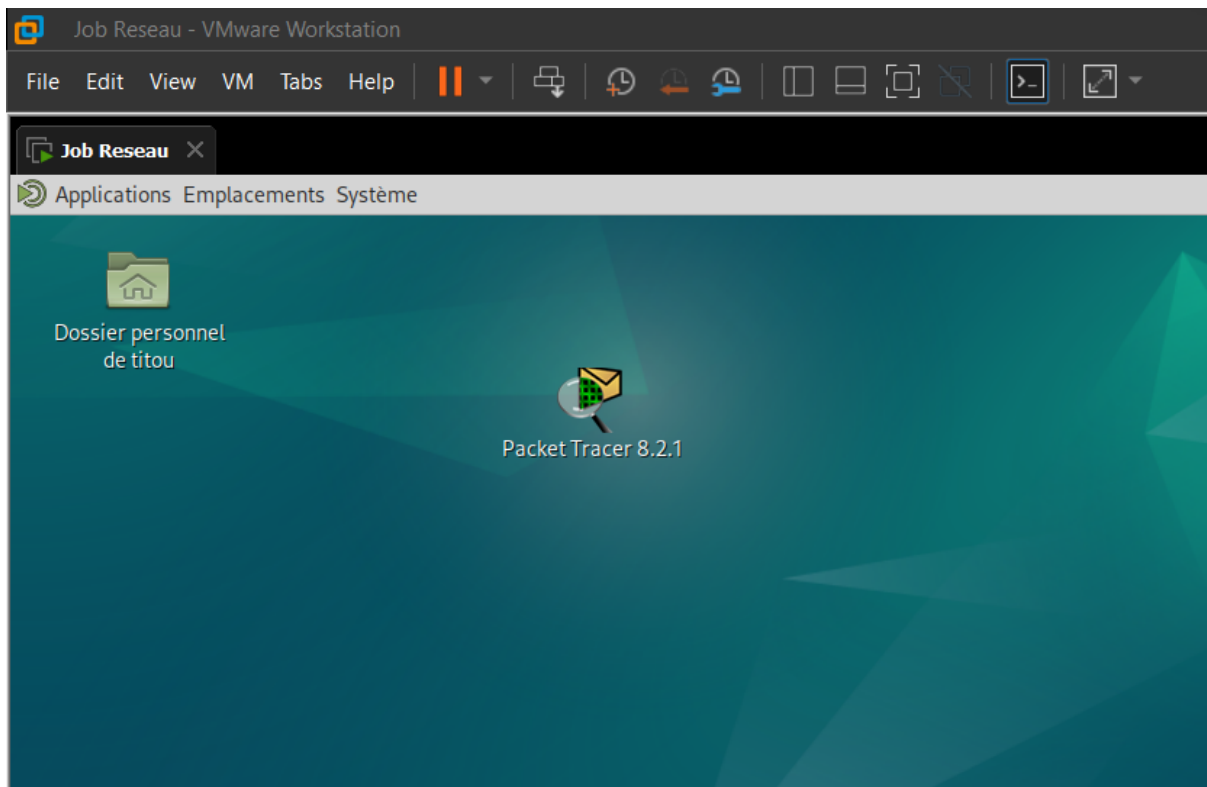


JOB 1:



J'ai du mettre à jour APT afin d'installer packet tracer sur mon nouveau clone de debian.

JOB 2:

→ Qu'est-ce qu'un réseau ?

C'est un ensemble d'[équipements](#) électroniques reliés entre eux pour échanger des informations. Il existe différents types de réseaux classés en fonction de leur emplacement géographique:

- LAN pour les réseaux locaux
- MAN réseaux métropolitain plus vaste que les LAN mais plus petit que les WAN ils peuvent couvrir une ville ou une métropole par exemple
- WAN réseaux étendues (internet est un exemple de WAN mondiale)
- WLAN réseaux sans fil sont des WAN qui utilise le wifi
- Réseaux cellulaires permettent la communication entre téléphones / tablettes

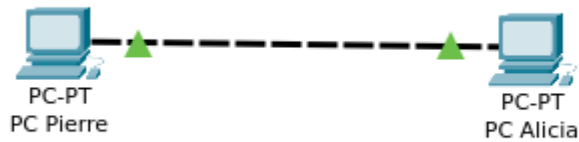
→ À quoi sert un réseau informatique ?

Un réseau informatique permet aux appareils de se connecter et de communiquer entre eux sans limites de distance, rapidement ce qui facilite donc le partage d'informations.

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

- Des périphériques : c'est ce qui sera connecté au réseau (ordinateurs, imprimantes, caméra, etc ...)
- Des dispositifs réseaux :
 - Routeurs : Ils permettent de diriger les informations vers l'extérieur du réseau internet par exemple
 - Hub ou Switches : ils permettent de relier plusieurs périphériques au sein d'un réseau local, leur permettant de communiquer entre eux
 - Points d'accès Wi-Fi : si besoin de connecter des périphériques sans fil
- Des câbles ethernet : pour connecter les périphériques et les dispositifs au réseau
- Des câbles d'alimentation : pour alimenter les différents composants de mon réseau
- Des infrastructures physiques : armoires de communication ou baies informatiques

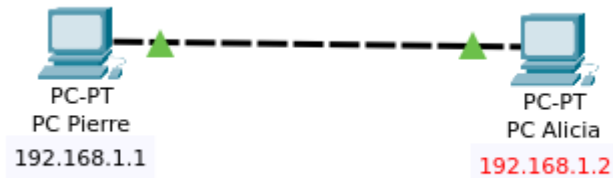
JOB 3:



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

J'ai choisi d'utiliser un câble croisé. Même si de nos jours les ordinateurs sont équipés de carte réseaux capable de s'adapter en fonction du câble utilisé, il est préférable d'utiliser un câble croisé lorsque l'on relie deux périphériques identiques. *Lorsque nous relions deux périphériques différents il est préférable d'utiliser un câble droit, car ces deux périphériques communiquent de façon complémentaire.*

JOB 4:



→ Qu'est-ce qu'une adresse IP ?

Cela veut dire Internet Protocol, il s'agit d'une sorte d'identité numérique attribuée à chaque périphérique. Il en existe deux types :

- Ipv4 composé de 4 groupes de chiffres séparés par des points. Chaque groupe de chiffres allant de 0 à 255.
- Ipv6 notation en hexadécimale, beaucoup plus longue que l'ipv4, permettant d'avoir un nombre d'adresse unique très grand, elle est la réponse à la limitation du nombre d'adresse ipv4.

→ À quoi sert un IP ?

Cela sert à identifier et à localiser les différents périphériques connectés au réseau. Elles permettent également l'échange de données entre les différents appareils, similaire à une adresse postale dans le monde physique.

→ Qu'est-ce qu'une adresse MAC ?

"Media access Control", c'est une adresse unique attribuée à chaque carte réseau d'un appareil. Contrairement à l'adresse ip qui est gérée par un logiciel, l'adresse mac est intégrée directement au matériel, elle est donc unique. Elle est composée de 12 caractères chiffres ou lettres, regroupés par pair.

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

L'ip publique est l'adresse visible depuis l'extérieur du réseau, elle est unique et utilisée par les serveurs web pour nous envoyer des données. L'ip privée quant à elle n'est pas accessible depuis internet et permet d'identifier les appareils au sein d'un réseau local.

→ Quelle est l'adresse de ce réseau ?

192.168.1.0

JOB 5:

PC Pierre	PC Alicia
Physical Config <u>Desktop</u> Programming Attributes	Physical Config <u>Desktop</u> Programming Attributes
Command Prompt	Command Prompt
<pre>Cisco Packet Tracer PC Command Line 1.0 C:\>ip config Invalid Command. C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Link-local IPv6 Address.....: FE80::204:9AFF:FE8 IPv6 Address.....: :: IPv4 Address.....: 192.168.1.1 Subnet Mask.....: 255.255.255.0 Default Gateway.....: :: 0.0.0.0 Bluetooth Connection: Connection-specific DNS Suffix.: Link-local IPv6 Address.....: :: IPv6 Address.....: :: IPv4 Address.....: 0.0.0.0 Subnet Mask.....: 0.0.0.0 Default Gateway.....: :: 0.0.0.0 C:\></pre>	<pre>Cisco Packet Tracer PC Command Line 1.0 C:\>ipconfig FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Link-local IPv6 Address.....: FE80::202:17FF:FE2 IPv6 Address.....: :: IPv4 Address.....: 192.168.1.2 Subnet Mask.....: 255.255.255.0 Default Gateway.....: :: 0.0.0.0 Bluetooth Connection: Connection-specific DNS Suffix.: Link-local IPv6 Address.....: :: IPv6 Address.....: :: IPv4 Address.....: 0.0.0.0 Subnet Mask.....: 0.0.0.0 Default Gateway.....: :: 0.0.0.0 C:\></pre>

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

Commande "ipconfig"

JOB 6:

```
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:\>|
```

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

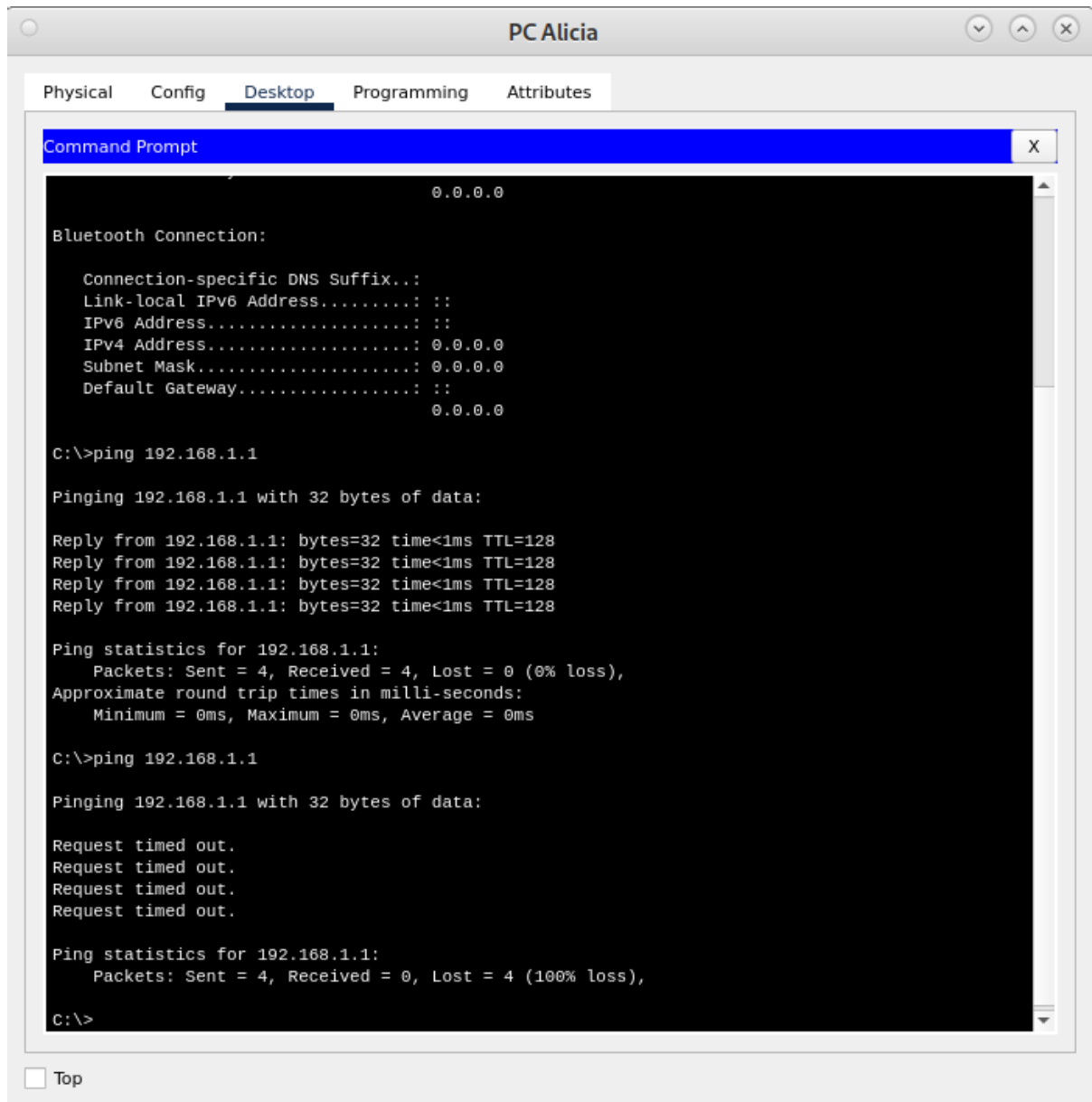
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|
```

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

Commande "ping"

JOB 7:



```
PC Alicia
Physical  Config  Desktop  Programming  Attributes

Command Prompt

0.0.0.0

Bluetooth Connection:

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

C:\>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
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
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:\>
```

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

Non

→ Expliquez pourquoi.

Le pc de Pierre était éteint donc sa carte réseau non alimentée, il n'était donc pas connecté au pc d'Alicia.

JOB 8:

```
PC Pierre
Physical Config Desktop Programming Attributes
Command Prompt
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:\>
ping 192.168.1.6
Pinging 192.168.1.6 with 32 bytes of data:
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=6ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.6:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms
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=5ms 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 = 5ms, Average = 1ms
C:\>

PC7
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
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:\>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:\>
```

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

Un hub est un répéteur, il reçoit des données, et les transferts à tous ses autres ports, tous les appareils reçoivent donc les données qu'il soit concerné ou pas par celles-ci. Un switch quant à lui est capable de reconnaître les adresses mac connectés à ses ports, de ce fait lorsqu'il reçoit des données il est capable de reconnaître le destinataire et d'envoyer les données uniquement à celui-ci.

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

Il est peu coûteux et simple d'utilisation mais comme dit précédemment le hub reçoit des informations et les envoi à tous ses ports via la bande passante. De plus, tous les ports ont la même bande passante, ce qui a pour conséquence de le rendre moins performant dans le traitement des données et la gestion du trafic. En termes de sécurité, toutes les données circulent en clair sur tous les ports, ce qui est problématique et fortement déconseillé dans un environnement où la confidentialité est importante.

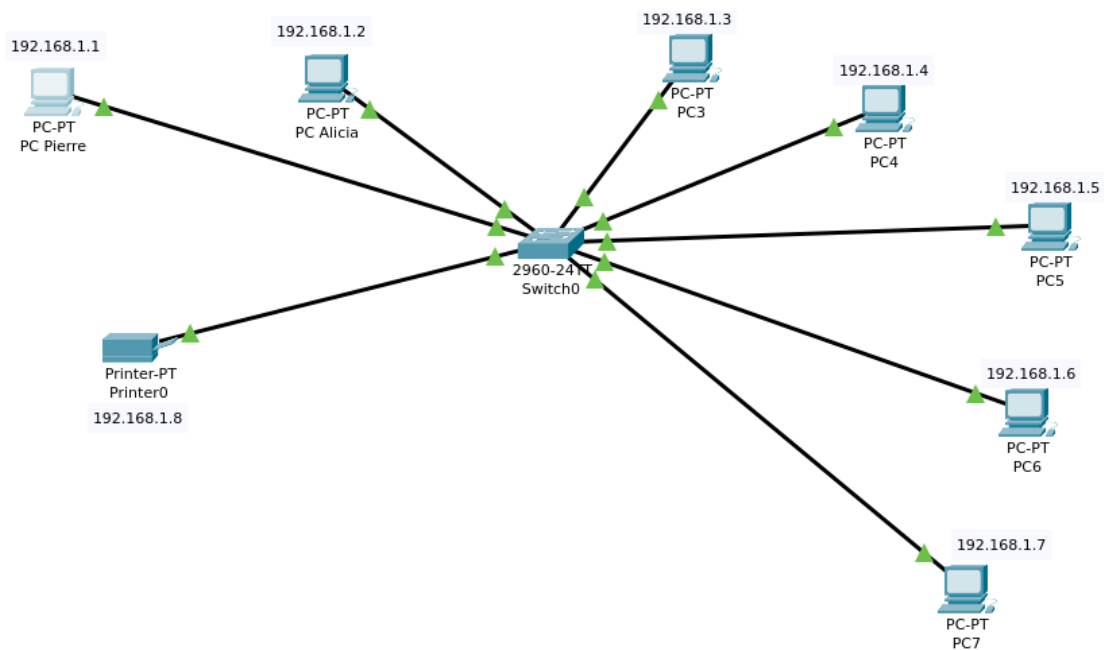
→ Quels sont les avantages et inconvénients d'un switch ?

Chaque port à sa propre bande passante dédiée tous les appareils peuvent donc communiquer à pleine vitesse, ceci est rendu possible par le fait qu'il transmet les données uniquement ou cela est nécessaire, le transfert est donc plus rapide et efficace. Pour la sécurité, une fois de plus l'identification du destinataire permet plus de confidentialité. Bien que les switches soit préférés au hub dans la majeure partie des cas, ils restent tout de même plus complexes à configurer, plus chère à l'achat et surtout limités en termes de port. Ils nécessitent des compétences techniques plus avancées en cas de saturation du réseau ou de panne.

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

Lorsqu'un switch reçoit une trame de données, il examine l'en-tête de la trame pour extraire l'adresse MAC source et la mémoriser. Il utilise ensuite sa table de commutation pour associer cette adresse MAC à un port spécifique. Ainsi, il sait quel port est connecté à quel appareil. Lorsqu'il reçoit une autre trame avec une adresse MAC de destination, il utilise cette table pour déterminer quel port doit être utilisé pour transmettre la trame.

JOB 9:

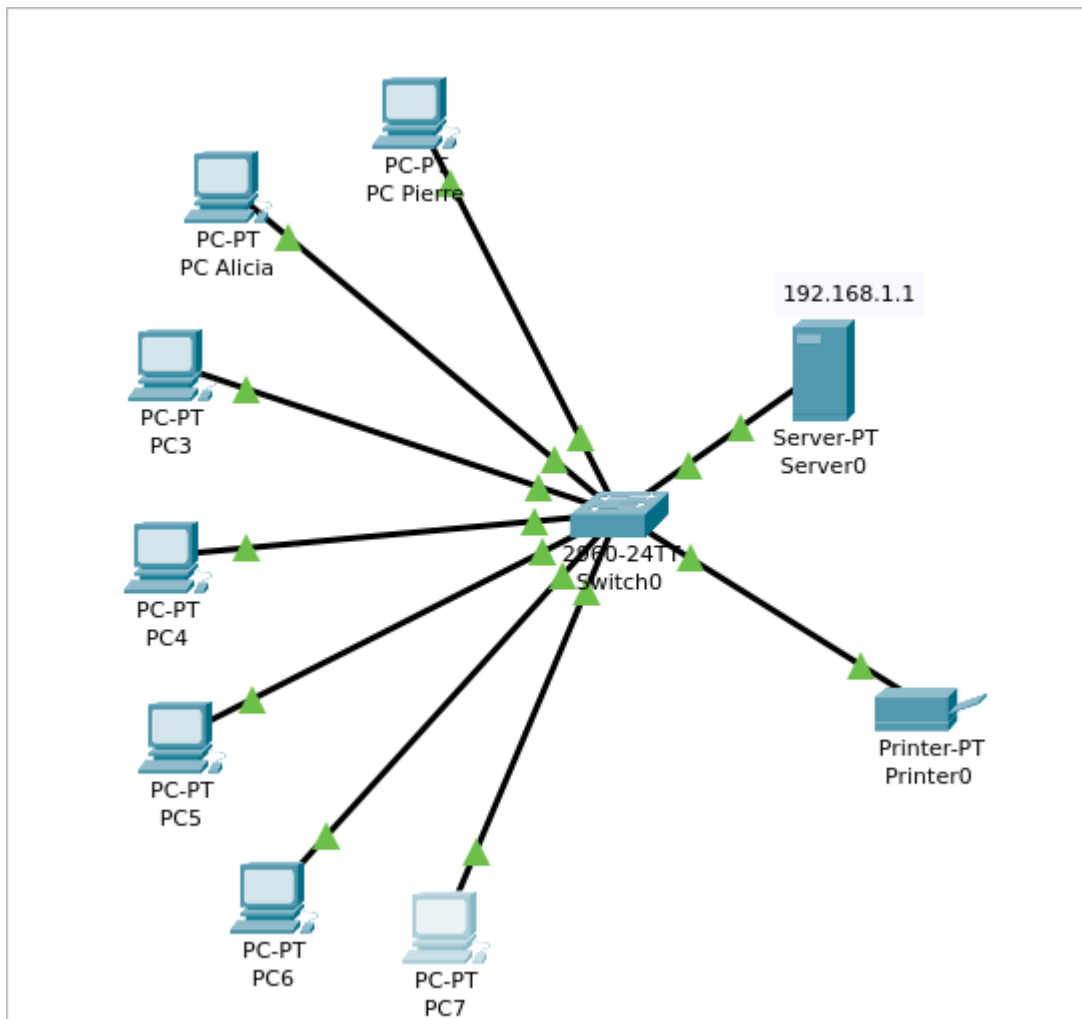


→ identifiez au moins trois avantages importants d'avoir un schéma

- **Une visualisation du réseau claire**, un schéma du réseau permet d'un rapide coup de connaître l'ensemble des composants qui composent le réseau et de comprendre comment les appareils sont connectés et communiquent entre eux.
- **Planification et conception du réseau**, un schéma permet d'avoir une vision du réseau dans son ensemble, ce qui a pour avantage de planifier l'emplacement des composants, les connexions et composants nécessaires à sa réalisation.
- **Identifications des composants**, un schéma permet de connaître les périphériques dont nous avons besoin lors de sa mise en place physique et ainsi éviter les oublis.

Dans l'ensemble il s'agit une étape cruciale de la conception au dépannage, cela facilite la visualisation, la planification et l'optimisation de celui-ci pour le dépannage ou pour l'étendre si cela s'avère nécessaire. Le schéma fait partie intégrante de la documentation informatique de notre réseau.

JOB 10:



Server0

Physical Config Services **Desktop** Programming Attributes

IP Configuration X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 192.168.1.1

IPv6 Configuration

Server0

Services
Desktop
Programming
Attributes

DHCP

Interface FastEthernet0

Pool Name serverPool

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Start IP Address : 192 168 1 2

Subnet Mask: 255 255 255 0

Maximum Number of Users : 254

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Service ☒ On ☐ Off

Add
Save
Remove

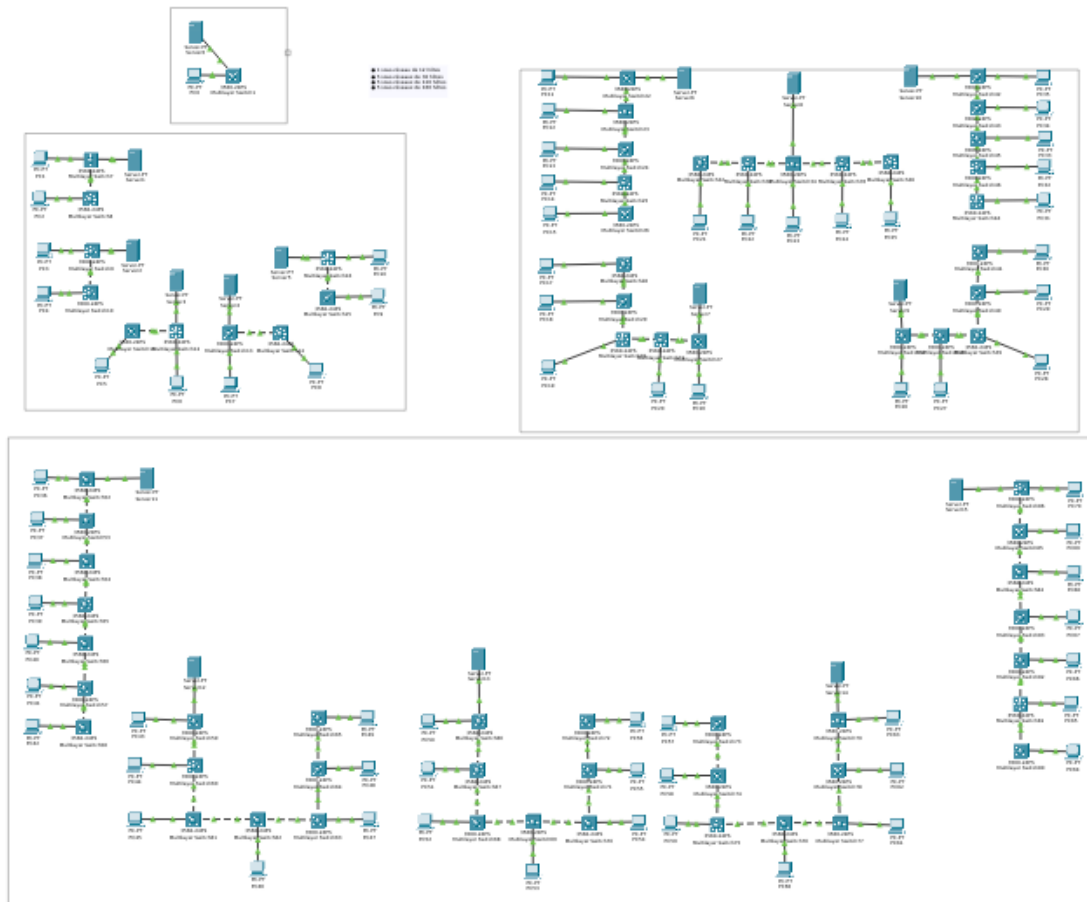
Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
serverPool	0.0.0.0	0.0.0.0	192.16...	255.25...	254	0.0.0.0	0.0.0.0

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

L'adresse ip statique est attribuée manuellement pour chaque appareil par l'administrateur réseau, elle restera inchangée tant que l'admin ne la modifie pas. Elle offre de la stabilité puisque le périphérique conserve toujours la même adresse, cependant il peut y avoir risque de conflit si cette même adresse est attribuée à un autre périphérique par erreur de l'admin ou par l'utilisation d'un DHCP.

L'adresse ip DHCP est attribuée par un serveur du même nom sur le réseau. Elles peuvent changer à chaque nouvelle connexion de l'appareil sur le réseau. Le serveur est conçu pour éviter les conflits d'adresse, il surveille les adresses déjà attribuées en et s'assure qu'elle ne soit pas de nouveau utilisée. Il facilite grandement la gestion d'adresse dans les grands réseaux, ou la configuration manuelle de chaque appareils serait fastidieuse et sujette aux erreurs pour l'administrateur réseau.

JOB 11:



Chaque serveur a pour adresse 10.0.X.1, ou "X" varie de 0 à 15 selon le sous réseau auquel il est affecté !

Le masque de sous réseau a été modifié en fonction du nombre d'utilisateurs demandé par chaque sous réseau:

- 255.255.255.240 pour 12 utilisateurs
- 255.255.255.224 pour 30 utilisateurs
- 255.255.255.128 pour 120 utilisateurs
- 255.255.255.0 pour 160 utilisateurs

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

La classe A a un masque de sous réseau par défaut 255.0.0.0 permettant ainsi d'avoir beaucoup de périphériques sur le réseau. De plus, il est possible d'allouer plus de bit d'hôtes en sous-réseaux, dans notre cas nous avons changé le masque de sous-réseau en fonction du nombre d'hôtes sur le sous-réseau concerné. Au vu de sa capacité d'accueil ce type d'adresse est particulièrement adaptées au réseau très vastes comme ceux utilisés par les grandes entreprises

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

Chaque classe a sa propre plage d'adresses, plage conçue pour répondre à des besoins spécifiques selon le réseau. C'est le premier groupe de chiffres qui varie, permettant plus ou moins en fonction de la classe un nombre d'hôtes sur le réseau. Elles sont au nombre de 5, **A (premier octet 0)** pour les grandes organisations, **B (premier octet 10)** adaptées au réseau de taille moyenne, **C (premier octet 1110)** pour les réseaux locaux, **D (premier octet 11110)** réserver à la diffusion de données et **E (premier octet 11111)** pour la recherche.

JOB 12:

Définitions :

Le modèle OSI (Open Systems Interconnection) est un cadre conceptuel qui définit comment les systèmes réseau communiquent et envoient des données d'un expéditeur à un destinataire.

Le modèle est utilisé pour décrire chaque composant de la communication de données pour pouvoir établir des règles et des normes pour les applications et l'infrastructure du réseau. Sans le modèle OSI, il n'y aurait pas de méthode standard pour concevoir l'infrastructure et les protocoles utilisés pour la communication : il serait donc plus difficile pour les administrateurs d'installer de nouveaux équipements et de les intégrer à des réseaux autres que le leur. Grâce à ces normes, les administrateurs peuvent concevoir leur propre infrastructure, mais l'équipement peut toujours communiquer avec les autres de manière universelle.

Le modèle OSI contient sept couches qui s'empilent conceptuellement. Chacune représentant un niveau de fonctionnalité distinct dans la communication entre les ordinateurs. Chaque couche communique avec les couches adjacentes par des interfaces normalisées.

Le Modèle OSI "Open Systems Interconnection"		
Les Couches	Description	Matériels / Protocoles
Physique	<p>Comme son nom l'indique, la couche physique est responsable de l'équipement qui facilite le transfert des données, comme les câbles et les routeurs installés sur le réseau.</p> <p>Cette couche est l'un des aspects de la transmission réseau où les normes sont essentielles. Sans normes, la transmission entre les appareils de différents fabricants est impossible.</p>	<p>Ethernet Cable RJ45 Fibre Optique Wi-Fi Routeur</p>
Liaisons des données	<p>Cette couche gère la communication entre des appareils connectés directement sur le même réseau local.</p> <p>La couche liaison de données transforme les paquets reçus de la couche réseau en trames. Tout comme la couche réseau, la couche liaison de données est responsable du contrôle des erreurs et du flux pour garantir la réussite de la transmission.</p>	MAC
Réseau	<p>La couche réseau gère le routage des données à travers des réseaux interconnectés. Elle est responsable de l'acheminement des paquets de données entre différents réseaux, en utilisant des adresses IP.</p> <p>Elle est chargée de décomposer les données sur l'appareil de l'expéditeur et de les réassembler sur l'appareil du destinataire lorsque la transmission s'effectue sur deux réseaux différents.</p> <p>Lorsque l'on communique au sein d'un même réseau, la couche réseau est inutile, mais la plupart des utilisateurs se connectent à d'autres réseaux, tels que les réseaux dans le cloud.</p> <p>Lorsque les données traversent différents réseaux, la couche réseau est chargée de créer de petits paquets de données acheminés vers leur destination, puis reconstruits sur l'appareil du destinataire.</p>	<p>IPv4</p> <p>IPv6</p>

Transport	<p>La couche transport est chargée de prendre les données et de les décomposer en petits morceaux.</p> <p>Lorsque des données sont transférées sur un réseau, elles ne sont pas transférées en un seul paquet.</p> <p>Pour rendre les transferts plus efficaces et plus rapides, la couche transport divise les données en segments plus petits. Ces petits segments contiennent des informations d'en-tête qui peuvent être réassemblées sur le périphérique cible.</p> <p>Les données segmentées sont également dotées d'un contrôle d'erreur qui indique à la couche session de rétablir une connexion si les paquets ne sont pas entièrement transférés au destinataire ciblé.</p>	<p>SSL/TLS</p> <p>UDP</p>
Session	<p>Pour communiquer entre deux appareils, une application doit d'abord créer une session, qui est unique à l'utilisateur et l'identifie sur le serveur distant.</p> <p>La couche session établit, maintient et synchronise les connexions entre les systèmes finaux.</p> <p>Par exemple, si 10 Mo de données sont transférés et que seuls 5 Mo sont complets, la couche session s'assure que seuls 5 Mo sont retransmis. Ce transfert rend la communication sur un réseau plus efficace au lieu de gaspiller des ressources et de transférer l'intégralité du fichier.</p>	<p>PPTP</p> <p>SSL/TLS</p>
Présentation	<p>Cette couche s'occupe de la représentation des données, assurant que les données sont converties, si nécessaire, en un format compréhensible pour les deux parties.</p> <p>Par exemple, la communication avec un serveur Web via HTTPS utilise des informations chiffrées. La couche de présentation est responsable de l'encodage et du décodage des informations afin qu'elles puissent être affichées en clair.</p> <p>La couche de présentation est également responsable de la compression et de la décompression des données lorsqu'elles passent d'un appareil à un autre.</p>	<p>TCP</p>

Application	<p>La couche application est la couche la plus proche de l'utilisateur final. Elle fournit des interfaces pour les applications utilisateur et des services réseau tels que le courrier électronique, le transfert de fichiers, la navigation web, etc.</p> <p>Par exemple, un client de messagerie qui transfère des messages entre le client et le serveur fonctionne sur la couche 7. Lorsqu'un message est reçu sur le logiciel client, c'est la couche application qui le présente à l'utilisateur.</p>	<p>FTP</p> <p>HTML</p>
-------------	--	------------------------

JOB 13:

→ Quelle est l'architecture de ce réseau ?

Ceci est un réseau de type LAN

→ Indiquer quelle est l'adresse IP du réseau ?

Convertissons d'abord une des adresses du réseau ainsi que le masque de sous réseau, en binaire et réalisons un "E logique" afin de déterminer à quel réseau elle appartient

Pour ce faire il suffit d'ajouter l'ip au masque de sous réseau avec 3 possibilités:

- 1 et 1 = 1
- 1 et 0 = 0
- 0 et 0 = 0

IP: 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 0 0 0 0

Masque : 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 1 1 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0

ELog : 1 1 0 0 0 0 0 0 . 1 0 1 0 1 0 0 0 . 0 0 0 0 1 0 1 0 . 0 0 0 0 0 0 0 0

Nous traduisons l'E logique pour obtenir l'adresse ip de ce reseau qui est donc 192.168.10.0

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

Ici nous séparons les 1 qui correspondent au réseau des 0 qui correspondent aux hôtes dans le masque de sous-réseau. Nous prenons le nombre de zéro donc ici 8.

Nous élevons 2 à la puissance du nombre de zéro, pour obtenir 256.

Puis nous retirons 2 qui correspond au 0 (adresse du réseau) et 255 (adresse de broadcast), pour obtenir 254.

Il y a donc 254 machines qui peuvent se brancher sur ce réseau.

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

Il s'agit de la dernière adresse dites "broadcast" soit 192.168.10.255

JOB 14:

- 145.32.59.24 = 10010001.00100000.00111111.00011000
- 200.42.129.16 = 11001000.00101010.10000001.00010000
- 14.82.19.54 = 00001110.01010010.00010001.00110110

JOB 15:

→ Qu'est-ce que le routage ?

Le routage fait référence au processus de sélection du chemin optimal pour faire passer des données d'un point à un autre à travers un réseau. Il s'agit essentiellement de prendre des décisions sur la manière de faire circuler les paquets de données entre les différents nœuds (comme les routeurs) d'un réseau.

→ Qu'est-ce qu'un gateway ?

Une passerelle, souvent appelée "gateway" en anglais, est un périphérique ou un logiciel qui agit comme une interface entre deux réseaux différents, permettant ainsi la communication entre eux. C'est un élément essentiel pour connecter et faire communiquer des réseaux qui utilisent des technologies différentes. Elle assure le transfert de données entre ces réseaux, en veillant à ce que les informations soient correctement acheminées vers leur destination. Les routeurs et les NAT sont des exemples de gateway.

→ Qu'est-ce qu'un VPN ?

Un VPN, ou Réseau Privé Virtuel en français, est une technologie qui permet de créer un réseau sécurisé et chiffré au-dessus d'un réseau public, comme Internet. Il offre plusieurs avantages, notamment la confidentialité, la sécurité et l'accès à distance aux ressources d'un réseau privé.

→ Qu'est-ce qu'un DNS ?

Un DNS, ou Domain Name System, est un système essentiel qui permet de traduire les noms de domaine conviviaux (comme www.example.com) en adresses IP numériques (comme 192.0.2.1) utilisées par les ordinateurs pour communiquer sur un réseau. Il simplifie l'accès à Internet en utilisant des noms de domaine conviviaux au lieu de devoir mémoriser des adresses IP numériques de plus il joue un rôle central dans le fonctionnement fluide d'Internet.