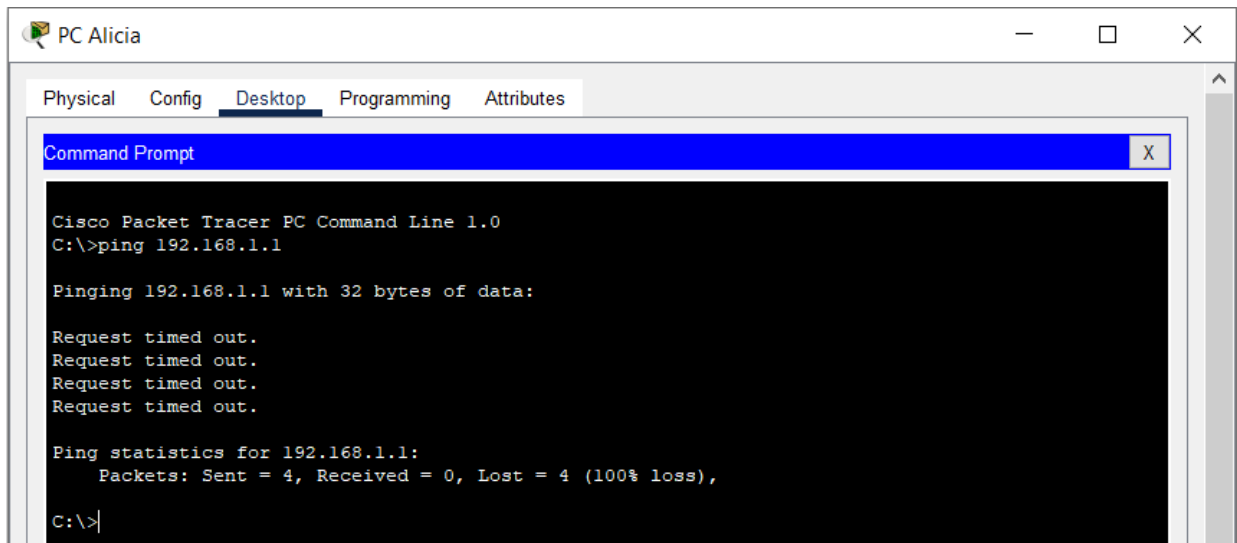
Pour vérifier l'IP de chaque PC, j'ai utilisé ici la commande **ipconfig**

JOB 6 : Tester la connectivité des deux ordinateurs en utilisant la commande PING



Pour vérifier la connectivité des deux ordinateurs, j'ai utilisé la commande ping suivit de l'IP de l'ordinateur distant ex : **ping 192.168.1.1**

JOB 7 : Effectuer un ping depuis le PC d'Alicia vers celui de Pierre, sachant que ce dernier est éteint.



Lors du ping vers le **PC Pierre (192.168.1.1)** avec des paquets de 32 octets de données, les **quatre tentatives** n'ont pas abouti.

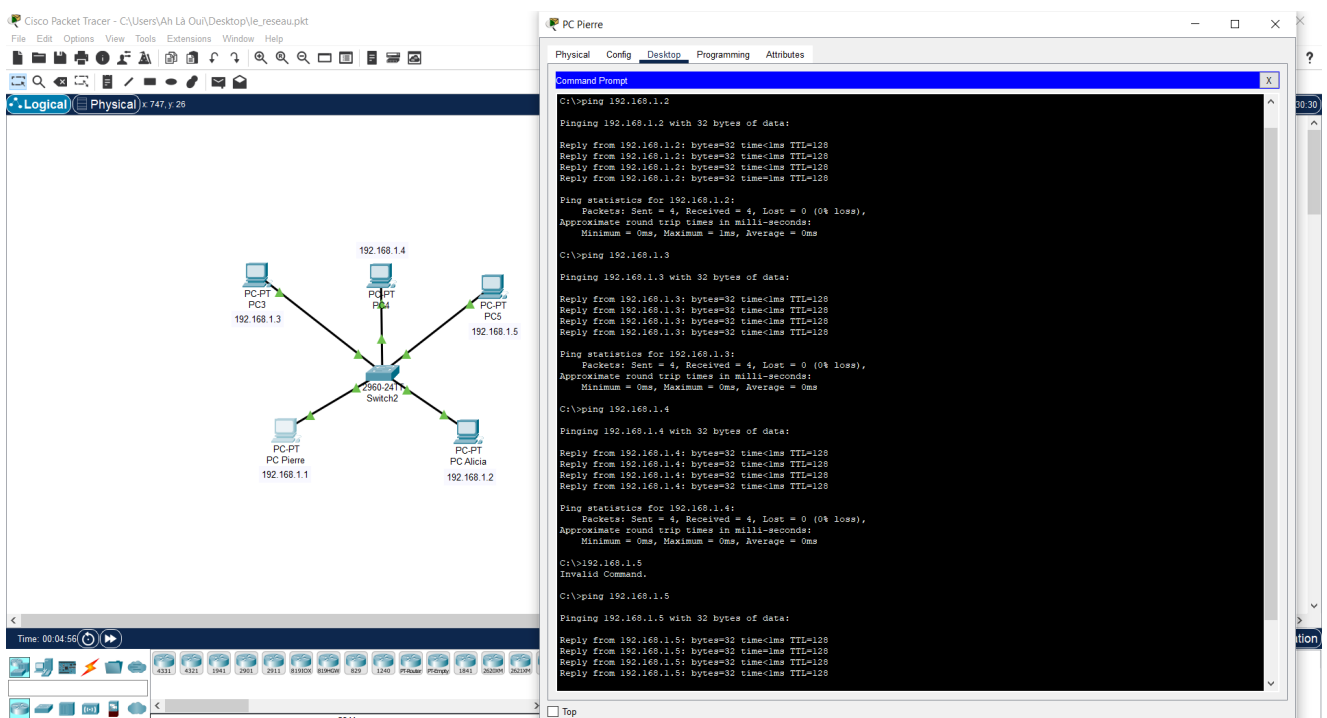
Chaque demande a expiré, ce qui est indiqué par le message **"Request timed out"** (demande expirée).

Les statistiques du ping révèlent que sur les 4 paquets envoyés, **aucun n'a été reçu** avec une perte totale de **100%**.

Cela indique que l'ordinateur à l'adresse IP **192.168.1.1** n'a pas répondu aux demandes de ping.

Les raisons possibles peuvent inclure une **défaillance matérielle**, un **problème de réseau** ou simplement le fait que l'ordinateur cible **était éteint** ou **indisponible** au moment du test.

JOB 8 : Agrandir le sous réseau avec cinq ordinateurs et les configurer sur le même réseau



Quelle est la différence entre un hub et un switch ?

=> La différence entre le **hub** et le **switch** est la façon dont les trames sont livrées.

Avec **un hub**, une trame est transférée ou « transmise » à tous les ports. Peu importe que la trame soit destinée à un seul port. Le hub n'a **aucun moyen de distinguer vers quel port une trame doit être envoyée**. Transmettre ces trames à chaque port garantit qu'il atteindra sa destination. Cela génère **beaucoup de charge** sur le réseau et peut conduire à des temps de réponse plus longs.

En comparaison, **un commutateur (switch)** conserve un registre des adresses MAC (Media Access Control) de tous les appareils qui y sont connectés. Grâce à ces informations, **un commutateur réseau peut identifier quel appareil se trouve sur chaque port**. Ainsi, lorsqu'une trame est reçue, celui-ci **sait exactement à quel port l'envoyer**, sans augmenter les temps de réponse du réseau.

Ainsi, quel que soit la quantité de terminaux transmettant des données, les utilisateurs auront toujours accès **à la plus grande largeur** de bande possible.

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

=> **Un hub** fonctionne au niveau physique (**couche 1**) du **modèle OSI**. Lorsqu'il reçoit des données d'un appareil, il les transmet à tous les autres ports, indépendamment du destinataire. En d'autres termes, **il utilise la diffusion (broadcast)** pour envoyer des données à tous les périphériques connectés.

Avantages d'un Hub :

Coût : Les hubs sont généralement moins chers que les switches.

Facilité d'utilisation : Ils sont simples à mettre en œuvre et ne nécessitent généralement pas de configuration complexe.

Inconvénients d'un Hub :

Collisions : En raison de la diffusion, les collisions peuvent survenir, surtout dans des réseaux plus importants, ce qui peut entraîner une diminution des performances.

Bande passante partagée : La bande passante disponible est partagée entre tous les périphériques, ce qui peut entraîner une congestion dans les réseaux plus chargés.

Manque de séparation : Les données sont transmises à tous les ports, compromettant la sécurité et la confidentialité des données.

Quels sont les avantages et inconvénients d'un switch ?

Avantages d'un Switch :

Efficacité : Les switches fonctionnent au niveau de la couche de liaison de données (**couche 2**), ce qui leur permet de transmettre sélectivement des données uniquement aux périphériques destinataires, améliorant ainsi l'efficacité du réseau.

Performances : Ils offrent généralement de meilleures performances que les hubs, en particulier dans les réseaux de taille moyenne à grande.

Moins de collisions : En raison de la commutation, les collisions sont réduites, ce qui améliore la qualité du réseau.

Bande passante dédiée : Chaque port a sa propre bande passante dédiée, évitant ainsi les problèmes de congestion.

Inconvénients d'un Switch :

Coût : Les switches sont généralement plus coûteux que les hubs.

Complexité : Ils peuvent nécessiter une configuration plus avancée, bien que de nombreux switches modernes soient plug-and-play.

Gestion des VLANs : La configuration des VLANs (Virtual Local Area Networks) peut être complexe pour les utilisateurs non avertis.

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

=> Un switch gère le trafic réseau en utilisant la **commutation (switching)**. Lorsqu'il reçoit des données d'un périphérique, il examine l'adresse MAC de destination dans le paquet.

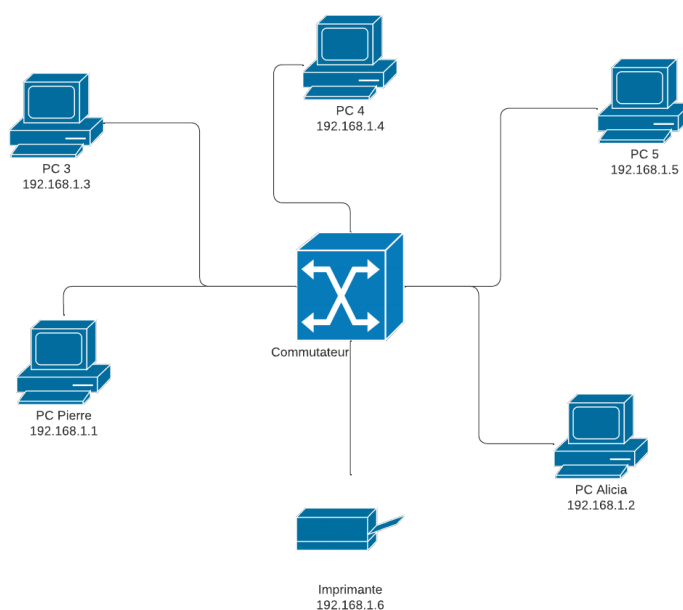
En fonction de cette adresse, le switch détermine le port auquel le périphérique de destination est connecté. Il transmet ensuite sélectivement les données uniquement à ce port, évitant ainsi la diffusion à tous les ports comme c'est le cas avec les hubs.

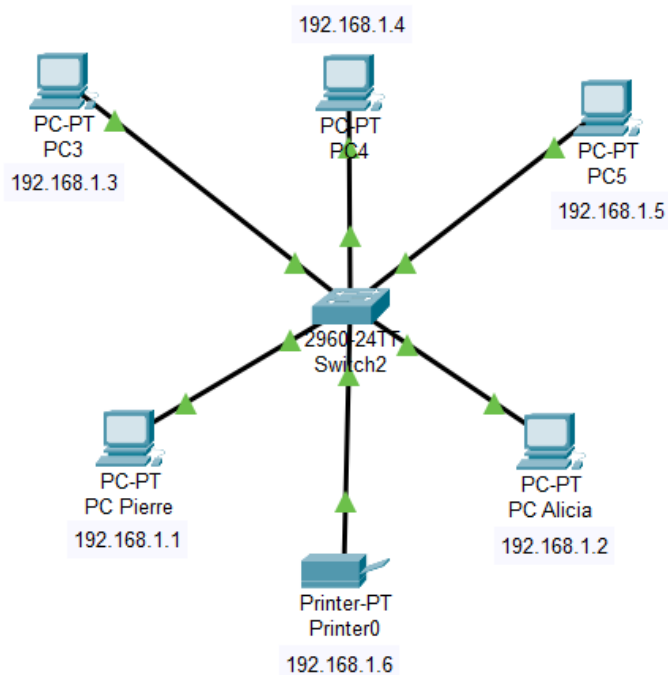
Cette approche permet aux switches d'optimiser l'utilisation de la bande passante, de minimiser les collisions et d'améliorer les performances globales du réseau.

JOB 9 : Ajout d'une imprimante, vérifier qu'elle soit connecter et schématiser le réseau

JOB 9 - SCHEMA DE NOTRE RESEAU

SAID ALI TSARAVELONA ALLAOUI | October 17, 2023





L'élaboration d'un schéma réseau offre plusieurs avantages, notamment :

Clarté visuelle : Un schéma réseau fournit une représentation visuelle de la structure du réseau, ce qui rend plus facile la compréhension de sa complexité. Il permet aux administrateurs réseau, aux ingénieurs et aux techniciens de visualiser l'architecture dans son ensemble.

Ils peuvent également rendre compréhensibles des informations abstraites ou non perceptibles (des idées, des théories, des concepts) en permettant leur visualisation, et donc leur analyse.

Dépannage plus efficace : En cas de problèmes réseau, un schéma clair peut accélérer le processus de dépannage. Les administrateurs peuvent identifier rapidement les composants, les connexions et les points faibles potentiels, ce qui facilite la localisation des problèmes.

Planification et conception : Lors de la planification d'un réseau ou de l'ajout de nouveaux composants, un schéma peut servir de guide visuel. Cela permet de concevoir des modifications de manière plus précise et d'anticiper les besoins futurs.

Documentation : Le schéma réseau sert de documentation précieuse pour le réseau. Il peut inclure des informations telles que les adresses IP, les noms d'hôtes, les adresses MAC, les équipements réseau, etc. Cette documentation facilite la gestion du réseau au fil du temps.

Communication facilitée : Un schéma réseau fournit un moyen clair de communiquer la structure du réseau aux membres de l'équipe, aux parties prenantes et aux intervenants externes. Cela peut être particulièrement utile dans les équipes techniques où plusieurs personnes travaillent sur le même réseau.

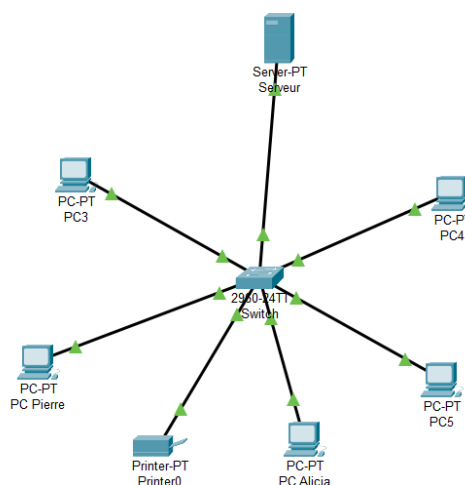
Sécurité : En identifiant clairement les points d'accès, les pare-feu, les zones de sécurité et les autres éléments liés à la sécurité, un schéma réseau contribue à renforcer la posture de sécurité globale du réseau.

Optimisation des performances : En comprenant visuellement la topologie du réseau, les administrateurs peuvent optimiser la disposition des périphériques pour améliorer les performances et la redondance.

Évolutivité : Un schéma réseau peut aider à anticiper les besoins futurs et à concevoir des architectures réseau évolutives. Cela est particulièrement important pour les entreprises en croissance ou pour les projets qui nécessitent une extension progressive du réseau.

En résumé, avoir un schéma réseau informatique offre des avantages significatifs en termes de compréhension, de planification, de dépannage et de documentation, contribuant ainsi à la gestion efficace et à la sécurité des réseaux informatiques.

JOB 10 : Mise en place d'un serveur DHCP



CONFIG DE NOTRE SERVEUR DHCP

Serveur

Physical Config Services **Desktop** Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Définition du passerelle par défaut, sauvegarde et démarrage du service !

Serveur

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: 192.168.1.0

DNS Server: 0.0.0.0

Start IP Address: 192 168 1 1

Subnet Mask: 255 255 255 0

Maximum Number of Users: 255

TFTP Server: 0.0.0.0

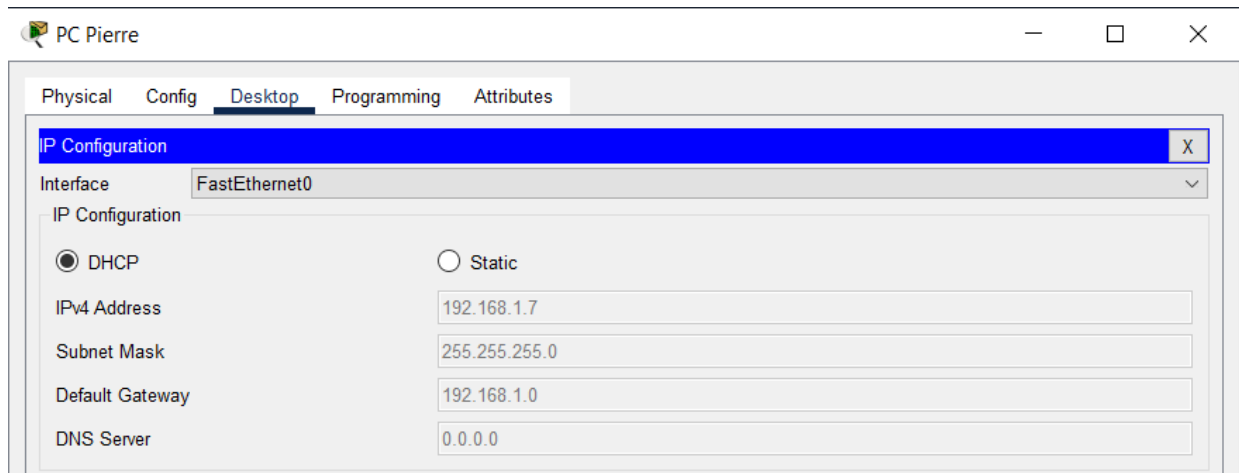
WLC Address: 0.0.0.0

Add Save Remove

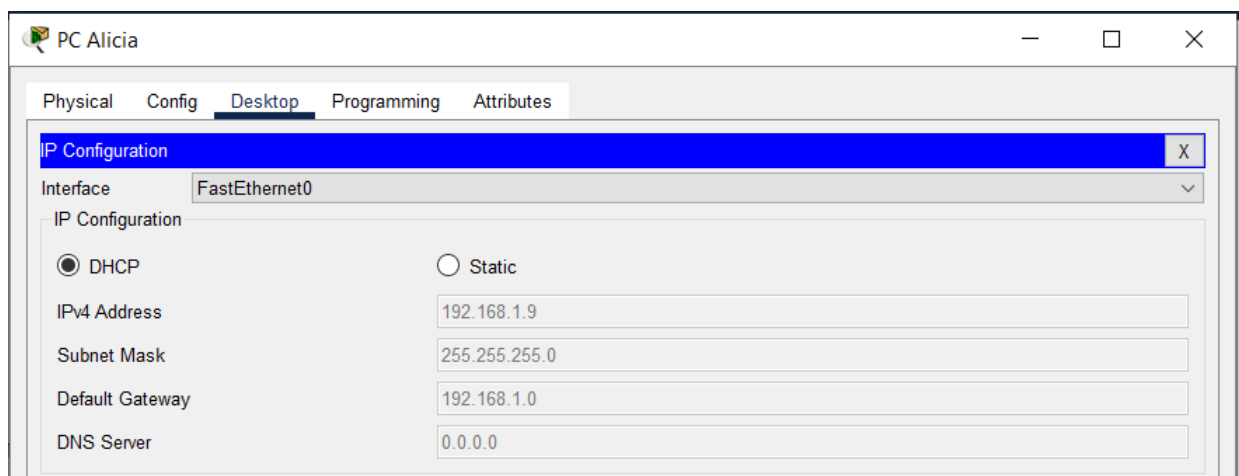
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	192.168.1.0	0.0.0.0	192.168.1.1	255.255.2...	255	0.0.0.0	0.0.0.0

VÉRIFIONS SI L'ASSIGNATION AUTO DES IP FONCTIONNE !

SCREENSHOT PC PIERRE EN DHCP



SCREENSHOT PC ALICIA EN DHCP



CA MARCHE !

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

Adresse IP statique :

Configurée manuellement.

Permanente.

Souvent utilisée pour les serveurs et les périphériques nécessitant une stabilité d'adresse.

Adresse IP attribuée par DHCP :

Attribution automatique par un serveur DHCP.

Dynamique, peut changer.

Pratique pour la gestion automatique des adresses IP dans des réseaux dynamiques.

JOB 11 : L'adressage Réseau

On a une adresse réseau de classe A 10.0.0.0.

On nous demande de créer 16 sous-réseaux et doit prendre en charge :

- 1 sous-réseau de 12 hôtes
- 5 sous-réseaux de 30 hôtes
- 5 sous-réseaux de 120 hôtes
- 5 sous-réseaux de 160 hôtes

Sous-réseau	Adresse réseau	CIDR	Plage d'adresses utilisables	Nbres de Host	Broadcast	Masque de sous-réseau
1	10.0.0.0	/28	10.0.0.1 - 10.0.0.14	14	10.0.0.15	255.255.255.246
2	10.1.0.0	/29	10.1.0.1 - 10.1.0.30	30	10.1.0.31	255.255.255.224
3	10.2.0.0	/29	10.2.0.1 - 10.2.0.30	30	10.2.0.31	
4	10.3.0.0	/29	10.3.0.1 - 10.3.0.30	30	10.3.0.31	
5	10.4.0.0	/29	10.4.0.1 - 10.4.0.30	30	10.4.0.31	
6	10.5.0.0	/29	10.5.0.1 - 10.5.0.30	30	10.5.0.31	
7	10.6.0.0	/25	10.6.0.1 - 10.6.0.126	126	10.6.0.127	255.255.255.128
8	10.7.0.0	/25	10.7.0.1 - 10.7.0.126	126	10.7.0.127	
9	10.8.0.0	/25	10.8.0.1 - 10.8.0.126	126	10.8.0.127	
10	10.9.0.0	/25	10.9.0.1 - 10.9.0.126	126	10.9.0.127	
11	10.10.0.0	/25	10.10.0.1 - 10.10.0.126	126	10.10.0.127	
12	10.11.0.0	/24	10.11.0.1 - 10.11.0.254	254	10.11.0.255	255.255.255.0
13	10.12.0.0	/24	10.12.0.1 - 10.12.0.254	254	10.12.0.255	
14	10.13.0.0	/24	10.13.0.1 - 10.13.0.254	254	10.13.0.255	
15	10.14.0.0	/24	10.14.0.1 - 10.14.0.254	254	10.14.0.255	
16	10.15.0.0	/24	10.15.0.1 - 10.15.0.254	254	10.15.0.255	

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

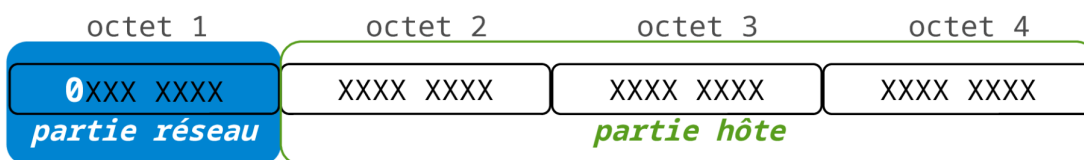
Les adresses de classe A ont un octet dédié au réseau, ce qui signifie qu'elles permettent un grand nombre de sous-réseaux avec un grand nombre d'hôtes par sous-réseau.

Dans notre cas, on a utilisé une adresse de classe A car elle offre une grande plage d'adresses pour répondre aux besoins de sous-réseaux et d'hôtes.

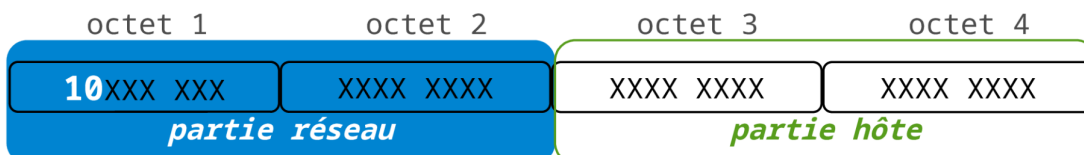
Quelle est la différence entre les différents types d'adresses ?

- Les adresses IP sont divisées en classes (A, B, C, D) en fonction du premier octet.
- Classe A : Premier octet est le réseau, trois octets sont pour les hôtes.
- Classe B : Deux premiers octets sont le réseau, deux octets sont pour les hôtes.
- Classe C : Trois premiers octets sont le réseau, un octet est pour les hôtes.
- Classe D : Utilisée pour le multicast.

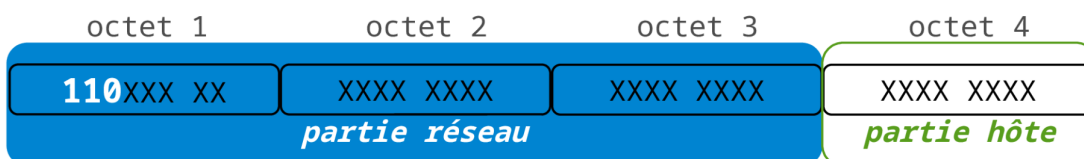
Classe A



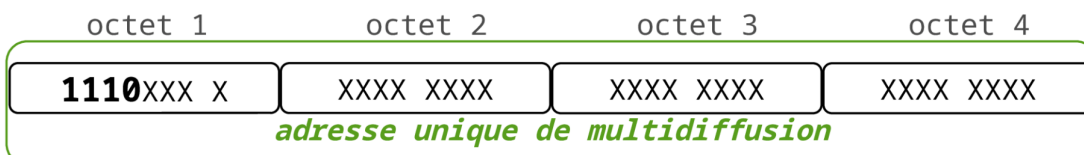
Classe B



Classe C



Classe D



JOB 12 : Créez un tableau des sept couches du OSI, et décrire le rôle de chaque couche.

Couche OSI	Fonctions et Description	Matériels/Protocoles
7 - Application	Fournit des interfaces pour les applications réseau, offre des services de communication réseau aux applications.	FTP, HTML, SSL/TLS, PPTP
6 - Présentation	Gère la syntaxe et la sémantique de l'information échangée entre les applications. Assure la traduction, la compression et le chiffrement des données.	SSL/TLS, HTML
5 - Session	Établit, maintient et termine les sessions entre les applications. Gère la synchronisation et la récupération des données.	PPTP
4 - Transport	Gère la communication de bout en bout. Fournit le contrôle de flux, la correction d'erreur, et la segmentation/reconstruction des données.	TCP, UDP
3 - Réseau	Gère le routage des données à travers le réseau. Assure la connectivité logique entre les hôtes sur différents réseaux.	IPv4, IPv6, routeur
2 - Liaison de données	Gère l'accès au support physique, détecte et corrige les erreurs liées à la transmission de données brutes.	Ethernet, MAC, Wi-Fi, câble RJ45
1 - Physique	Transmet des bits sur un support physique. Gère la topologie, la tension, la synchronisation, etc.	Fibre optique, câble RJ45, Wi-Fi

JOB 13 : Réponses au questions

Quelle est l'architecture de ce réseau ?

Il s'agit d'un réseau local de type LAN avec des adresses IP de classe C (192.168.x.x) et un masque de sous-réseau de 255.255.255.0.

Indiquer quelle est l'adresse IP du réseau ?

=> L'adresse IP du réseau est 192.168.10.0

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

=> La plage d'adresses utilisables pour les machines est de 192.168.10.1 à 192.168.10.254, permettant jusqu'à 254 appareils.

Quelle est l'adresse de diffusion de ce réseau ?

=> L'adresse de diffusion est 192.168.10.255

JOB 14 : Convertir les adresses ip en binaire

145.32.59.24 :

-	128	64	32	16	8	4	2	1
145	1	0	0	1	0	0	0	1
32	0	0	1	0	0	0	0	0
59	0	0	1	1	1	0	1	1
24	0	0	0	1	1	0	0	0

145 = 10010001 | 32 = 00100000 | 59 = 00111011 | 24 = 00011000

Donc l'IP 145.32.59.24 en binaire est : 10010001.00100000.00111011.00011000

200.42.129.16 :

-	128	64	32	16	8	4	2	1
200	1	1	0	0	1	0	0	0
42	0	0	1	0	1	0	1	0
129	1	0	0	0	0	0	0	1
16	0	0	0	1	0	0	0	0

200 = 11001000 | 42 = 00101010 | 129 = 10000001 | 16 = 00010000

Donc l'IP 200.42.129.16 en binaire est : 11001000.00101010.10000001.00010000

14.82.19.54 :

-	128	64	32	16	8	4	2	1
14	0	0	0	0	1	1	1	0
82	0	1	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
54	0	0	1	1	0	1	1	0

14 = 00001110 | 82 = 01010010 | 19 = 00010011 | 54 = 00110110

Donc l'IP 14.82.19.54 en binaire est : 00001110.01010010.00010011.00110110

JOB 15 : Répondre aux questions

Qu'est-ce que le routage ?

Le routage est le processus de transmission de données d'un point à un autre à travers un réseau. Dans le contexte des réseaux informatiques, le routage implique le choix du chemin optimal pour acheminer des paquets de données d'un point de départ à une destination.

Les routeurs sont des dispositifs clés dans ce processus, car ils prennent des décisions basées sur des informations telles que les adresses IP, les tables de routage et les protocoles de routage.

Qu'est-ce qu'un gateway ?

Une passerelle est un dispositif ou un logiciel qui connecte deux réseaux distincts, permettant ainsi la communication entre eux. Les passerelles sont utilisées pour connecter des réseaux hétérogènes qui utilisent des protocoles différents.

Par exemple, un routeur peut faire office de passerelle entre un réseau local (LAN) utilisant le protocole Ethernet et un réseau étendu (WAN) utilisant le protocole Internet (IP)

Qu'est-ce qu'un VPN ?

Un VPN, ou réseau privé virtuel, est une technologie qui permet de créer une connexion sécurisée et chiffrée sur un réseau public, comme Internet. Les VPN sont souvent utilisés pour garantir la confidentialité des communications en ligne, en cryptant les données entre l'utilisateur et le serveur VPN.

Cela est particulièrement utile lorsque l'on accède à Internet à partir de réseaux publics, car cela protège contre la surveillance et le vol de données.

Qu'est-ce qu'un DNS ?

Le DNS est un système utilisé pour traduire les noms de domaine conviviaux pour l'homme (comme www.google.com) en adresses IP numériques (142.251.37.238) que les ordinateurs utilisent pour identifier les serveurs sur Internet.

En d'autres termes, le DNS permet de faire correspondre des noms de domaine à des adresses IP. Lorsque vous saisissez une URL dans votre navigateur, le système DNS est utilisé pour résoudre ce nom en une adresse IP, permettant ainsi d'établir une connexion avec le serveur web associé.