Job 01:

On commence par se créer un compte Cisco.
Étant sous Debian 12, je télécharge le paquet .deb, puis exécute dpkg afin de l'installer.
Il manque de dépendances, alors j'exécute sudo apt install -f (option qui sert à **f**ix les problèmes d'installation, ici de dépendances).
Voilà, je lance packet tracer avec la commande packettracer.

Job 02:

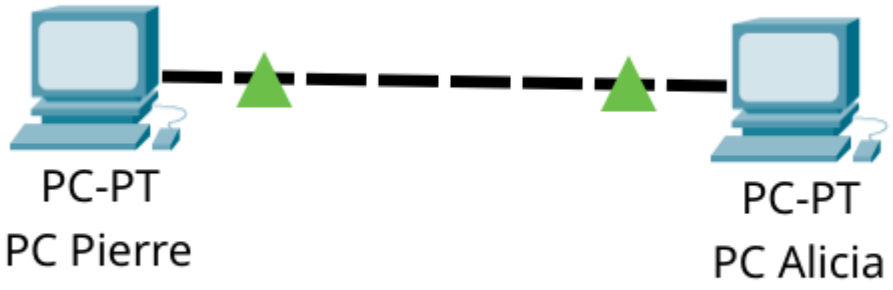
Un réseau désigne un ensemble d'entités connectées entre elles et pouvant échanger des informations. L'analogie la plus courante est celle de la toile d'araignée: chaque noeud du réseau correspond à l'intersection d'un fil, et chaque fil correspond à une liaison où peuvent circuler des ressources.
Un réseau peut être physique, entre des personnes, comme dans un groupe d'amis par exemple, ou "virtuel" (bien que les liaisons soient bien physiques et tangibles), comme un réseau informatique.
Un réseau informatique est donc plus particulièrement un ensemble d'équipements informatiques pouvant communiquer entre eux.

Un réseau informatique sert à relier entre elles des machines informatiques, telles que des ordinateurs, des routeurs, des commutateurs, etc. Un réseau informatique s'organise généralement autour de ce qu'on appelle le modèle OSI, qui est une norme (à la fois théorique, pédagogique, et praticable) qui définit comment doit se structurer la communication entre divers éléments informatiques. Chaque élément d'un réseau informatique se doit, en bonne pratique, d'être relié à plusieurs autres, ou à un ou plusieurs noeuds importants par lesquels transiter pour avoir accès au reste du réseau, afin de garantir une décentralisation des données. Ainsi, si un élément devient hors-service, le réseau restera opérationnel et les données pourront continuer de transiter.

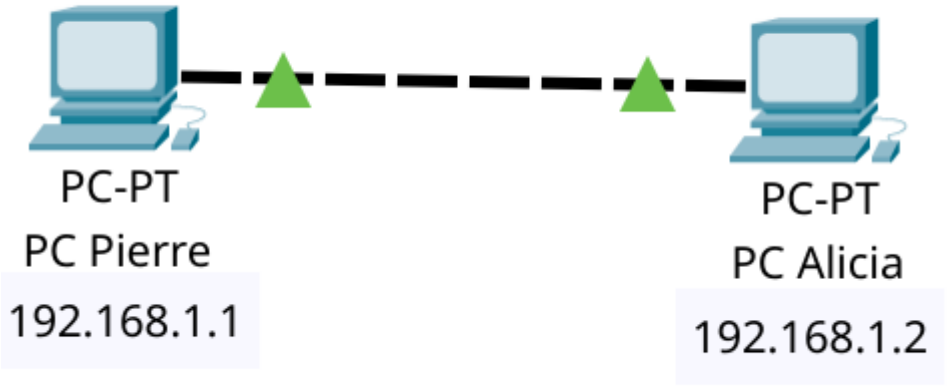
Pour constituer un réseau informatique, on aura besoin de plusieurs choses, que l'on peut mettre en parallèle avec la première couche du modèle OSI:
Des ordinateurs (comprendre aussi des serveurs), équipés de carte réseau ou d'un port RJ45 (par exemple), qui seront en mesure de recevoir et envoyer des données.
Des liaisons physiques, qu'elles soient par mouvements d'électrons dans des câbles (typiquement, des câbles RJ45), ou par ondes électromagnétiques (comme des ondes radio pour les protocoles Wi-Fi).
Des équipements permettant la transmission et la redirection (ou non) des trames tels que des switch ou hub.
D'équipements permettant la redirection du trafic vers d'autres réseaux distants, tels que des routeurs et des modems.
Notons qu'aujourd'hui les box fournies par les FAI (Fournisseurs d'Accès à Internet) contiennent à la fois des switch, des routeurs et des modems, et intègrent des services DHCP et DNS.

Job 03:

On crée deux ordinateurs, puis on les renomme en cliquant directement une fois sur leur nom.
Pour les connecter entre eux par câble, on utilise un câble croisé en cuivre (copper cross-over), étant donné que ces deux éléments informatiques sont similaires.
Si l'on avait voulu connecter un ordinateur à un switch, par exemple, nous aurions utilisé un câble droit (copper straight-through).



Job 04:



Une adresse ip (pour Internet Protocol), par analogie avec une adresse postale (malgré quelques divergences notables), est un identifiant unique d'un matériel informatique faisant partie d'un réseau utilisant ce protocol. Elle est attribuée plus particulièrement à l'interface réseau de la machine. Une machine avec plusieurs interfaces réseau aura donc plusieurs IP différentes. Une adresse IP pour être statique (attribuée à la main, processus complexe pour éviter les doublons au sein d'un réseau), ou dynamique (souvent attribuée à la machine par le routeur: la machine envoie une requête au serveur DHCP, pour Dynamic Host Configuration Protocol, qui indique à l'ordinateur quelle ip il pourra utiliser pendant sa connexion au réseau par le routeur).

À l'instar d'une adresse postale, une adresse IP sert à donner un identifiant unique à un ordinateur ou équipement informatique, afin que d'autres ordinateurs et équipements informatiques puissent le repérer et faire transiter des données jusqu'à lui, par un processus de routage.

Une adresse MAC (pour Media Access Control) est une adresse unique, statique, que chaque constructeur de carte réseau et/ou interface réseau quelconque attribue au composant. L'adresse MAC est modifiable au niveau logiciel, dans la configuration de l'ordinateur. L'utilitaire ip link sous Linux permet de le faire.
Une adresse MAC est généralement codée sur 6 octets, donc 48 bits.
L'adresse MAC est l'identifiant physique d'un ordinateur, ainsi, étant indépendante de l'endroit où l'on se trouve, et si l'adresse MAC est inchangée, il sera plus évident de traquer précisément un ordinateur particulier avec une adresse MAC qu'avec une adresse IP, ce dont plusieurs fabricants tels qu'Apple ou Microsoft ont maintenant contré en modulant les adresses MAC lors de la recherche de connexion/la connexion à un réseau.

La différence entre adresse IP publique et privée réside dans leur utilisation: une adresse IP privée sert aux éléments informatiques (ordinateurs, imprimantes, smartphones, objets connectés) d'un réseau à communiquer entre eux et/ou à avoir une identité auprès du routeur.
Une adresse IP publique sert à un élément informatique (le plus souvent un routeur) à avoir une identité auprès d'un réseau plus grand, comme Internet.
L'adresse IP publique est donc unique au sein de ce réseau, et sert donc à identifier, publiquement, à la fois le routeur et les périphériques qui y sont connectés.
L'adresse IP privée, quant à elle, est unique uniquement au sein des appareils connectés au routeur, et n'est pas visible directement par le réseau auquel est connecté le routeur.
Le routage d'un paquet se fait alors par le service NAT (Network Address Translation): supposons qu'un ordinateur veuille envoyer un ping au serveur DNS de Google, à l'adresse 8.8.8.8. Le ping passera d'abord par l'interface réseau de l'ordinateur, avec l'IP privée 192.168.0.1 (exemple type d'adresse privée de Classe C), transitera par le routeur, qui lui a à la fois une IP privée (permettant de l'identifier sur le réseau) l'IP publique (permettant de l'identifier sur un réseau plus grand, en l'occurence internet).

L'adresse de ce réseau est 192.168.0.0/24

Job 05:

La commande permettant de voir l'ip d'un ordinateur sur Packet Tracer est: ipconfig
Elle est à exécuter depuis l'ordinateur dont on veut voir l'IP, dans l'onglet Desktop puis Command Prompt:
Pour le PC de Pierre

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::2D0:FFFF:FE5D:802D
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.1
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
```

Pour le PC de Alicia

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.........: FE80::201:C7FF:FE80:49C7
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     0.0.0.0
```

Job 06:

Pour tester la connectivité entre les deux ordinateurs, on utilise la commande ping suivie de leur adresse ip, depuis le Command Prompt.

Donc ici:

```
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
```

On envoie ici un ping au PC de Pierre, et on obtient plusieurs informations:
Tout d'abord, on voit qu'on envoie 4 pings (Sent = 4) et qu'on en reçoit 4 (Received = 4), et qu'aucun ping n'a perdu son chemin/n'est arrivé incomplet (Lost = 0 (0% loss))
On voit que le parcours du ping, donc depuis le PC Alicia, jusqu'au PC Pierre, et le retour au PC Alicia, a pris moins d'une milliseconde sur chacun des 4 pings (time<1ms), que le TTL est à 128, ce qui signifie que le ping est arrivé directement et sans détour chez PC Pierre.
Note: le TTL (pour Time To Live) est une sorte de compte à rebours de routeurs. Il s'initie communément à 128 (selon le paramétrage de la commande ping) et se décrémente de 1 à chaque routeur traversé jusqu'à atteindre sa destination.

Ici, on lance un ping 192.168.1.1 (le PC Pierre) depuis le PC Alicia. Les deux étant directement reliés, il n'y a rien à traverser avant d'arriver à la destination, ainsi le TTL est à 128 - 0 (nombre de routeurs traversés) = 128
On effectue maintenant un ping dans le sens inverse, qui marche tout naturellement:

```
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
```

Job 07:

Une fois le PC Pierre éteint, le ping depuis le PC Alicia donne ceci:

```
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),
```

Le ping ne peut en effet pas aboutir si le PC Pierre est éteint:
PC Alicia envoie un ping, PC Pierre ne peut rien recevoir ni rien renvoyer, PC Alicia attend donc suffisamment longtemps sans rien recevoir pour déclarer un time out.
On le voit d'ailleurs à chaque ligne "Request timed out ." puis en dessous dans "Lost = 4 (100% loss)", signifiant que chacune des requêtes ping que l'on a envoyées n'a pas été retournée et s'est donc perdue.
Le PC Pierre n'a donc reçu aucun paquet, et seul le PC Alicia garde en mémoire une trace de l'envoi des paquets, sans leur retour, qui lui permet de déclarer la perte des paquets/le time out.

Job 08:

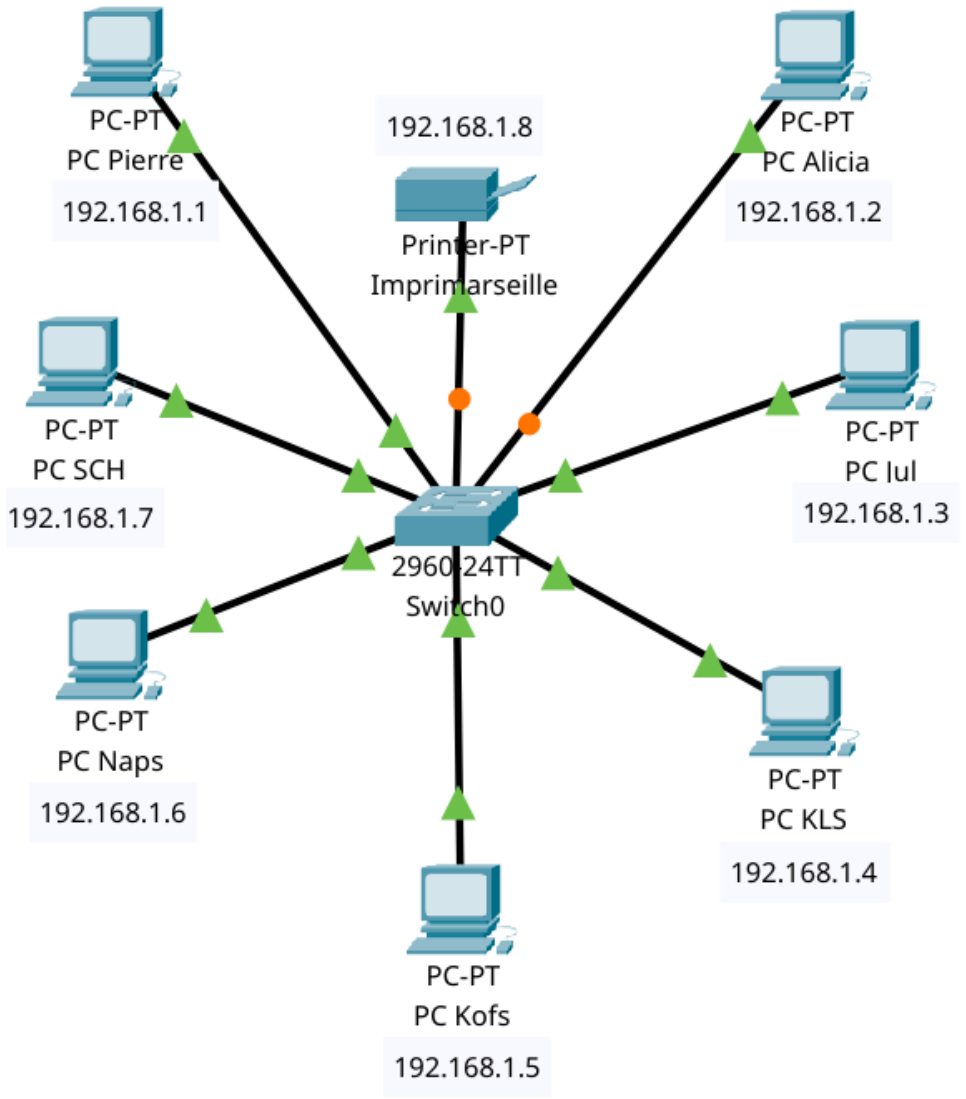
La différence principale entre un hub et un switch réside dans la redirection des trames.
Note: Une trame est une structure de données qui intervient dans la couche 2 (Data link, liaison de données) du modèle OSI. Celle-ci sert à encapsuler des données entre un header (en-tête) et un trailer (littéralement une "remorque", comprendre "la queue de la trame").
Le paquet qui doit transiter est donc inclus dans les données de cette trame. La trame est ensuite directement traduite en bits qui circulent au niveau physique.

Dans un hub, une trame reçue au niveau du hub est redirigée vers l'ensemble des machines/segments qui y sont connectées, le hub ne prend donc pas en compte de port de destination, et envoie un paquet à tous ses ports.
Un switch, cependant, retient le port ayant émis la trame, et prend en compte la destination du paquet, pour l'envoyer dans le port spécifié.
Ainsi, le hub est dit de "passif", étant donné qu'il ne calcule pas de route à suivre, tandis que le switch est dit d'"actif".
Que ce soit un hub ou un switch, l'adresse utilisée pour la transmission des données est l'adresse MAC des périphériques connectés.

Le hub a pour avantage de gérer automatiquement le trafic dans l'optique où l'on a besoin d'avoir la même information sur plusieurs périphériques, pour analyser un trafic réseau, par exemple.
De plus, un hub (bien que négligeable de nos jours) sera moins cher qu'un switch à l'achat.
Un hub, cependant, engendrera une plus grosse congestion du trafic étant donné que chaque paquet sera envoyé autant de fois qu'il y a de segments connectés.

Le switch, quant à lui, sera bien plus utile pour la communication entre un ordinateur et un autre, ou entre un segment et un autre. Il permettra une sécurité accrue en compartimentant les échanges de données, et réduira la congestion sur le réseau en allouant une bande passante dédiée à chaque port. Il sera cependant plus coûteux que le hub.

Job 09:



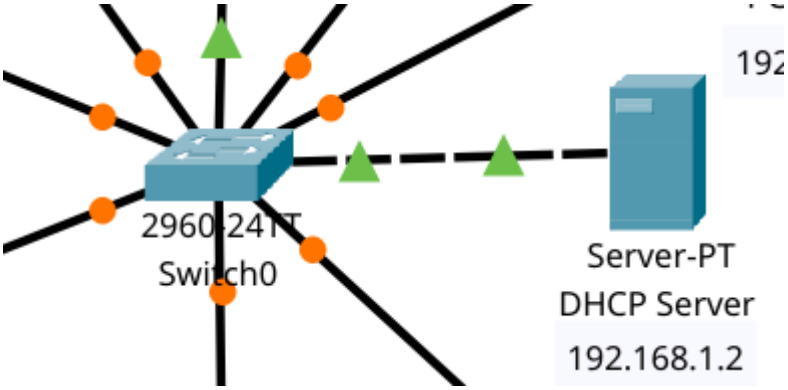
Pour faire le schéma d'un réseau simple comme celui-ci, nous utilisons simplement Cisco Packet Tracer qui effectue très bien la tâche.
Nous aurions pu, le cas échéant, utiliser un outil tel que diagrams.net.
Ici, nous avons volontairement placé les périphériques en "étoile" autour du switch, pour représenter la topologique en étoile de ce réseau.

On peut identifier plusieurs avantages à avoir un schéma de réseau:
Premièrement, le plus évident, la compréhension visuelle instinctive. En effet, en tant qu'humains nous sommes naturellement habitués à comprendre comment s'organise un terrain, une ville, en la regardant directement ou depuis un point élevé. Il est plus évident de savoir où mène le Cours Lieutaud en regardant le Cours Lieutaud depuis la boutique Maxi Scoot qui s'y trouve, plutôt que de lire en caractères pixélisés: le Cours Lieutaud part du Boulevard Baille jusqu'au Boulevard Garibaldi qui en est son prolongement, en s'arrêtant à l'intersection avec la Canebière.
C'est le même principe pour un réseau. Plutôt que de lire des adresses IP, des Gateway, des adresses MAC, on se représente graphiquement la topologie du réseau efficacement et simplement par des éléments simplifiés comme sur Cisco Packet Tracer.

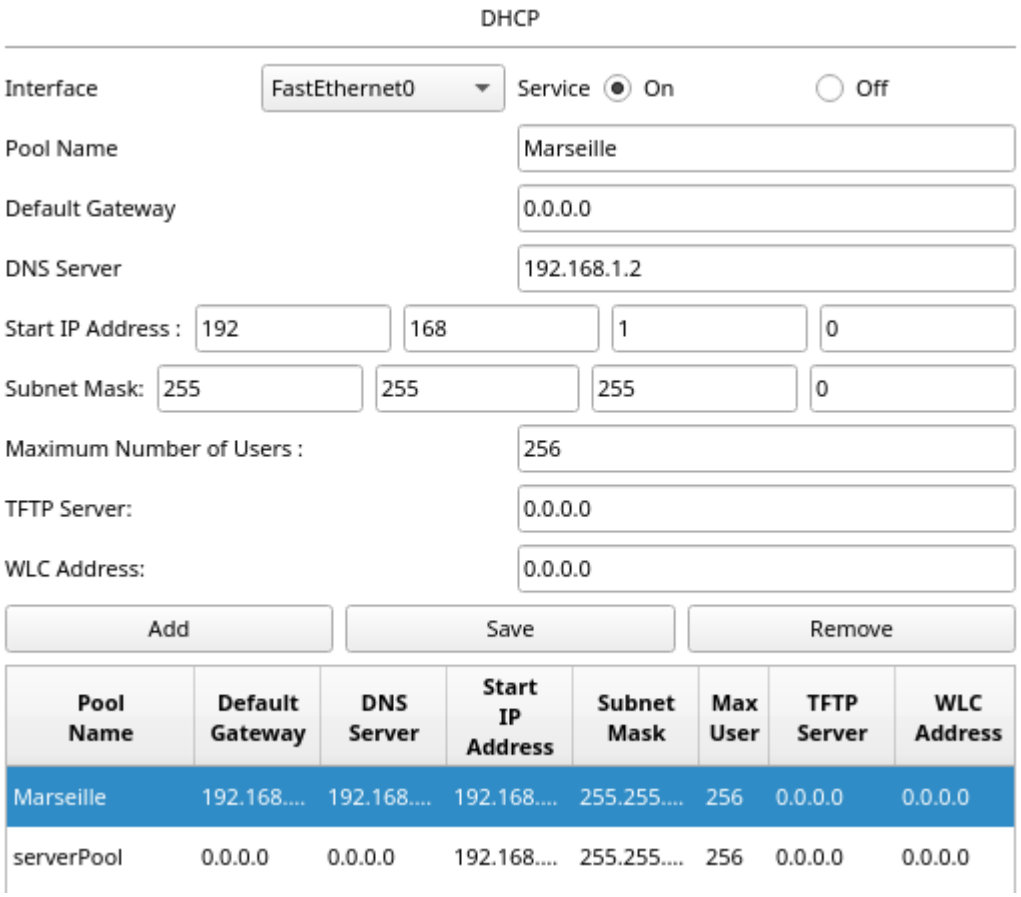
Cette compréhension visuelle aidera donc à la communication entre opérateurs et administrateurs, ainsi qu'à l'obtention d'informations sur les équipements dans le réseau, que l'on pourra inclure.
D'autres avantages significatifs suivent ce premier avantage:
On pourra établir simplement et efficacement un diagnostic de panne et/ou de sécurité, en comprenant les tenants et aboutissants du réseau étudié, avec ses points d'entrée publiques, ses éventuels sous-réseaux pouvant causer des problèmes, et caetera.
De plus, comme on vient de le faire ici avec l'imprimante, un schéma de réseau permet de mieux modéliser et anticiper les éventuelles évolutions du réseau, qu'elles soient dans l'optique d'ajouter du matériel, ou d'en retirer sans mettre à mal la stabilité de l'infrastructure.
Enfin, on peut aussi noter qu'un schéma pour son réseau permet, par la compréhension visuelle une fois encore, d'anticiper la répartition du trafic, ainsi que ses points clés, et de prévoir un désengorgement pour une évolution future, comme par exemple en mettant un tunnel gratuit sous le Cours Lieutaud, ou en ajoutant un switch à un réseau s'il y a déjà trop d'ordinateurs sur le premier.

Job 10:

On commence par ajouter un Server-PT dans l'interface Cisco PT.
On le renomme DHCP Server pour des questions de compréhension et on lui attribue l'IP 192.168.1.15.



On configure ensuite le service comme suit:



Ici ce qu'on fait: On donne un nom à la configuration (Pool Name, sous-entendre "nom de la plage d'adresses"), puis on met une Gateway par défaut. Ceci sert normalement dans le cas où notre réseau aurait un routeur pour communiquer avec l'extérieur. Ici, on n'a qu'un switch, qui n'a pas de capacité de routage à proprement dit, étant donné qu'il agit au niveau de la couche 2 du modèle OSI (Data link).
On met donc 0.0.0.0.
On configure ensuite l'adresse du serveur DNS, étant donné que l'on en n'a pas, on met celle du serveur DHCP, 192.168.1.2, étant donné que les adresses à traduire sont directement dans le DHCP.
Enfin, en "Start IP Address", on définit le début de la plage d'adresses à utiliser, puis dans "Subnet Mask" on indique au serveur DHCP que les adresses qu'il distribuera varieront uniquement sur le dernier octet.
Enfin, on positionne le service sur "On" après avoir fait "save", puis on redémarre toutes les machines du réseau.
Voilà, les machines, à leur démarrage, se voient attribuées une IP par le serveur DHCP, qui vérifie les IP déjà utilisées (ici, celle de l'imprimante ainsi que celle du serveur lui-même), et qui assigne une IP disponible à l'ordinateur démarré, dans la plage des IP 192.168.1.x

Une adresse IP statique doit être attribuée manuellement par l'administrateur réseau (ou un quelconque configurateur du réseau), elle ne changera pas au redémarrage de l'appareil et sur le long terme. La gestion est donc manuelle, et l'administrateur, s'il veut éviter les conflits, devra garder une trace écrite de l'ensemble des IP déjà attribuées et vérifier que la nouvelle n'est pas utilisée.

Les adresses IP statiques sont pratiques (et même souvent nécessaires) pour des équipements qui doivent être accessibles en permanence de façon claire et immuable, comme un routeur, un serveur ou même une imprimante.
Une adresse IP attribuée par DHCP, à l'inverse, est dite "dynamique". Le serveur DHCP l'attribue au périphérique qui se connecte au réseau, en vérifiant automatiquement les IP déjà utilisées. Lorsque le périphérique se déconnecte du réseau puis s'y reconnecte, le serveur DHCP lui réattribue une nouvelle adresse IP (bien souvent, elle sera la même que celle qu'il avait avant de se déconnecter, étant donné que la plage d'IP disponibles reste la même et que seule manque la sienne). Ceci évite naturellement les conflits et limite l'intervention humaine, coûteuse en temps et en moyens. Le serveur DHCP attribue une date limite à l'IP qu'il a donnée au périphérique, et renouvelle l'IP à terme de cette date, ceci permet d'éclaircir la plage d'adresses en réattribuant de façon claire des adresses IP, en plus de garantir une certaine sécurité en assurant une rotation des adresses IP des équipements.

Job 11:

Un plan d'adressage peut se faire de différentes manières, mais la suivante est viable et assez classique, en plus d'être facilement compréhensible.

N° subnet	Subnet mask	IP du réseau	IP utilisables (pour avoir le nombre d'hôtes désiré)	IP DHCP	Broadcast adress
1	255.255.255.240	10.0.0.0	10.0.0.2 - 10.0.0.13	10.0.0.1	10.0.0.14
2	255.255.255.224	10.0.1.0	10.0.1.2 - 10.0.1.31	10.0.1.1	10.0.1.32
3	255.255.255.224	10.0.2.0	10.0.2.2 - 10.0.2.31	10.0.2.1	10.0.2.32
4	255.255.255.224	10.0.3.0	10.0.3.2 - 10.0.3.31	10.0.3.1	10.0.3.32
5	255.255.255.224	10.0.4.0	10.0.4.2 - 10.0.4.31	10.0.4.1	10.0.4.32
6	255.255.255.224	10.0.5.0	10.0.5.2 - 10.0.5.31	10.0.5.1	10.0.5.32
7	255.255.255.128	10.0.6.0	10.0.6.2 - 10.0.6.121	10.0.6.1	10.0.6.122
8	255.255.255.128	10.0.7.0	10.0.7.2 - 10.0.7.121	10.0.7.1	10.0.7.122
9	255.255.255.128	10.0.8.0	10.0.8.2 - 10.0.8.121	10.0.8.1	10.0.8.122
10	255.255.255.128	10.0.9.0	10.0.9.2 - 10.0.9.121	10.0.9.1	10.0.9.122
11	255.255.255.128	10.0.10.0	10.0.10.2 - 10.0.10.121	10.0.10.1	10.0.10.122
12	255.255.255.0	10.0.11.0	10.0.11.2 - 10.0.11.161	10.0.11.1	10.0.11.162
13	255.255.255.0	10.0.12.0	10.0.12.2 - 10.0.12.161	10.0.12.1	10.0.12.162
14	255.255.255.0	10.0.13.0	10.0.13.2 - 10.0.13.161	10.0.13.1	10.0.13.162
15	255.255.255.0	10.0.14.0	10.0.14.2 - 10.0.14.161	10.0.14.1	10.0.14.162
16	255.255.255.0	10.0.15.0	10.0.15.2 - 10.0.15.161	10.0.15.1	10.0.15.162

Il existe 5 classes d'adresses IP, qui correspondent à la configuration des 5 premiers bits du premier octet de l'adresse.

La classe A, comme celle que nous utilisons, correspond à un premier octet dont le premier bit est à 0, donc: 0xxx xxxx
Par exemple, l'adresse de classe A 10.0.0.1 se traduit, en binaire, par:
0000 1010.0000 0000.0000 0000.0000 0001

Pour une adresse de classe B: 10xx xxxx
Pour une adresse de classe C: 110x xxxx
Comme par exemple pour les ip privées sur un réseau local: 192.168.1.1
Qui se traduit en binaire par: **110**0 0000.1010 1000.0000 0001.0000 0001
Pour une adresse de classe D: 1110 xxxx
Pour une adresse de classe E: 1111 xxxx

Ces cinq classes vont être utilisées selon le nombre d'adresses que l'on veut attribuer, et certaines auront un but précis.
Dans un réseau familial, pour une maison par exemple, on utilisera généralement une adresse de classe C, telle que 192.168.x.x.

Utiliser une adresse de classe A permet d'avoir un grand nombre d'adresses différentes, et donc une grande flexibilité concernant le nombre de sous-réseaux que l'on peut avoir, en plus de pouvoir leur attribuer de grandes tailles.

Les adresses de classe B seront l'intermédiaire entre la classe A et la classe C, et permettront à de moyennes entreprises d'attribuer suffisamment d'IP aux équipements.

Les adresses de classe E auront un but expérimental, tandis que les adresses de classe D seront utilisées pour le multicast (forme de cast, au même titre que le broadcast - l'envoi de paquets à plusieurs destinataires en même temps -, ou que l'unicast - l'envoi de paquets à un seul destinataire -, le multicast sert à l'envoi de paquets à plusieurs destinataires sélectionnés, ce qui le différencie du broadcast).

Job 12:

Le modèle OSI, pour Open Systems Interconnections, est un modèle à la fois pédagogique et pratique d'organisation du réseau. Il se divise en sept couches, qu'on peut retenir par le moyen mnémotechnique: Please Do Not Throw Sausage Pizza Away.
Donc, de haut en bas:
Physical: C'est la couche où les données sont les plus brutes d'un point de vue électronique: une salade de bits qui circulent dans des câbles en cuivre, ou sous forme de photons dans des câbles en fibre optique. Un hub, par exemple, est à cette couche, il n'effectue aucun traitement ou compréhension des données, simplement un transport physique.

Data link: Ici, les données sont encapsulées dans des trames, qui circulent plus intelligemment, par un protocole Ethernet, dans des Switch par exemple, qui redirigent les trames aux bons endroits.

Network: C'est la couche où les données sont véritablement dirigées, elles deviennent des paquets qui circulent grâce à des protocoles tels que l'IP (Internet Protocol). Interviennent ici les notions de routage et d'adressage.

Transport: Les paquets obéissent à de nouveaux protocoles, comme le TCP ou l'UDP, qui vont venir définir la façon dont communiquent deux processus sur des périphériques distants.

Session: Cette couche sert à la synchronisation des échanges, c'est-à-dire à la cohésion des sessions des machines distantes, à leur ouverture, à leur fermeture.

Presentation: Cette couche prépare la couche application. Elle transcrit les données binaires en données applicatives compréhensibles par le processus.

Application: Cette couche est la dernière étape avant l'utilisateur directement: les données deviennent human-readable (lisibles par l'Homme), par le biais de différents protocoles et applications: le DNS (Domain Name Server) en est un exemple, il transcrit des informations en caractères latins en adresses ip.

Concrètement, donc, une information qui doit circuler dans le réseau passe par ces couches du modèle OSI:

L'application transforme une information humaine en données suivant un protocole et une requête, comme le HTTP.
Puis le presentation fait la liaison entre l'application et le session, en précisant le type de données que l'on lui présente.
Le session s'assure de la synchronicité entre les deux périphériques communicants, ainsi que le port utilisé pour la communication.
Le transport encapsule ces données avec des protocoles tels que le Transmission Control Protocol, qui détermineront la façon dont se fera la communication.
Le network ajoute un nouveau protocole au paquet nouvellement créé, comme le Internet Protocol, qui permettra le routage de l'information à transmettre.
Le data link transfère ce paquet dans une trame, qui circule par le protocole Ethernet par exemple.
Le physical, enfin, gère au niveau électrons/photons (comprendre "de façon la plus palpable qui soit") le transport de l'information, dans des câbles de différents types.

Le périphérique qui veut lire cette information, enfin, lui fait faire le chemin inverse.

Le câble de fibre optique, le câble RJ45, ont des éléments situés à la couche Physical.
L'Ethernet, l'adresse MAC, le protocole Wi-Fi sont des éléments situés à la couche Data link.
L'IPv4, l'IPv6, le routeur, sont situés à la couche Network.
Le TCP, l'UDP, sont situés à la couche Transport.
Le PPTP est situé à la couche Session.
Le SSL/TLS et le FTP sont situés à la couche Presentation.
Le HTML, et le FTP (une fois encore), sont situés à la couche Application.

Job 13:

Ce réseau suit une architecture LAN (Local Area Network), en forme d'étoile.

C’est-à-dire qu’il correspond à un réseau d’une petite zone géographique, telle qu’une pièce d’open-space, une petite entreprise, une maison; qu’il n’est pas relié à un réseau plus grand tel qu’internet ou à d’autres réseaux, et que tous les périphériques sont connectés à un seul qui s’occupe de la redirection de l’ensemble du trafic (architecture en étoile).
Il existe d’autres architectures topologiques telles que les WAN (Wide Area Network, comprendre “Réseau d’un quartier, d’une ville, et au-delà”), et typologiques, telles que les architectures en anneau (chaque appareil est relié à son voisin de “gauche” et son voisin de “droite”, en cercle), ou en ligne (chaque appareil est relié à son voisin de “gauche” et son voisin de “droite”, mais l’appareil au début de la ligne et celui à la fin ne sont pas reliés entre eux directement).

L’adresse IP du réseau est 192.168.10.0/24 avec le subnet mask 255.255.255.0.

On peut brancher jusqu’à 254 machines sur ce réseau, étant donné qu’on gardera une adresse pour le réseau et une adresse de diffusion.

L’adresse de diffusion est ici la dernière disponible, soit 192.168.10.255/24

Job 14:

145.32.59.24 en base 10 = 1001 0001.0010 0000.0011 1011.0001 1000 en base 2
200.42.129.16 en base 10 = 1100 1000.0010 1010.1000 0001.0001 0000 en base 2
14.82.19.54 en base 10 = 0000 1110.0101 0010.0001 0011.0011 0110 en base 2

Job 15:

Le routage est l’acheminement des données d’un réseau vers un autre, c’est-à-dire le calcul d’un itinéraire à suivre pour atteindre un destinataire défini. Le routage est calculé au niveau des routeurs, et se situe à la couche Network du modèle OSI.
Ceci se fait par des tables de routage et des algorithmes tels que l’algorithme de Dijkstra permettant de pré-calculé l’itinéraire le plus court d’un point A à un point B, sont utiles pour comprendre le fonctionnement de ce procédé.

Une gateway est un passage entre votre réseau et un autre. Un réseau domestique, par exemple, a pour gateway un routeur qui le relie à internet. On peut configurer, sur une machine, la default gateway, c’est-à-dire le passage par défaut où sont envoyées les données si rien n’est précisé/si la gateway précisée n’existe pas.

Un VPN, pour Virtual Private Network, est une interface qui vient se placer entre votre périphérique réseau et le réseau auquel vous voulez vous connecter (communément internet). En passant par cette interface, vos données vont généralement être cryptées, votre adresse IP émettrice masquée. Ainsi, la communication entre vous, votre VPN, et le réseau distant, sera bien plus complexe à intercepter pour un attaquant lambda.

Un DNS, pour Domain Name System, est un système (supporté par des serveurs spécifiques) qui traduit un nom de domaine de caractères lisibles (tel que drive.google.com) en adresse IP qui servira au routage. Ceci évite à l’utilisateur d’avoir à retenir une suite de chiffres et de points et lui permet de se rendre de façon intuitive sur des sites web, par

exemple. Le DNS agira donc comme une sorte de traducteur, que votre ordinateur interrogera lorsque vous lui demanderez un site spécifique. Google, par exemple, possède un serveur DNS, et l'on peut indiquer à notre machine d'aller chercher directement dans le serveur DNS de google pour les noms de domaine que l'on recherchera dans le futur.