

RUNTRACK RÉSEAU

JOB 01:

Installation de cisco packet tracer

JOB 02:

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.

A quoi sert un réseau informatique?

Le réseau informatique désigne les appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux. Ces appareils en réseau utilisent un système de règles, appelées protocoles de communication, pour transmettre des informations sur des technologies physiques ou sans fil.

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

La construction d'un réseau nécessite plusieurs éléments clés. Voici les composants de base ainsi que leurs fonctions :

1. Routeur : Un routeur est un appareil qui relie différents réseaux informatiques. Il est utilisé pour transmettre des données entre ces réseaux en choisissant les chemins les plus efficaces. Les routeurs sont essentiels pour diriger le trafic de données entre les différents appareils connectés à un réseau.
2. Commutateur (Switch) : Un commutateur est un appareil réseau qui connecte des périphériques sur un réseau local (LAN). Il dirige le trafic réseau en fonction de l'adresse MAC des périphériques dans le réseau. Les commutateurs améliorent les performances en permettant des communications directes entre les périphériques connectés.
3. Firewall : Un pare-feu est un dispositif de sécurité réseau qui surveille et contrôle le trafic entrant et sortant du réseau. Il empêche les accès non autorisés et les menaces potentielles en filtrant le trafic en fonction de règles de sécurité prédéfinies. Les pare-feu peuvent être mis en place pour protéger les réseaux locaux ou les réseaux étendus.

4. Points d'accès sans fil (Access Points) : Les points d'accès sans fil sont utilisés pour étendre un réseau local câblé en permettant la connectivité sans fil pour les appareils tels que les ordinateurs portables, les smartphones et les tablettes. Ils permettent aux appareils de se connecter au réseau via des connexions Wi-Fi.

5. Modem : Un modem est un périphérique qui convertit les signaux numériques en signaux analogiques et vice versa. Il est utilisé pour établir une connexion à Internet en convertissant les signaux numériques des ordinateurs en signaux analogiques qui peuvent être transmis via des lignes téléphoniques ou des câbles coaxiaux.

6. Câbles et connecteurs : Les câbles Ethernet sont essentiels pour connecter les périphériques au réseau. Ils assurent la transmission rapide et fiable des données entre les différents composants du réseau. Les connecteurs tels que les prises Ethernet et les connecteurs RJ45 sont utilisés pour connecter les câbles aux dispositifs réseau.

7. Serveur : Un serveur est un ordinateur ou un logiciel qui fournit des services, des ressources ou des données à d'autres ordinateurs, connus sous le nom de clients, dans le réseau. Il peut s'agir de serveurs de fichiers, de serveurs Web, de serveurs de messagerie, etc. Les serveurs jouent un rôle crucial dans la gestion et le stockage des données au sein du réseau.

JOB 03:

Quels câbles avez-vous choisis pour relier les deux ordinateurs ? Expliquez votre choix.

Câble Ethernet : Il s'agit d'un câble filaire qui permet de connecter des périphériques entre eux sur un réseau local (LAN). Les câbles Ethernet offrent des connexions rapides et fiables, et ils sont souvent utilisés pour les connexions réseau filaires. Ils sont une solution idéale pour relier deux ordinateurs de bureau ou deux ordinateurs portables sur un réseau domestique ou dans un petit bureau.

JOB 04:

Qu'est-ce qu'une adresse IP?

Une adresse IP est une représentation numérique de l'endroit où un appareil est connecté à Internet.

A quoi sert un IP?

L'adresse IP sert à gérer la connexion entre un appareil et un site de destination.

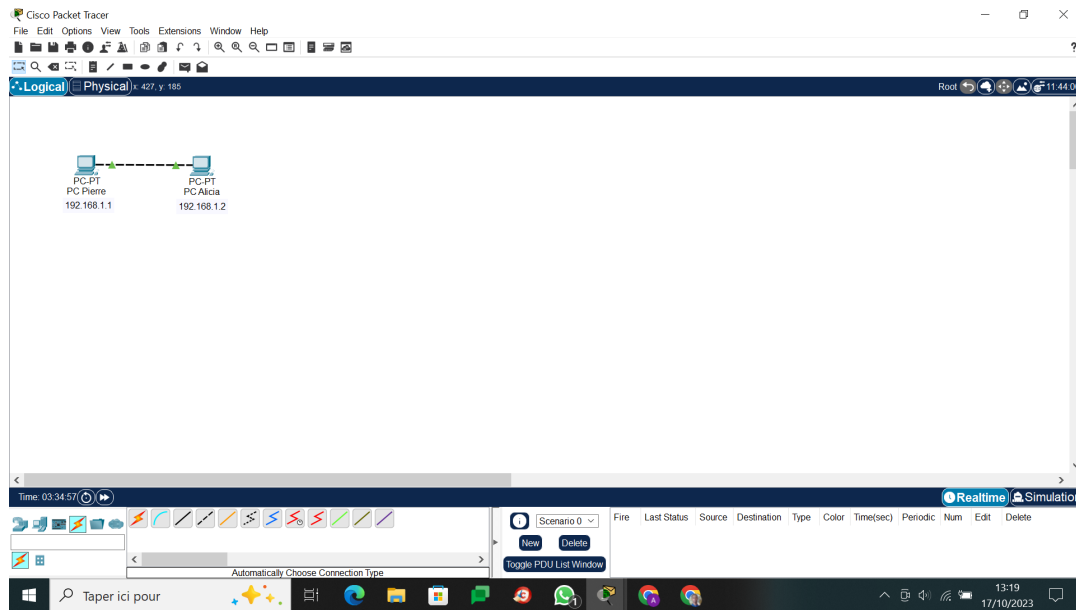
Qu'est-ce qu'une adresse MAC?

Une adresse MAC, parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire.

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

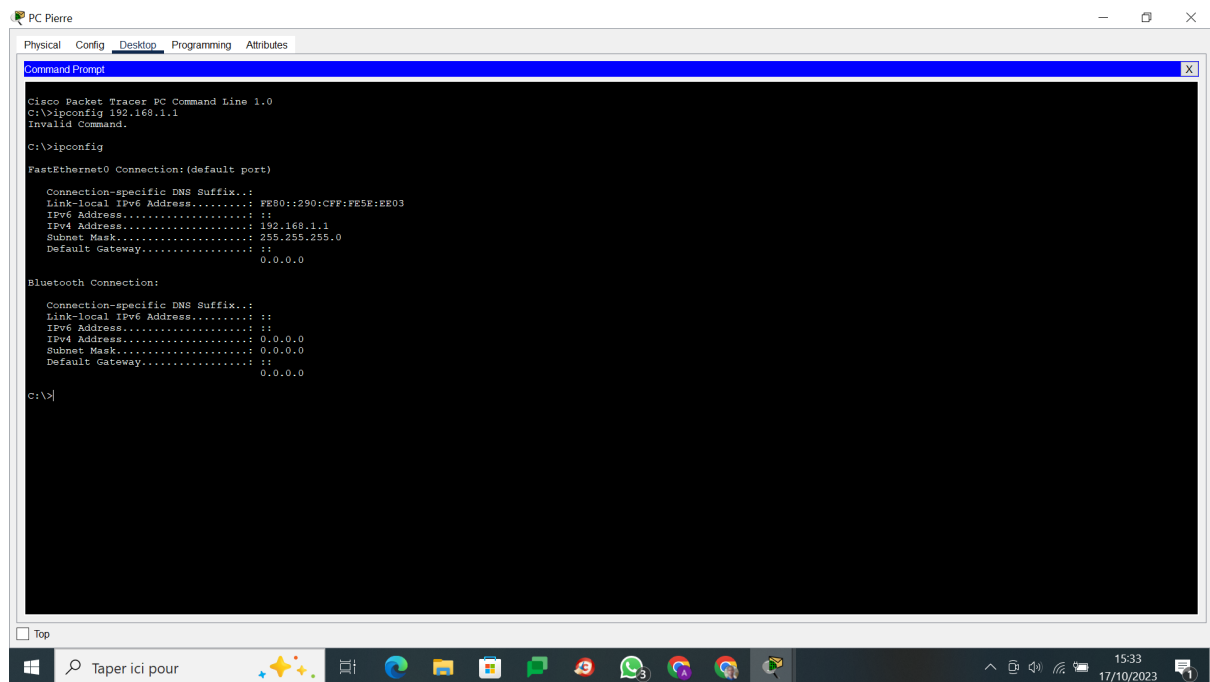
Une adresse IP publique vous identifie auprès du réseau Internet, de telle sorte que toutes les informations que vous recherchez puissent vous retrouver. Une adresse IP privée est

utilisée à l'intérieur d'un réseau privé pour établir une connexion sécurisée à d'autres appareils du réseau.

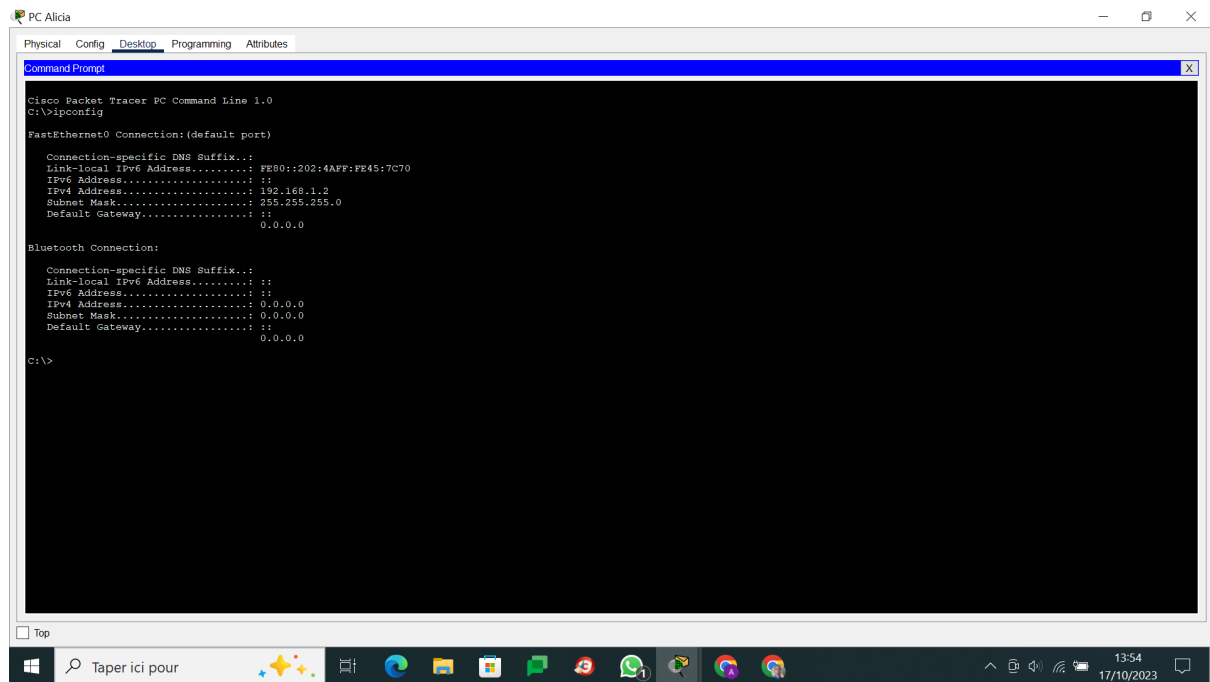


JOB 05:

PC Pierre,



PC Alicia,



```
PC Alicia
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:4AFF:FE45:7C70
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::

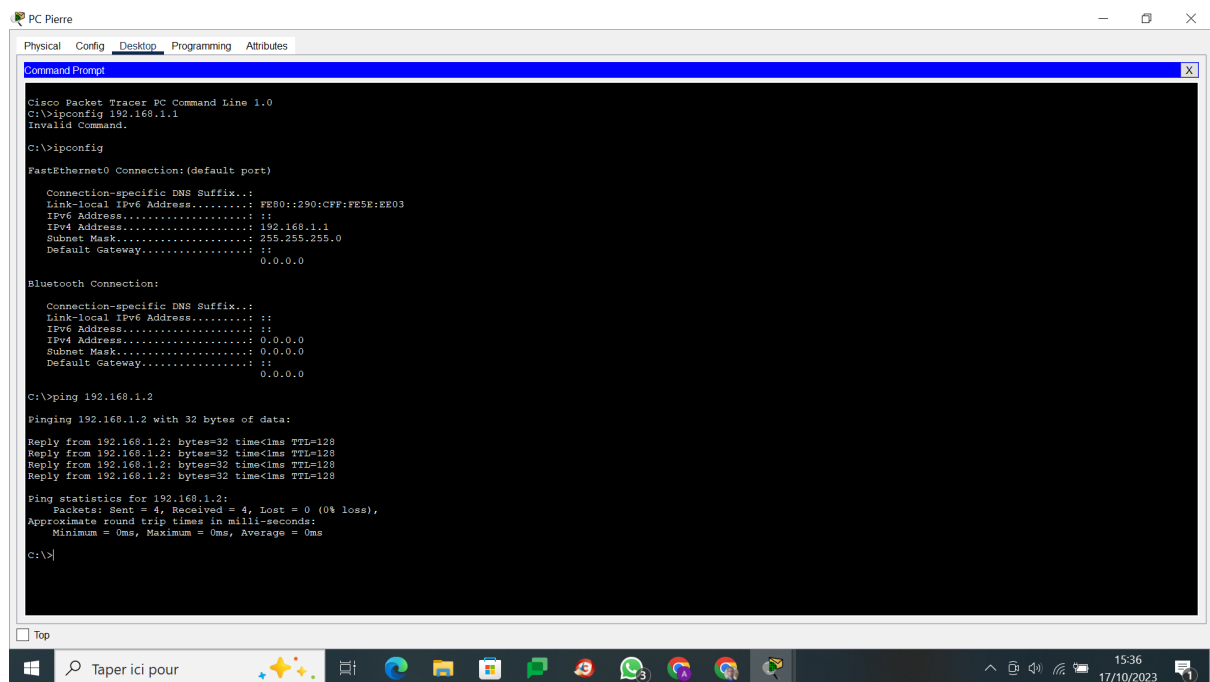
Bluetooth Connection:

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

C:\>
```

Pour justifier l'IP des machines, j'ai utilisé la ligne de commande "ipconfig".

JOB 06:



```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig 192.168.1.1
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::290:CFE:FE5E:EE03
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.1
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::

Bluetooth Connection:

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

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

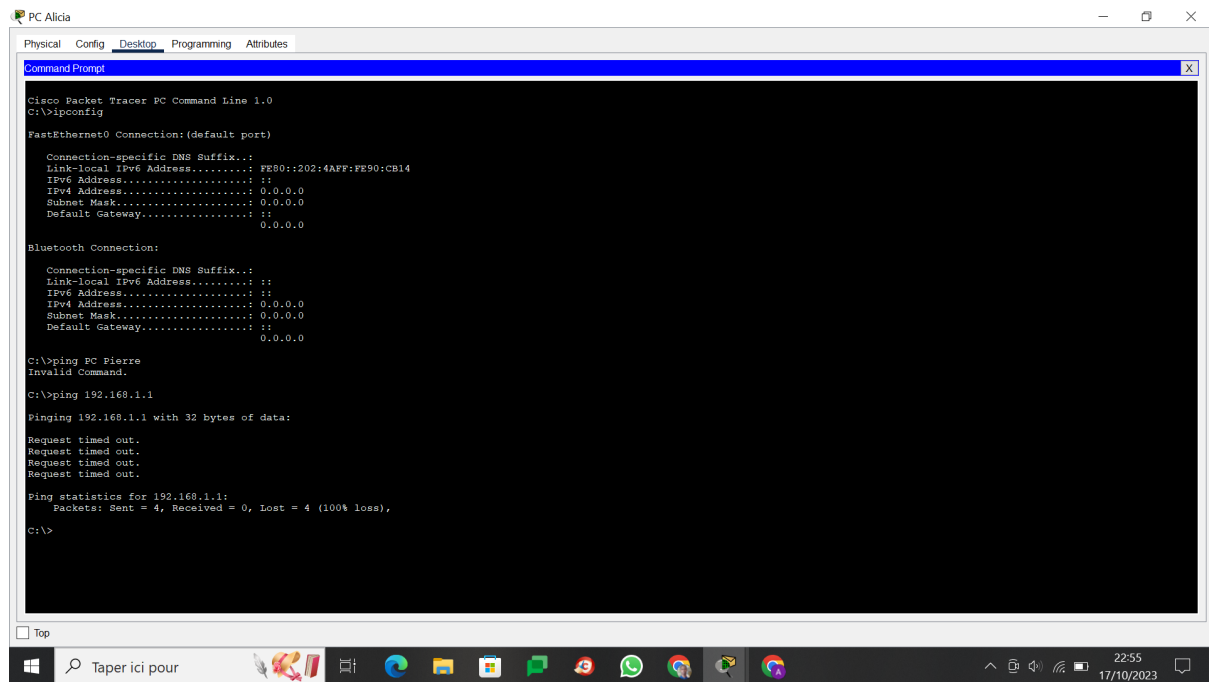
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

On a utilisé la commande ping <l'adresse ip> d'Alicia dans le PC de Pierre.

JOB 07:



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

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::202:4AFF:FE90:CB14
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::

Bluetooth Connection:

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

C:\>ping PC Pierre
Invalid Command.

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:\>
```

Non.

Vu les résultats du ping, cela signifie que le PC Pierre n'a pas reçu les paquets envoyés par Alicia. Car on a éteint le PC de Pierre.

JOB 08:

Différence entre un hub et un switch :

- Un hub est un dispositif simple qui agit comme un amplificateur de signal. Il transmet les données qu'il reçoit sur tous ses ports à tous les autres ports, ce qui signifie que les données sont diffusées à tous les appareils connectés. Un hub fonctionne au niveau de la couche physique du modèle OSI.
- Un switch, en revanche, est plus avancé. Il possède une table de correspondance d'adresses MAC, ce qui lui permet de transmettre les données uniquement vers le port approprié. Cela réduit le trafic inutile sur le réseau par rapport à un hub, offrant ainsi de meilleures performances.

Fonctionnement d'un hub, ses avantages et ses inconvénients :

Un hub transmet simplement les données qu'il reçoit à tous les périphériques connectés. Son principal avantage est sa simplicité et son coût peu élevé. Cependant, l'utilisation d'un hub peut entraîner des collisions de données, des goulots d'étranglement et des performances réseau médiocres.

Avantages et inconvénients d'un switch :

Les switches améliorent les performances réseau en transmettant les données uniquement là où elles doivent aller. Ils réduisent les collisions et les congestions. De plus, les switches permettent des communications simultanées entre plusieurs ports. Cependant, les switches sont généralement plus chers que les hubs.

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

Les switches utilisent une table de correspondance d'adresses MAC pour diriger le trafic uniquement vers le port approprié. Lorsqu'un paquet de données arrive, le switch vérifie l'adresse MAC de destination et transmet le paquet uniquement au port connecté à cet appareil spécifique, réduisant ainsi le trafic inutile sur le réseau. Cela permet des transferts de données plus efficaces et réduit les collisions.

JOB 09:

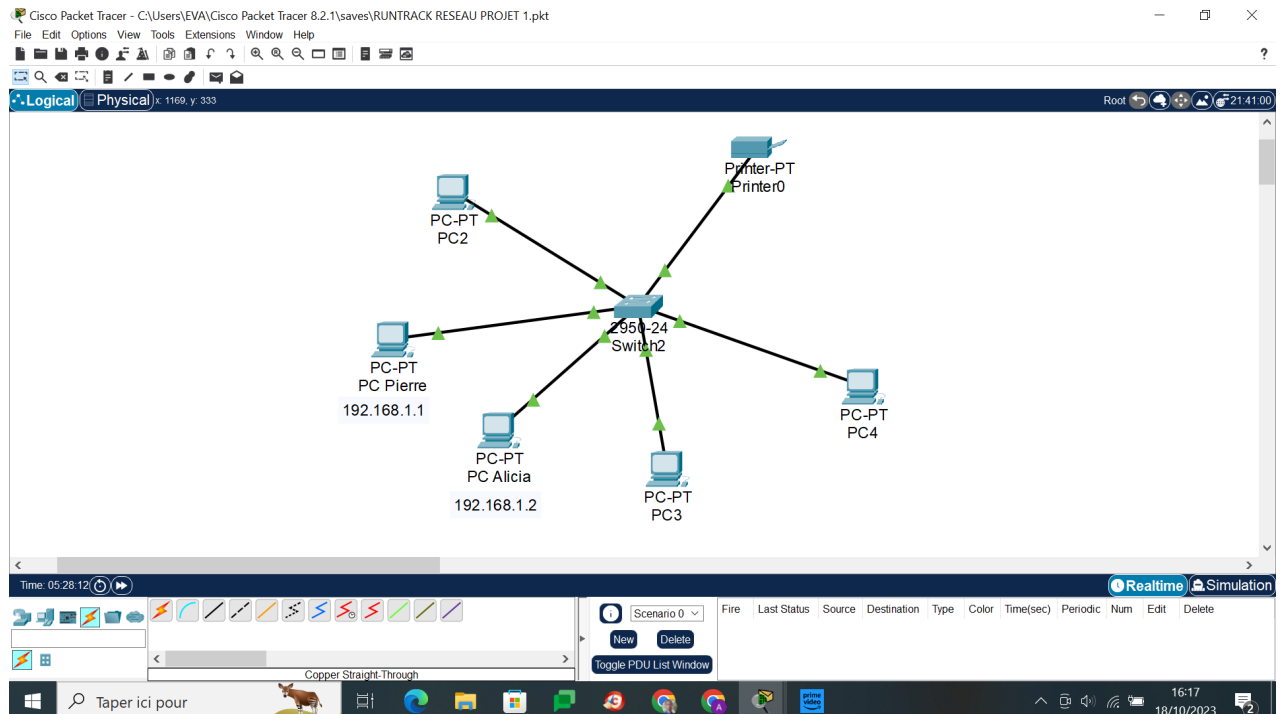
3 avantages d'avoir un schéma;

Compréhension globale du réseau : Un schéma de réseau clairement défini offre une vision globale de l'infrastructure, des connexions et des composants, ce qui facilite la compréhension de la configuration générale du réseau.

Dépannage facilité : En cas de problème, un schéma de réseau peut servir de référence précieuse pour localiser rapidement les problèmes de connexion, de matériel ou de configuration. Cela permet un dépannage plus efficace et rapide.

Planification et expansion : Un schéma de réseau bien documenté permet de planifier de manière stratégique les mises à niveau et les extensions du réseau. Il fournit une base solide pour évaluer les besoins futurs en matière d'infrastructure et de connectivité.

Schéma:



JOB 10:

Une adresse IP statique est une adresse réseau qui est attribuée manuellement à un périphérique, ce qui signifie qu'elle ne change pas, sauf si elle est modifiée manuellement. Cela signifie que chaque fois qu'un périphérique se connecte à un réseau, il conserve la même adresse IP. Les adresses IP statiques sont généralement utilisées pour les serveurs, les imprimantes réseau, les routeurs ou tout autre périphérique qui doit être accessible en permanence sous une même adresse.

D'autre part, une adresse IP attribuée par DHCP (Dynamic Host Configuration Protocol) est une adresse réseau attribuée automatiquement par un serveur DHCP à un périphérique lorsqu'il se connecte au réseau. L'attribution se fait de manière dynamique et peut changer à chaque fois que le périphérique se reconnecte au réseau. Cela signifie que les périphériques n'ont pas d'adresse IP fixe et peuvent se voir attribuer des adresses différentes à chaque connexion.

JOB 11:
Définissez le plan d'adressage.

Types de sous-réseaux	Nombres d'hôtes	Nombres de bits de sous-réseau	Masque de sous-réseau	Plage d'adresses
1*12 hôtes	12	4	255.255.255.240	10.0.0.0 - 10.0.0.15
5*30 hôtes	30	5	255.255.255.224	10.0.0.16 - 10.0.0.47
5*120 hôtes	120	7	255.255.255.128	10.0.0.48 - 10.0.0.175
5*160 hôtes	160	8	255.255.255.0	10.0.0.176 - 10.0.0.255

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

L'adresse 10.0.0.0 de classe A a été choisie parce qu'elle offre une plage d'adresses IP suffisamment grande pour accommoder les exigences de l'ensemble des sous-réseaux sans avoir à empiéter sur d'autres classes d'adresses. La classe A fournit 8 bits pour le réseau, ce qui donne une capacité de 2^{24} adresses IP.

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

Adresses IPv4 de classe A : Elles sont utilisées pour les grands réseaux car elles offrent un grand nombre d'adresses IP. Le premier octet représente le réseau, et les trois autres octets sont utilisés pour les hôtes.

Adresses IPv4 de classe B : Elles sont utilisées pour les réseaux de taille moyenne. Les deux premiers octets représentent le réseau, et les deux derniers octets sont utilisés pour les hôtes.

Adresses IPv4 de classe C : Elles sont utilisées pour les petits réseaux car elles offrent un nombre d'adresses IP limité. Les trois premiers octets représentent le réseau, et le dernier octet est utilisé pour les hôtes.

Adresses IPv4 de classe D : Elles sont utilisées pour le multicasting.

Adresses IPv4 de classe E : Elles sont réservées à des fins expérimentales et ne sont pas utilisées pour les réseaux publics.

JOB 12:

Voici le tableau détaillant les sept couches du modèle OSI avec une brève description de chaque couche et l'association des différents matériels ou protocoles :

Couche OSI	Description du rôle	Matériels ou protocoles associés
7. Application	Cette couche fournit des interfaces de communication pour les applications réseau.	HTTP, FTP, HTML, PPTP, SSL/TLS
6. Présentation	Elle gère la syntaxe et la sémantique des informations échangées entre les applications.	SSL/TLS, HTML
5. Session	Cette couche établit, gère et termine les connexions entre les applications.	SSL/TLS, PPTP
4. Transport	Elle assure la livraison des données de manière fiable et ordonnée entre les points de terminaison du réseau.	TCP, UDP
3. Réseau	Cette couche gère la connectivité logique et la sélection des chemins de transmission des données à travers le réseau.	IPv4, IPv6, routeur

2. Liaison de données	Elle fournit des moyens fiables pour transférer les données entre les entités du réseau, en détectant et en corrigeant les erreurs qui pourraient survenir dans la couche physique.	Ethernet, Wi-Fi, MAC
1. Physique	Cette couche définit les spécifications électriques, mécaniques, procédurales et fonctionnelles pour l'activation, le maintien et la désactivation des connexions physiques pour la transmission des bits.	Fibre optique, câble RJ45

En fonction de cette table, voici l'association des différents matériels ou protocoles aux couches respectives du modèle OSI :

- Ethernet : Couche 2 (Liaison de données)
- TCP : Couche 4 (Transport)
- MAC : Couche 2 (Liaison de données)
- Fibre optique : Couche 1 (Physique)
- PPTP : Couches 5 (Session) et 7 (Application)
- IPv4 : Couche 3 (Réseau)
- SSL/TLS : Couches 4 (Transport), 5 (Session) et 6 (Présentation)
- Wi-Fi : Couche 2 (Liaison de données)
- IPv6 : Couche 3 (Réseau)
- UDP : Couche 4 (Transport)
- FTP : Couche 7 (Application)
- Routeur : Couche 3 (Réseau)
- HTML : Couches 6 (Présentation) et 7 (Application)
- Câble RJ45 : Couche 1 (Physique)

JOB 13:

Avec un masque de sous-réseau 255.255.255.0, nous avons affaire à un réseau de classe C.

Voici les réponses aux questions posées :

Quelle est l'architecture de ce réseau ?

Ce réseau appartient à la classe C, ce qui signifie que les 24 premiers bits sont utilisés pour identifier le réseau et les 8 bits restants sont réservés pour les hôtes.

Indiquer quelle est l'adresse IP du réseau ?

Avec le masque de sous-réseau 255.255.255.0, l'adresse IP du réseau est obtenue en appliquant un "ET logique" entre l'adresse IP et le masque. Supposons que l'adresse IP soit de la forme X.X.X.Y, alors l'adresse réseau serait X.X.X.0.

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

Avec un masque de sous-réseau 255.255.255.0, le dernier octet (8 bits) est réservé pour les hôtes. Cela signifie qu'il y a $2^8 - 2 = 256 - 2 = 254$ adresses d'hôtes disponibles. La

soustraction de 2 est due à la réserve de l'adresse pour le réseau et de l'adresse de diffusion.

Quelle est l'adresse de diffusion de ce réseau ?

L'adresse de diffusion de ce réseau est l'adresse dans laquelle tous les bits d'hôtes sont définis sur 1. Pour un réseau de classe C avec un masque de sous-réseau 255.255.255.0, l'adresse de diffusion est obtenue en prenant l'adresse réseau (X.X.X.0) et en réglant tous les bits d'hôtes à 1, ce qui donne X.X.X.255.

JOB 14:

Pour convertir une adresse IP en binaire, nous devons d'abord convertir chaque octet (nombre entre les points) en binaire. Voici les conversions pour les adresses IP que vous avez données :

145.32.59.24 :

- 145 en binaire est 10010001
- 32 en binaire est 00100000
- 59 en binaire est 00111011
- 24 en binaire est 00011000

Ainsi, 145.32.59.24 en binaire est 10010001.00100000.00111011.00011000.

200.42.129.16 :

- 200 en binaire est 11001000
- 42 en binaire est 00101010
- 129 en binaire est 10000001
- 16 en binaire est 00010000

Par conséquent, 200.42.129.16 en binaire est 11001000.00101010.10000001.00010000.

14.82.19.54 :

- 14 en binaire est 00001110
- 82 en binaire est 01010010
- 19 en binaire est 00010011
- 54 en binaire est 00110110

Par conséquent, 14.82.19.54 en binaire est 00001110.01010010.00010011.00110110.

JOB 15:

Qu'est-ce que le routage?

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

Qu'est-ce qu'un gateway?

Une gateway désigne en informatique un dispositif matériel et logiciel qui permet de relier deux réseaux informatiques, ou deux réseaux de télécommunications, aux caractéristiques différentes.

Qu'est-ce qu'un VPN?

Le VPN est un service qui permet de connecter deux réseaux à travers un tunnel sécurisé.

Qu'est ce qu'un DNS?

Le DNS est une base de données qui associe des noms à des adresses IP.