

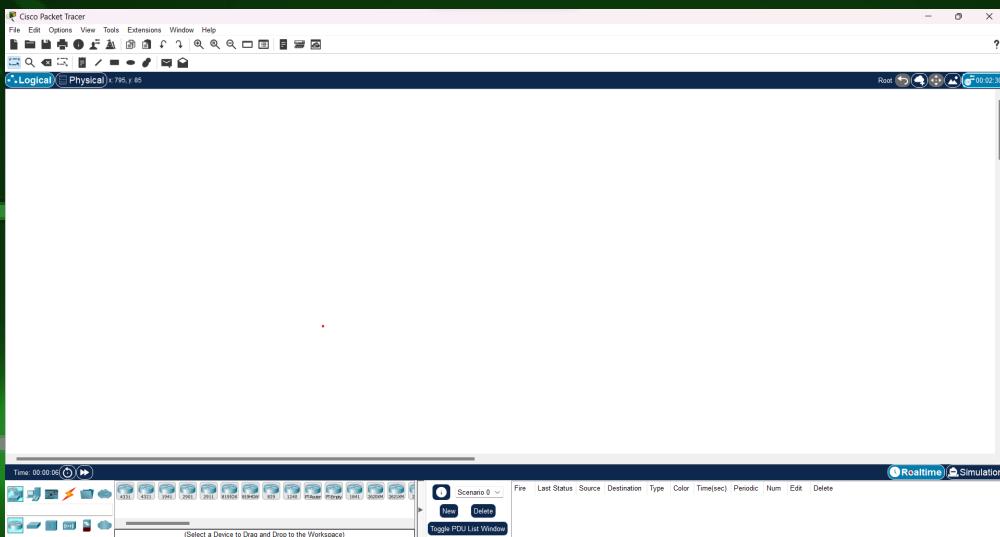


Runtrack

Les réseaux

JOB01

Télécharger et installer Cisco Packet Tracer.



JOB02

→ Qu'est-ce qu'un réseau ?

Dans les technologies de l'information, un réseau est défini par la mise en relation d'au moins deux systèmes informatiques au moyen d'un câble ou sans fil. Le réseau le plus basique comporte deux ordinateurs reliés par un câble. On parle aussi dans ce cas de réseau peer-to-peer (P2P) ou en français pair à pair. Ce genre de réseau n'a pas de hiérarchie : les deux participants sont au même niveau. Chaque ordinateur a accès aux données de l'autre et ils peuvent partager des ressources, comme un disque de stockage, des programmes, ou des périphériques (imprimante, etc.).

Les réseaux modernes sont un peu plus complexes en général et comportent bien plus que deux ordinateurs. Pour les systèmes à plus de dix participants, on utilise habituellement une configuration de type client/serveur. Dans ce modèle, un ordinateur agissant comme point de commutation central (serveur) met ses ressources à disposition des autres participants au réseau (clients).

→ À quoi sert un réseau informatique ?

La fonction principale d'un réseau est de fournir aux participants une plateforme pour l'échange de données et l'utilisation commune des ressources. Cette fonction revêt une importance cruciale, à tel point qu'on aurait aujourd'hui beaucoup de peine à imaginer notre quotidien et le monde du travail actuel sans l'existence des réseaux.

Les principaux avantages des réseaux sont donc :

Le partage des données

Le partage des ressources

*La gestion centralisée des programmes et des données
Le stockage et la sauvegarde centralisés des données
Le partage de la puissance de calcul et la capacité de stockage
L'administration simple des permissions et responsabilités*

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

Pour construire un réseau informatique, vous avez besoin de plusieurs composants matériels essentiels, chacun ayant des fonctions spécifiques pour assurer le bon fonctionnement du réseau. Voici une liste des principaux composants matériels et leurs fonctions :

1. Serveurs

Fonction : Stocker, gérer et traiter les données et applications centrales du réseau.

Description : Les serveurs sont des ordinateurs puissants dédiés à des tâches spécifiques telles que le stockage de données, l'hébergement de sites web, la gestion des e-mails, etc. Ils fournissent des services aux clients du réseau.

2. Switches

Fonction : Faciliter la communication entre les différents appareils connectés au réseau en acheminant les données vers leur destination.

Description : Les commutateurs (switches) dirigent le trafic réseau en fonction des adresses MAC (Media Access Control) des appareils connectés, permettant ainsi un transfert de données rapide et efficace.

3. Routeurs

Fonction : Acheminer les paquets de données entre les réseaux en utilisant des tables de routage.

Description : Les routeurs sont des appareils qui établissent des chemins efficaces pour le transfert de données entre différents réseaux, tels qu'Internet. Ils prennent des décisions de routage basées sur les adresses IP.

4. Cartes réseau (NIC - Network Interface Cards)

Fonction : Permettre à un appareil de se connecter physiquement au réseau.

Description : Les cartes réseau sont des composants matériels installés dans les ordinateurs, serveurs et autres appareils pour établir une connexion réseau physique. Elles convertissent les données en signaux compréhensibles par le réseau.

5. Câbles et Connecteurs

Fonction : Assurer la connectivité physique entre les appareils et les composants du réseau.

Description : Les câbles Ethernet et les connecteurs (comme les prises RJ45) permettent la transmission des signaux et des données entre les appareils connectés, assurant ainsi une connectivité réseau.

6. Firewalls

Fonction : Protéger le réseau en filtrant et en surveillant le trafic réseau, en empêchant l'accès non autorisé.

Description : Les pare-feu sont des dispositifs de sécurité qui contrôlent le trafic réseau en appliquant des règles de sécurité pour bloquer les menaces potentielles et protéger les données.

7. Modems

Fonction : Convertir les signaux numériques du réseau en signaux analogiques pour permettre la communication via les lignes téléphoniques ou les câbles.

Description : Les modems sont utilisés pour établir la connexion à l'Internet via divers types de liaisons, comme les lignes ADSL ou câbles.

8. Access Points (Points d'accès)

Fonction : Fournir un point d'accès sans fil au réseau pour les appareils compatibles Wi-Fi.

Description : Les points d'accès permettent aux appareils sans fil (ordinateurs, téléphones, tablettes, etc.) de se connecter au réseau en utilisant la technologie Wi-Fi.

9. Équipements de Stockage en réseau (NAS - Network-Attached Storage)

Fonction : Fournir un espace de stockage partagé accessible en réseau pour stocker et partager des fichiers.

Description : Les NAS sont des appareils de stockage spéciaux connectés au réseau, permettant aux utilisateurs de stocker, gérer et partager des fichiers de manière centralisée.

10. Équipements de Sauvegarde en réseau

Fonction : Sauvegarder les données du réseau de manière centralisée pour la protection et la récupération des données.

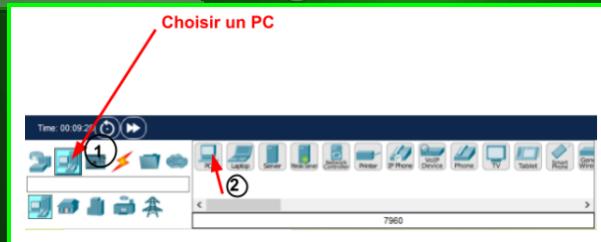
Description : Ces équipements permettent de sauvegarder régulièrement les données du réseau sur des dispositifs de stockage externes pour prévenir toute perte de données.

Chaque composant matériel joue un rôle crucial dans la construction et le fonctionnement d'un réseau, en permettant une communication fluide et sécurisée entre les appareils connectés.

JOB 03

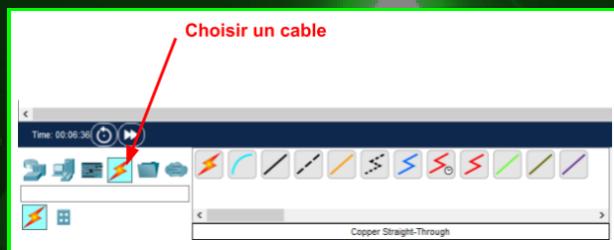
Maintenant que vous commencez à comprendre le réseau et que Packet Tracer est installé, vous allez pouvoir commencer à créer votre premier réseau.

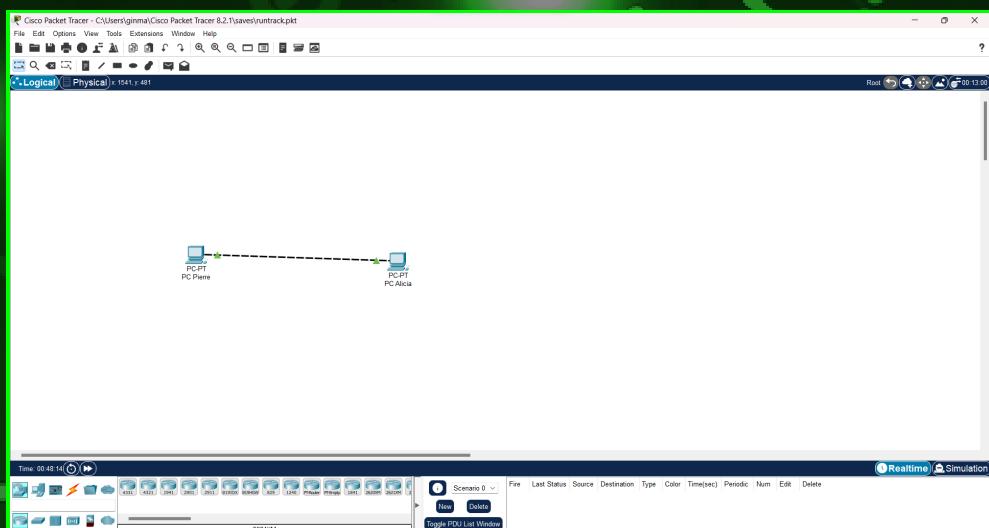
Commencez par mettre dans votre zone de travail deux ordinateurs de bureau, reliés entre eux par un câble.



→ Renommez les PCs en PC Pierre et PC Alicia.

→ Ensuite sélectionnez un câble approprié. Cliquez sur le premier ordinateur, puis sur le deuxième. Indiquez ensuite qu'il s'agit d'une connexion réseau "Fast Ethernet".





Voilà, un réseau est établi entre les deux machines.

→ Comme vous avez pu le constater, il existe des câbles croisés, droits... Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

Dans cet exercice, j'ai décidé de relier le PC de Pierre à celui d'Alicia avec un câble croisé. Le câble croisé permet d'envoyer des données dans les deux directions, ce qui dans notre cas, semble être le plus adapté pour relier un ordinateur à un autre. Le câble droit, lui, permet d'envoyer des données que dans une seule direction.

JOB 04

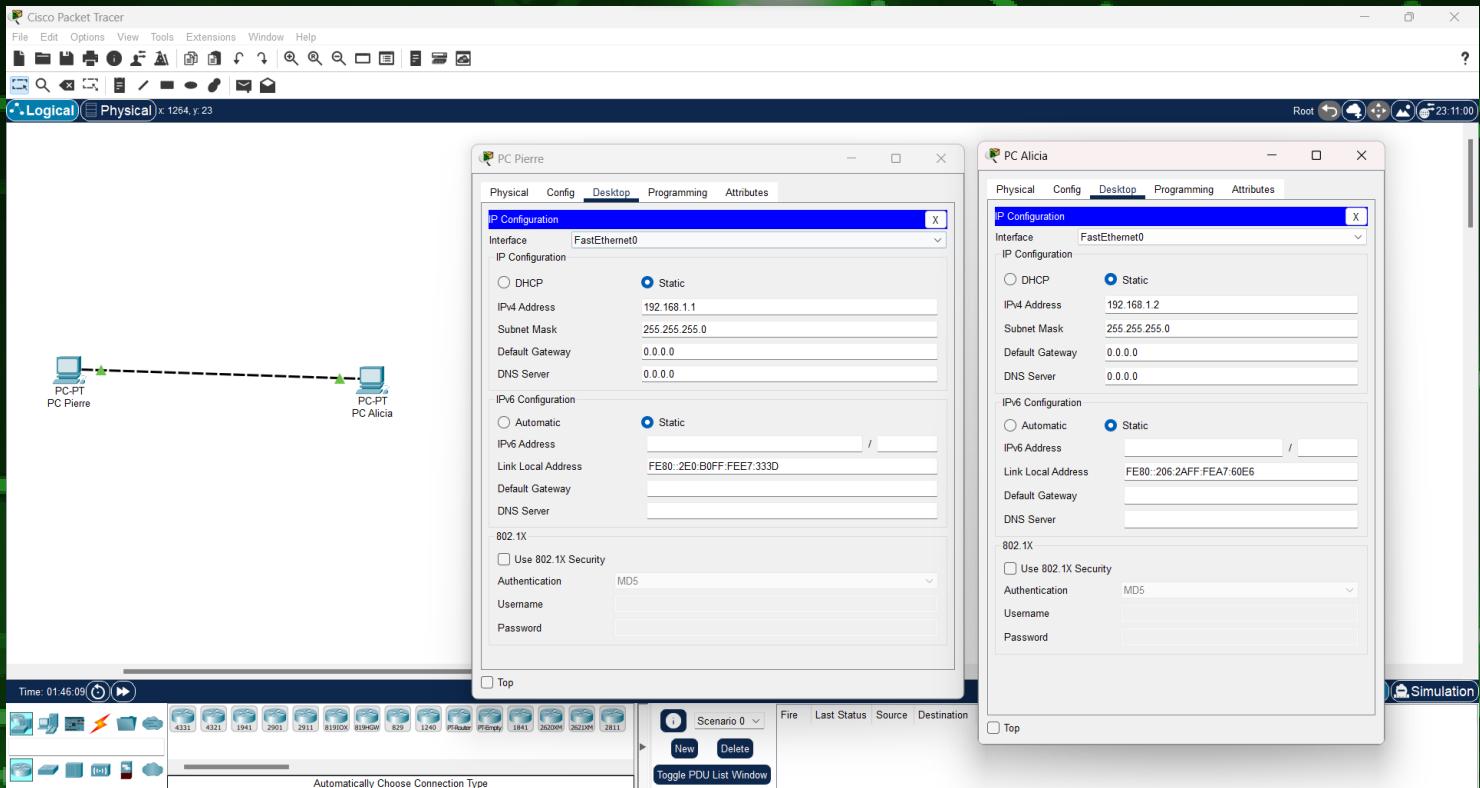
Maintenant que votre premier réseau est en place, configuez PC Pierre et PC Alicia comme suit :

• PC Pierre :

- Adress IP : 192.168.1.1
- Masque de sous-réseau : 255.255.255.0

• PC Alicia :

- Adress IP : 192.168.1.2
- Masque de sous-réseau : 255.255.255.0



→ Qu'est-ce qu'une adresse IP ?

Une adresse IP (*Internet Protocol address*) est un numéro unique attribué à chaque appareil connecté à un réseau informatique qui utilise le protocole Internet (IP). Ce numéro est utilisé pour identifier et localiser de manière unique cet appareil au sein d'un réseau et permettre sa communication avec d'autres appareils.

Il existe deux versions principales d'adresses IP utilisées actuellement : IPv4 (*Internet Protocol version 4*) et IPv6 (*Internet Protocol version 6*) :

IPv4

Format : Composé de quatre groupes de chiffres séparés par des points (par exemple, 192.168.1.1).

Longueur : Comprend 32 bits, ce qui permet environ 4,3 milliards d'adresses uniques.

Utilisation actuelle : Malgré le grand nombre d'adresses disponibles, la croissance rapide d'Internet a conduit à l'épuisement des adresses IPv4, d'où la nécessité de passer à IPv6.

IPv6

Format : Composé de huit groupes de chiffres et de lettres hexadécimales, séparés par des deux-points (par exemple, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Longueur : Comprend 128 bits, ce qui permet un nombre astronomiquement élevé d'adresses (plus de 340 milliards de milliards de milliards).

Utilisation actuelle : IPv6 a été développé pour remédier à la pénurie d'adresses IPv4 et pour accompagner la croissance continue d'Internet.

Les adresses IP permettent aux appareils de se connecter, de communiquer et de transmettre des données sur Internet ou au sein d'un réseau local. Chaque adresse IP est unique et assignée en fonction du réseau auquel l'appareil est connecté, permettant ainsi un routage approprié des données vers et depuis cet appareil.

→ A quoi sert un IP ?

Une adresse IP (Internet Protocol address) sert à plusieurs choses essentielles dans le contexte des réseaux informatiques et d'Internet :

Identification des appareils : L'adresse IP identifie de manière unique chaque appareil connecté à un réseau. Cela permet de distinguer un appareil d'un autre et de savoir où envoyer les données.

Communication : L'adresse IP est utilisée pour acheminer les données d'un appareil à un autre à travers le réseau. Les paquets de données sont dirigés vers leur destination en utilisant les adresses IP source et de destination.

Routage des données : Les routeurs utilisent les adresses IP pour déterminer le chemin optimal que doivent emprunter les paquets de données afin d'atteindre leur destination.

Localisation géographique : Dans certains cas, les adresses IP peuvent être utilisées pour estimer la localisation géographique approximative d'un appareil, bien que cette méthode ne soit pas précise.

Accès et sécurité : Les adresses IP sont utilisées dans des processus tels que le contrôle d'accès et les règles de sécurité (pare-feu) pour permettre ou bloquer l'accès à certaines ressources en fonction de l'adresse IP d'origine.

Hébergement de sites web et services : Les adresses IP sont attribuées aux serveurs qui hébergent des sites web et d'autres services en ligne. Lorsque vous tapez une URL dans votre navigateur, celle-ci est résolue en une adresse IP correspondant au serveur où le site est hébergé.

Systèmes de surveillance et d'analyse du trafic : Les adresses IP sont utilisées dans les systèmes de surveillance du trafic réseau pour suivre l'utilisation des réseaux, détecter les problèmes et effectuer des analyses de sécurité.

Attribution dynamique et statique : Les adresses IP peuvent être attribuées de manière dynamique (temporaire) ou statique (permanente). Les utilisateurs domestiques ont souvent des adresses IP dynamiques attribuées par leur fournisseur d'accès à Internet (FAI).

Les adresses IP sont des outils fondamentaux pour le fonctionnement d'Internet et des réseaux informatiques en général. Elles permettent d'identifier, de localiser et de diriger le trafic entre les appareils connectés, facilitant ainsi la communication et le transfert de données.

→ Qu'est-ce qu'une adresse MAC ?

Une adresse MAC (Media Access Control address), parfois appelée adresse physique, est un identifiant unique attribué à l'interface réseau d'un appareil, telle qu'une carte réseau, connectée à un réseau local (LAN). Contrairement à l'adresse IP, qui est logique et peut être modifiée, l'adresse MAC est généralement fixe et attribuée par le fabricant de l'appareil.

Voici quelques caractéristiques importantes concernant les adresses MAC :

Unicité : Chaque carte réseau a une adresse MAC unique. Aucune autre carte réseau ne devrait avoir la même adresse MAC, bien que dans la pratique, des collisions peuvent survenir lors de l'utilisation d'une immense quantité d'appareils.

Format : L'adresse MAC est généralement représentée sous la forme d'une série de chiffres hexadécimaux séparés par des deux-points ou des tirets (par exemple, 00:1A:2B:3C:4D:5E ou 00-1A-2B-3C-4D-5E).

Longueur : L'adresse MAC est composée de 48 bits (6 octets).

Composition : L'adresse MAC est généralement divisée en deux parties. Les trois premiers octets représentent l'identifiant d'organisation unique (OUI) attribué au fabricant du matériel réseau, tandis que les trois derniers octets sont un numéro de série unique attribué à l'appareil.

Attribution : L'adresse MAC est généralement attribuée par le fabricant de la carte réseau au moment de la fabrication. Elle est rarement modifiée pendant la durée de vie de l'appareil.

Utilisation : L'adresse MAC est utilisée pour acheminer les données au niveau de la couche de liaison dans le modèle OSI (couche 2). Les commutateurs réseau utilisent les adresses MAC pour diriger le trafic au sein du réseau local.

Relation avec l'adresse IP : L'adresse MAC est souvent utilisée en conjonction avec l'adresse IP. Lorsque des données sont envoyées à un appareil, elles sont d'abord acheminées en utilisant l'adresse IP, puis le réseau utilise l'adresse MAC pour diriger les données spécifiquement vers l'appareil correspondant.

L'adresse MAC est une adresse unique attribuée à chaque carte réseau, permettant de l'identifier de manière spécifique sur un réseau local. Elle est cruciale pour le routage efficace des données à travers le réseau au niveau de la couche de liaison.

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

Les adresses IP publiques et privées sont des types d'adresses IP utilisées pour différencier les appareils sur un réseau en fonction de leur accessibilité depuis Internet ou depuis un réseau local privé. Voici une explication de chaque type d'adresse IP :

Adresse IP Publique

Définition : Une adresse IP publique est une adresse unique attribuée à un appareil ou à un réseau qui est accessible depuis Internet. Elle peut être utilisée pour communiquer avec d'autres appareils et services sur Internet.

Fonction : Les adresses IP publiques permettent aux appareils de communiquer avec d'autres appareils situés sur Internet. C'est comme l'adresse postale de votre appareil sur le réseau mondial.

Exemple : 203.0.113.12

Adresse IP Privée

Définition : Une adresse IP privée est une adresse utilisée à l'intérieur d'un réseau local privé (comme votre réseau domestique ou d'entreprise). Ces adresses ne sont pas directement accessibles depuis Internet.

Fonction : Les adresses IP privées servent à identifier les appareils au sein d'un réseau local privé et permettent la communication interne entre ces appareils.

Exemples courants de plages d'adresses IP privées :

192.168.0.0 à 192.168.255.255 (Classe C)

Les adresses IP publiques sont utilisées pour permettre la communication entre différents réseaux sur Internet, tandis que les adresses IP privées sont utilisées pour organiser et permettre la communication entre les appareils à l'intérieur d'un réseau local (intranet). Pour permettre la communication entre le réseau local et Internet, les routeurs utilisent des techniques de traduction d'adresses réseau (NAT - Network Address Translation) pour traduire les adresses IP privées en adresses IP publiques et vice versa.

→ Quelle est l'adresse de ce réseau ?

L'adresse du réseau créé entre l'ordinateur de Pierre et celui d'Alicia est la suivante :

255.255.255.0

JOB05

→ Quelle ligne de commande avez-vous utilisée pour vérifier l'IP des machines ?

Pour vérifier L'IP des deux machines, il faut cliquer sur la machine concernée, se rendre dans l'onglet Desktop, cliquer sur la petite croix en haut à droite (au bout de la ligne bleue) et sélectionner "Command prompt". Cela ouvrira une nouvelle fenêtre où il faudra taper la commande suivante : **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::206:2AFF:FEA7:60E6
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.2
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
0.0.0.0

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE7:333D
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
0.0.0.0

C:\>
```

```
C:\>ip config
Invalid Command.

C:\>.ip config
Invalid Command.

C:\>ip config
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE7:333D
IPv6 Address.....: ::1
IPv4 Address.....: 192.168.1.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: ::1
0.0.0.0

Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::2E0:B0FF:FE7:333D
IPv6 Address.....: ::1
IPv4 Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: ::1
0.0.0.0

C:\>
```

Voilà, l'adresse IP s'affiche, il ne reste plus qu'à comparer avec l'IP affichée avec celle rentrée précédemment.

JOB06

→ Quelle est la commande permettant de Ping entre des PC ?

- Pour réaliser un ping entre deux machines, il faut ouvrir le terminal d'une des machines puis utiliser la commande ping suivi de l'adresse IP de la seconde machine. Ce qui donne, dans le cas où l'on veut réaliser un ping de la machine à Pierre à celui d'Alicia : **ping 192.168.1.2**

```
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:\>

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:\>
```

JOB07

Éteignez le PC de Pierre. Utilisez le terminal du PC d'Alicia et PING le PC le Pierre. Faites une capture d'écran du terminal d'Alicia.

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

→ Expliquez pourquoi.

The WMP300N module provides one 2.4GHz wireless interface suitable for connection to wireless networks. The module supports protocols that use Ethernet for LAN access.

Top


```
Cisco Packet Tracer PC Command Line 1.0
C:>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

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.

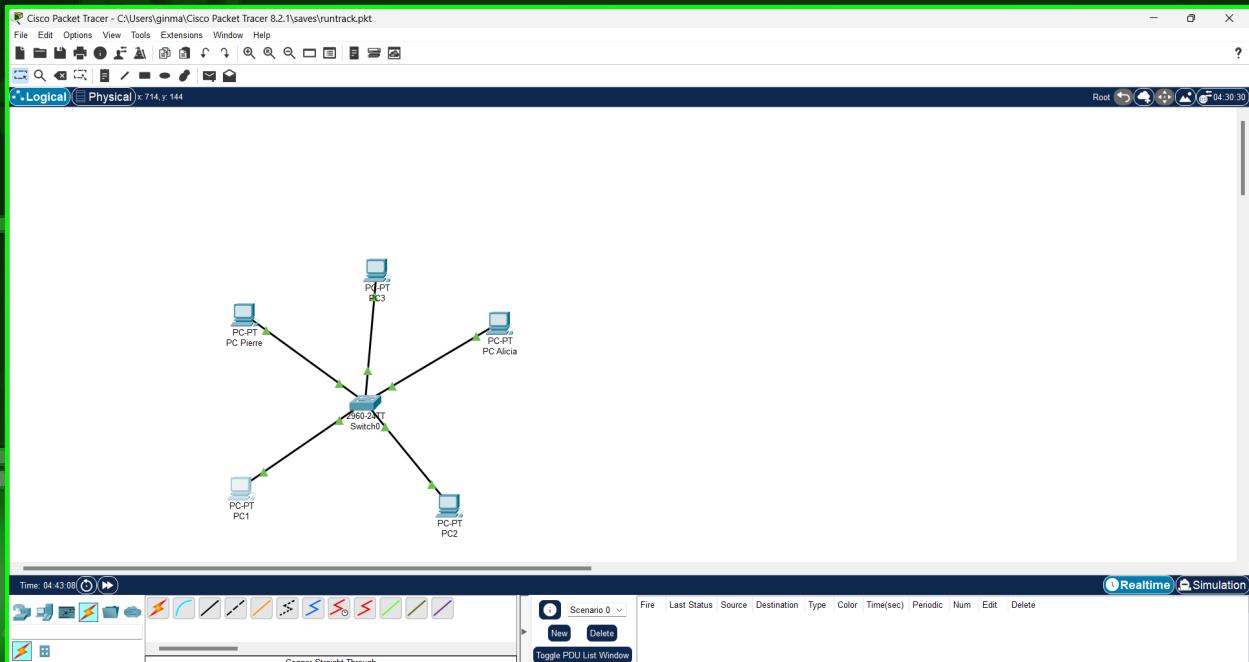
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:>
```

Top

Lorsque vous exécutez un ping vers une machine qui est éteinte (c'est-à-dire qu'elle n'est pas allumée ou qu'elle n'est pas connectée au réseau), les paquets ICMP (Internet Control Message Protocol) émis par la commande ping ne peuvent pas atteindre la machine car elle est hors ligne, ce qui conduit à l'absence de réponse lors du ping.

JOB 08

Agrandissez votre sous réseau avec cinq ordinateurs, et configuez vos ordinateurs sur le même réseau. Vérifiez qu'ils soient tous bien connectés en affectant un PING en utilisant le terminal prompt.



The screenshot shows the 'PC1' window in Cisco Packet Tracer. The tab bar at the top has 'Physical', 'Config', 'Desktop' (which is selected), 'Programming', and 'Attributes'. Below the tab bar is a 'Command Prompt' window with a blue header. The command entered is 'C:\>ping 192.168.1.3'. The output shows the ping results:

```
Cisco Packet Tracer PC Command Line 1.0
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=7ms TTL=128
Reply from 192.168.1.3: bytes=32 time=11ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms 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 = 13ms, Average = 7ms

C:\>
```

Pour vérifier que les ordinateurs sont tous bien connectés entre eux, il faut ouvrir le terminal prompt et effectuer une commande ping avec chaque ordinateur.

→ Quelle est la différence entre un hub et un switch ?

Un hub et un switch sont tous deux des dispositifs utilisés dans les réseaux informatiques pour connecter plusieurs appareils, mais ils fonctionnent de manière différente et ont des performances distinctes. Voici les principales différences entre un hub et un switch :

Fonctionnement :

Hub : Un hub est un appareil simple qui agit comme un répéteur. Lorsqu'il reçoit des données d'un port, il les transmet à tous les autres ports du hub, indépendamment de la destination. Cela signifie que tous les appareils connectés au hub voient toutes les données, et c'est au dispositif destinataire de déterminer si ces données lui sont destinées.

Switch : Un switch, en revanche, est plus intelligent. Il apprend les adresses MAC des appareils connectés à ses ports et utilise ces informations pour acheminer les données uniquement vers le port où se trouve le destinataire. Ainsi, il optimise le trafic en ne diffusant pas les données à tous les ports.

Transmission des données :

Hub : Les données reçues sur un port sont répétées et envoyées à tous les autres ports du hub, quelle que soit la destination.

Switch : Les données sont acheminées uniquement vers le port où se trouve le destinataire, en utilisant les adresses MAC pour déterminer le port de destination.

Sécurité et performances :

Hub : Les données sont transmises en broadcast, ce qui peut poser des problèmes de sécurité et de bande passante, car toutes les données sont accessibles à tous les appareils du réseau.

Switch : Les données sont transmises uniquement au port où se trouve le destinataire, améliorant la sécurité et optimisant l'utilisation de la bande passante.

Collisions :

Hub : Les collisions peuvent se produire car toutes les données sont diffusées à tous les ports, ce qui peut entraîner des interférences.

Switch : Les collisions sont réduites car les données sont acheminées directement vers le port de destination.

Un hub transmet les données à tous les ports, tandis qu'un switch achemine les données uniquement vers le port où se trouve le destinataire, améliorant ainsi l'efficacité, la sécurité et les performances du réseau. Les switches sont largement préférés aux hubs dans les réseaux modernes en raison de leur fonctionnement plus intelligent et de leurs avantages en termes de performance et de sécurité.

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

Un hub fonctionne en répétant les données reçues à tous les ports, ce qui signifie que toutes les données sont diffusées sur tous les appareils connectés. Cependant, cela conduit à des limitations de performance, des risques de collisions et une sécurité réduite, ce qui explique pourquoi les switches, offrant un acheminement intelligent des données vers la destination appropriée, sont désormais largement préférés aux hubs dans les réseaux modernes.

→ Quels sont les avantages et inconvénients d'un switch ?

Un switch est un dispositif de réseau qui permet de connecter plusieurs appareils au sein d'un réseau local (LAN) et de faciliter la communication entre eux. Voici les avantages et inconvénients associés à l'utilisation d'un switch dans un réseau :

Avantages :

- Acheminement intelligent :

Les switches acheminent les données uniquement vers le port où se trouve le destinataire, en utilisant les adresses MAC. Cela optimise le trafic et évite la diffusion des données à tous les ports comme c'est le cas avec un hub.

- Réduction des collisions :

Étant donné que les données sont acheminées directement vers le port de destination, les collisions sont réduites, ce qui améliore l'efficacité du réseau.

- Amélioration des performances :

Les switches permettent d'optimiser l'utilisation de la bande passante en transmettant les données uniquement vers les ports concernés. Cela améliore les performances du réseau en réduisant la congestion et les retards.

- Sécurité renforcée :

Étant donné que les données sont transmises uniquement au port du destinataire, les autres appareils sur le réseau ne peuvent pas intercepter ces données, ce qui améliore la sécurité du réseau.

- Capacité à segmenter le réseau :

Les switches permettent de diviser le réseau en segments logiques en créant des réseaux virtuels (VLAN), ce qui améliore la sécurité et la gestion du réseau.

- Auto-apprentissage des adresses MAC :

Les switches apprennent automatiquement les adresses MAC des appareils connectés et construisent une table d'adresses pour optimiser l'acheminement des données.

Inconvénients :

- Coût :

Les switches sont généralement plus chers que les hubs, ce qui peut être un inconvénient en termes de coût d'acquisition et d'installation.

- Complexité de gestion :

La configuration et la gestion d'un switch peuvent être plus complexes que celles d'un hub en raison de ses fonctionnalités avancées. Cela nécessite des compétences techniques pour une configuration optimale.

- Risques de saturation :

Bien que les switches optimisent la bande passante, ils peuvent toujours être saturés si le nombre d'appareils connectés est important ou si la bande passante disponible est insuffisante.

- Dépendance à l'énergie :

Un switch nécessite de l'électricité pour fonctionner. En cas de panne de courant, le réseau connecté au switch peut être hors service.

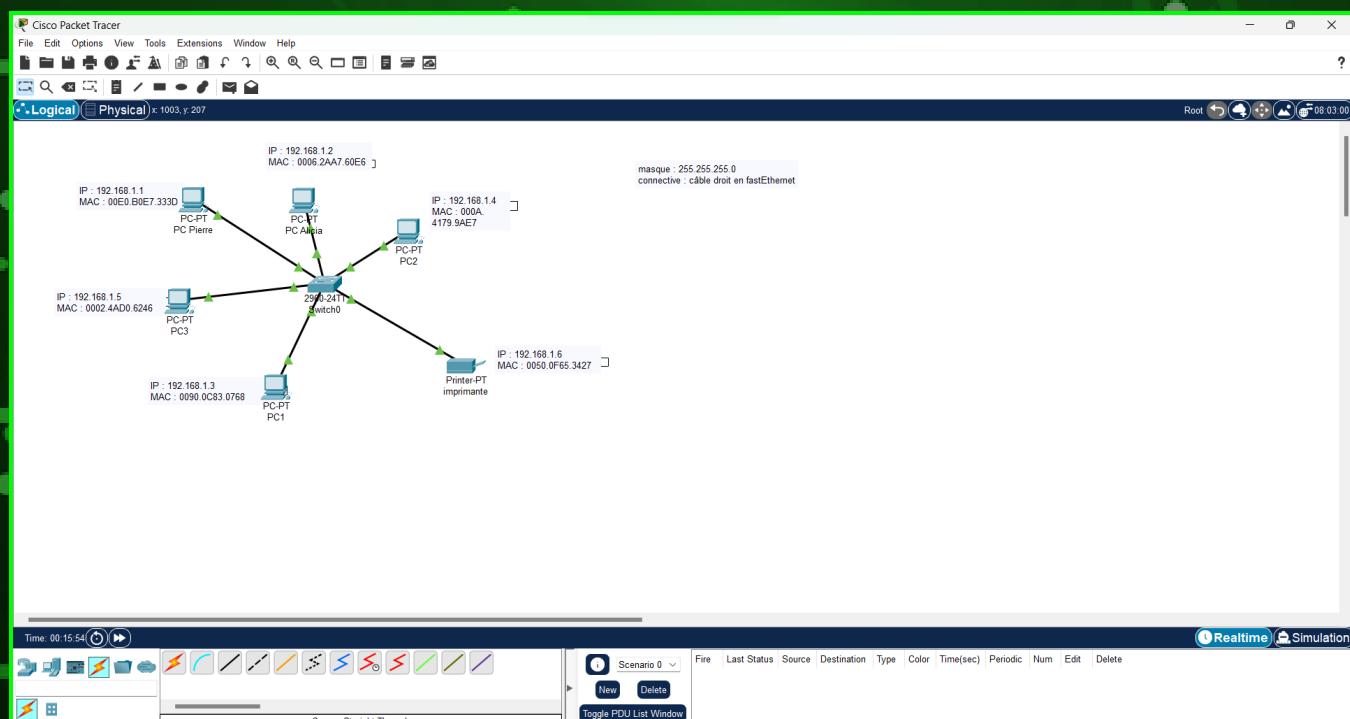
Les switches offrent des avantages majeurs tels que l'acheminement intelligent, la réduction des collisions, l'amélioration des performances et la sécurité renforcée, mais ils peuvent être plus coûteux et nécessiter une gestion plus complexe par rapport aux hubs. Il est important de considérer ces avantages et inconvénients lors de la conception et de la mise en place d'un réseau pour choisir la meilleure solution en fonction des besoins spécifiques.

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

Un switch gère le trafic en utilisant les adresses MAC pour acheminer les données directement vers le port où se trouve le destinataire, évitant ainsi la diffusion des données à tous les ports comme un hub le ferait. Cela optimise la bande passante et réduit les collisions, améliorant ainsi les performances du réseau. Le switch utilise une table d'adresses MAC pour associer chaque adresse MAC à un port spécifique, ce qui lui permet de transmettre sélectivement les données vers les destinataires appropriés.

JOB 09

Ajoutez une imprimante. Vérifiez qu'elle soit bien connectée. Réalisez un schéma de votre réseau en utilisant le logiciel de votre choix. Celui-ci devra représenter la topologie et la configuration de votre réseau, en incluant les composants (ordinateurs, commutateurs, ...) et ajoutez le schéma ainsi que vos explications sur votre documentation.



Identifiez au moins trois avantages importants d'avoir un schéma

Faire le schéma d'un réseau présente plusieurs avantages clés dans la gestion et la conception d'un réseau informatique :

Visualisation des composants : Le schéma du réseau fournit une représentation visuelle des composants du réseau, y compris les appareils, les connexions, les sous-réseaux, les serveurs, les routeurs, les commutateurs, etc. Cela permet à toute personne impliquée dans la gestion du réseau de comprendre rapidement sa structure et son architecture.

Facilitation de la communication : En visualisant le réseau, les équipes techniques et non techniques peuvent mieux communiquer et comprendre les interactions entre les différentes parties du réseau. Cela favorise la collaboration et la prise de décision informée.

Identification des problèmes : Un schéma de réseau bien élaboré permet d'identifier rapidement les problèmes et les goulets d'étranglement. Lorsqu'un dysfonctionnement survient, les techniciens peuvent se référer au schéma pour localiser et résoudre le problème plus efficacement.

Planification de l'expansion : En visualisant la topologie du réseau, les planificateurs peuvent mieux anticiper les besoins d'expansion, d'ajout de nouveaux appareils ou de mise à niveau des composants existants. Cela facilite la planification des ressources et des investissements futurs.

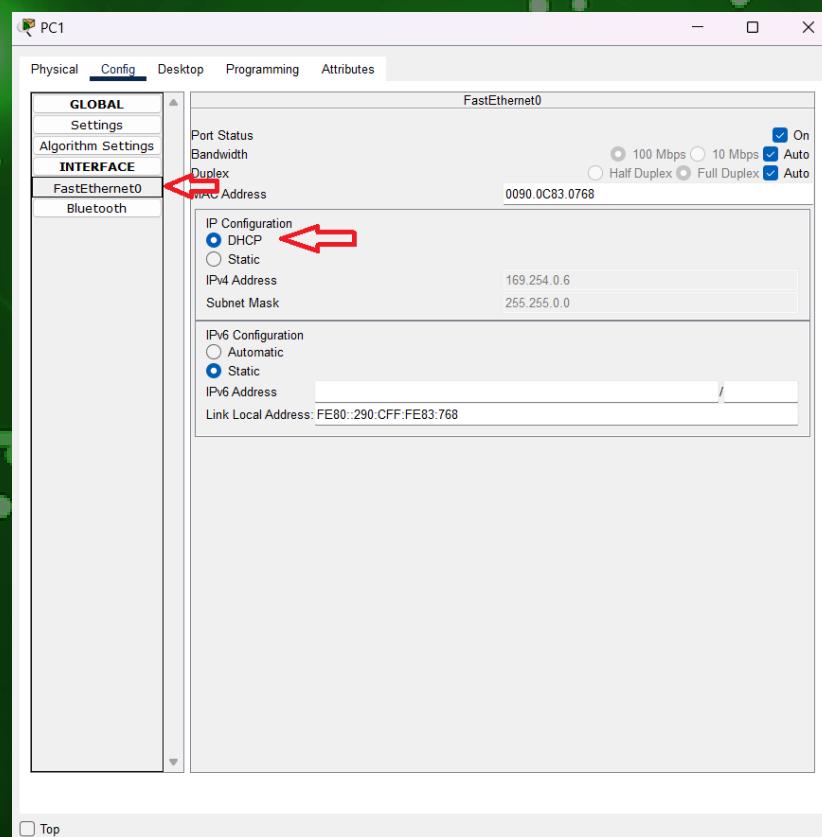
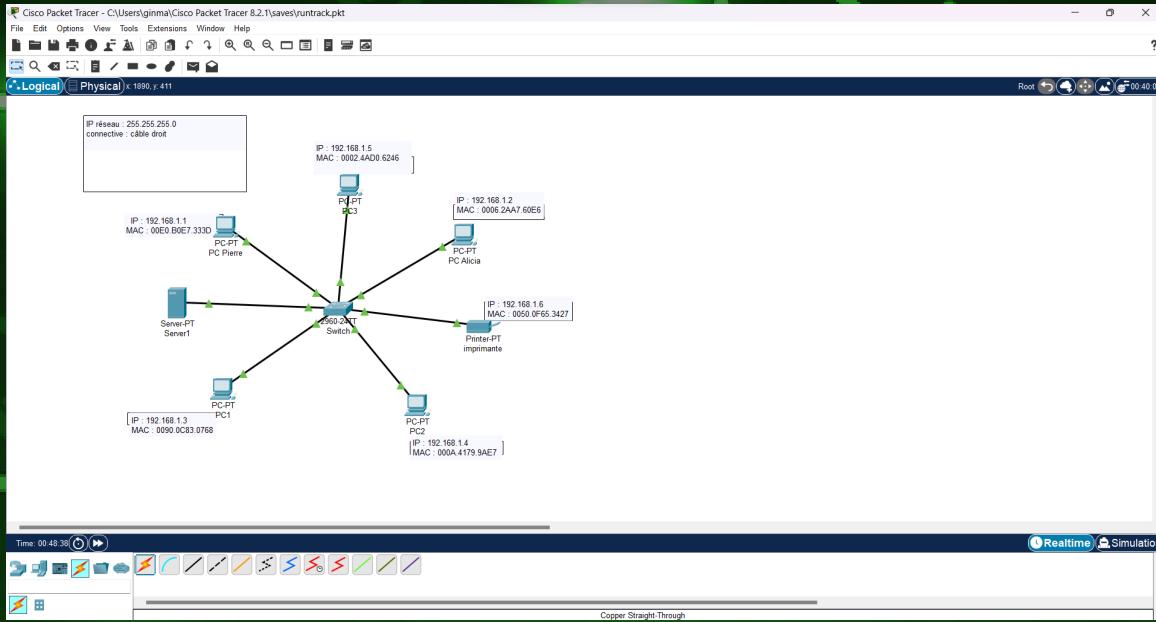
Sensibilisation à la sécurité : En incluant des informations sur les points d'accès, les pare-feu, les zones DMZ et autres éléments de sécurité, le schéma du réseau permet de sensibiliser aux risques et de planifier des mesures de sécurité appropriées.

Gestion des autorisations : En indiquant les différentes autorisations d'accès aux données et aux ressources, le schéma du réseau aide à gérer les niveaux d'accès et à garantir que seules les personnes autorisées ont accès à des parties spécifiques du réseau.

Créer un schéma de réseau offre des avantages majeurs tels que la clarté et la compréhension du réseau, la facilitation de la planification et du dépannage, ainsi que l'amélioration de la sécurité et de la gestion des risques. C'est un outil essentiel pour administrer, étendre et sécuriser efficacement un réseau informatique.

JOB10

Vous allez donc mettre en place un serveur DHCP, pour permettre la distribution automatique d'adresse IP. Cela va permettre aux ordinateurs de pouvoir communiquer entre eux sans que vous adressiez des IP fixes.



Après avoir posé et raccordé le serveur au switch, il faut allez dans les paramètres du serveur et cocher la fonction DHCP à la place de STATIC. Il faut répéter cette action auprès de tous les PC et périphériques. Ensuite votre serveur pourra générer automatiquement une adresse IP pour chaque matériel.

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

Une adresse IP statique est configurée manuellement sur chaque appareil, tandis qu'une adresse IP attribuée par DHCP est gérée par un serveur DHCP qui attribue automatiquement les adresses IP aux appareils sur le réseau.

Les adresses IP statiques restent constantes, tandis que les adresses IP attribuées par DHCP peuvent changer dynamiquement en fonction de la configuration du serveur DHCP.

JOB 11

1 sous-réseau de 12 hôtes

masque	adresse sous réseau	plage d'adresses utilisables	adresse de diffusion	nombre d'hôtes disponibles
255.255.255.240	10.1.0.0	10.1.0.1 à 10.1.0.14	10.1.1.15	16

5 sous-réseau de 30 hôtes

masque	adresse sous réseau	plage d'adresses utilisables	adresse de diffusion	nombre d'hôtes disponibles
255.255.255.224	10.2.0.0	10.2.0.1 à 10.2.0.30	10.2.0.31	32
255.255.255.224	10.3.0.0	10.3.0.1 à 10.3.0.30	10.3.0.31	32
255.255.255.224	10.4.0.0	10.4.0.1 à 10.4.0.30	10.4.0.31	32
255.255.255.224	10.5.0.0	10.5.0.1 à 10.5.0.30	10.5.0.31	32
255.255.255.224	10.6.0.0	10.6.0.1 à 10.6.0.30	10.6.0.31	32

5 sous-réseau de 120 hôtes

masque	adresse sous réseau	plage d'adresses utilisables	adresse de diffusion	nombre d'hôtes disponibles
255.255.255.128	10.7.0.0	10.7.0.1 à 10.7.0.126	10.7.0.127	128
255.255.255.128	10.8.0.0	10.8.0.1 à 10.8.0.126	10.8.0.127	128
255.255.255.128	10.9.0.0	10.9.0.1 à 10.9.0.126	10.9.0.127	128
255.255.255.128	10.10.0.0	10.10.0.1 à 10.10.0.126	10.10.0.127	128
255.255.255.128	10.11.0.0	10.11.0.1 à 10.11.0.126	10.11.0.127	128

5 sous-réseau de 160 hôtes

masque	adresse sous réseau	plage d'adresses utilisables	adresse de diffusion	nombre d'hôtes disponibles
255.255.255.0	10.12.0.0	10.12.0.1 à 10.12.0.160	10.12.0.161	256
255.255.255.0	10.13.0.0	10.13.0.1 à 10.13.0.160	10.13.0.161	256
255.255.255.0	10.14.0.0	10.14.0.1 à 10.14.0.160	10.14.0.161	256
255.255.255.0	10.15.0.0	10.15.0.1 à 10.15.0.160	10.15.0.161	256
255.255.255.0	10.16.0.0	10.16.0.1 à 10.16.0.160	10.16.0.161	256

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

Choisir une adresse de classe A pour un réseau est approprié lorsque vous avez besoin d'une grande plage d'adresses pour de nombreux hôtes, ou lorsque vous envisagez de diviser cette plage en plusieurs sous-réseaux. Cependant, les adresses de classe A sont rares et sont souvent réservées pour les grandes organisations ou les fournisseurs de services Internet.

Pour la plupart des réseaux, des plages d'adresses de classe B ou C sont plus appropriées en raison de leur taille plus modeste et de leur utilisation plus efficace de l'espace d'adressage IP.

Le choix de la classe d'adresse dépend des besoins spécifiques de votre réseau.

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

Les adresses IP sont divisées en classes en fonction de leur structure et de leur plage d'adresses. Il y a cinq classes d'adresses IP, notées de A à E, mais les classes A, B, et C sont les plus couramment utilisées. Voici la différence entre ces trois classes d'adresses IP :

Classe A

Format : Les adresses de classe A ont un format où le premier octet (8 bits) est réservé pour l'identification du réseau, et les trois octets restants (24 bits) sont alloués aux hôtes.

Plage : Les adresses de classe A vont de 0.0.0.0 à 127.255.255.255.

Utilisation typique : Les adresses de classe A sont généralement utilisées pour les réseaux très vastes, comme les réseaux de grande entreprise ou les fournisseurs de services Internet (ISP). Elles permettent un grand nombre d'hôtes, mais sont relativement peu nombreuses en raison de leur format.

Classe B

Format : Les adresses de classe B ont un format où les deux premiers octets (16 bits) sont réservés pour l'identification du réseau, et les deux octets suivants (16 bits) sont alloués aux hôtes.

Plage : Les adresses de classe B vont de 128.0.0.0 à 191.255.255.255.

Utilisation typique : Les adresses de classe B sont souvent utilisées pour les réseaux de taille moyenne à grande, tels que les réseaux d'entreprises et les institutions éducatives. Elles permettent un nombre modéré de hôtes et offrent une plus grande flexibilité que les adresses de classe A.

Classe C

Format : Les adresses de classe C ont un format où les trois premiers octets (24 bits) sont réservés pour l'identification du réseau, et le dernier octet (8 bits) est alloué aux hôtes.

Plage : Les adresses de classe C vont de 192.0.0.0 à 223.255.255.255.

Utilisation typique : Les adresses de classe C sont couramment utilisées pour les petits réseaux, comme les réseaux locaux (LAN) d'entreprises ou de particuliers. Elles permettent un nombre limité d'hôtes par réseau.

Il est essentiel de noter que les classes D (utilisées pour le multicast) et E (réservées à des fins expérimentales) ont des structures d'adressage différentes et ne sont pas aussi couramment utilisées que les classes A, B et C.

JOB12

7	couche application	point de contact avec les services réseaux	données	FTP
6	couche présentation	préparation des données pour la présentation (formatage, chiffrement, encodage etc.)	données	HTML
5	couche session	organisation de la session de communication (point de contrôle, etc.)	données	
4	couche transport	coordination du transfert des segments (numéro de port, contrôle réception, etc.)	segments	TCP, SSL/TLS, UDP
3	couche réseau	routage des paquets entre les noeuds d'un réseau	paquets	IPv4, IPv6, routeur
2	couche liaison	assure le transfert des trames de noeud à noeud	trames	Ethernet, MAC, PPTP, wi-fi
1	couche physique	transmission des bits	bits	fibre optique, câble RJ45

JOB13

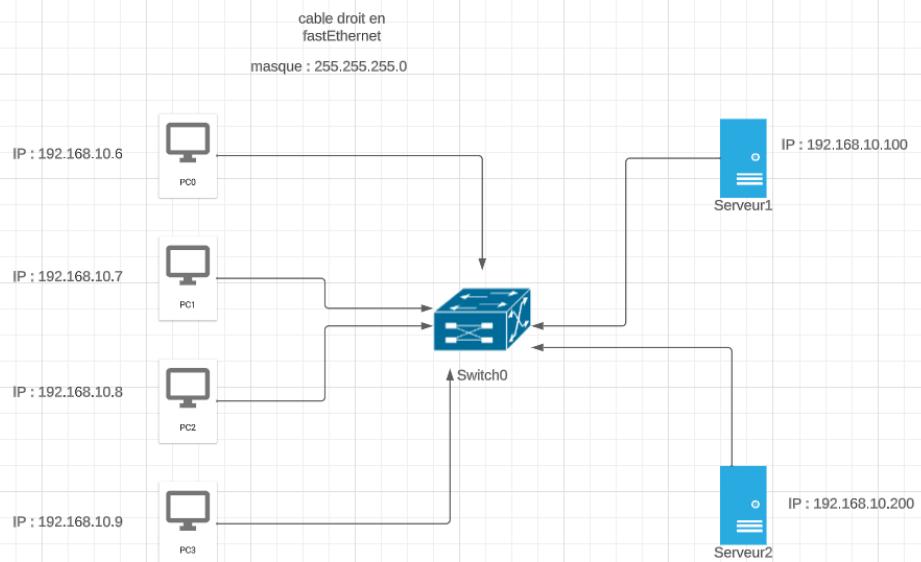
Vous êtes étudiants à l'école de la plateforme qui possède un parc informatique composé de 4 PCs. L'adressage IP du réseau est :

- PC0 : 192.168.10.6
- PC1 : 192.168.10.7
- PC2 : 192.168.10.8
- PC3 : 192.168.10.9
- Serveur 1 : 192.168.10.100
- Serveur 2 : 192.168.10.200

Avec un masque de sous-réseau :

255.255.255.0

→ Quelle est l'architecture de ce réseau ?



→ Indiquer quelle est l'adresse IP du réseau ?

L'adresse IP de ce réseau est : 192.168.10.0

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

D'après les informations disponibles sur ce réseau, on doit pouvoir y brancher 254 hôtes.

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

L'adresse de diffusion de ce réseau est : 192.168.10.255

JOB14

Convertissez les adresses IP suivantes en binaires :

- 145.32.59.24 = 10010001.00100000.00111011.00011000
- 200.42.129.16 = 11001000.00101010.10000001.00010000
- 14.82.19.54 = 00010010.01010010.00010011.00110110

JOB15

→ Qu'est-ce que le routage ?

Le routage est le processus de transmission de données dans un réseau informatique. Il utilise des adresses, des protocoles de routage et des routeurs pour déterminer le chemin optimal pour acheminer des données d'une source vers une destination. Il est fondamental pour le fonctionnement d'Internet et pour l'efficacité des réseaux locaux et étendus.

→ Qu'est-ce qu'un gateway ?

Une gateway, également appelée passerelle en français, est un dispositif matériel ou logiciel utilisé pour connecter deux réseaux informatiques distincts, permettant ainsi la communication entre eux. Les gateways agissent comme des points d'entrée ou de sortie entre ces réseaux et jouent un rôle essentiel dans le routage et la traduction des données.

C'est un élément clé pour permettre la communication entre des réseaux différents en assurant la traduction de protocoles, la sécurité, la connectivité et la gestion du trafic. Elle facilite l'interconnexion des réseaux hétérogènes, que ce soit au sein d'une même entreprise, sur Internet ou entre des environnements réseau variés.

→ Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel (Virtual Private Network en anglais), est une technologie de réseau qui permet de créer un tunnel de communication sécurisé et chiffré sur un réseau public, comme Internet.

Les VPN sont utilisés pour garantir la confidentialité, la sécurité et l'anonymat des données lors de leur transmission sur Internet ou entre réseaux distants.

Il est important de noter que bien que les VPN offrent un niveau élevé de sécurité et de confidentialité, ils ne sont pas totalement invulnérables et ne protègent que les données transitant sur le tunnel VPN.

Les mesures de sécurité supplémentaires, telles que la mise à jour du logiciel, la gestion des mots de passe et la vigilance en ligne, restent essentielles pour garantir une protection globale.

→ Qu'est-ce qu'un DNS ?

Le DNS, ou Domain Name System (Système de Noms de Domaine en français), est un protocole et un système essentiel dans le fonctionnement d'Internet. Son rôle principal est de traduire les noms de domaine conviviaux (comme www.exemple.com) en adresses IP (Internet Protocol) numériques, qui sont nécessaires pour identifier et localiser des serveurs et des ressources sur Internet. C'est un système de traduction qui rend Internet plus convivial en permettant l'utilisation de noms de domaine au lieu d'adresses IP. Il est essentiel au fonctionnement d'Internet en tant que fondation de la résolution des noms de domaine.