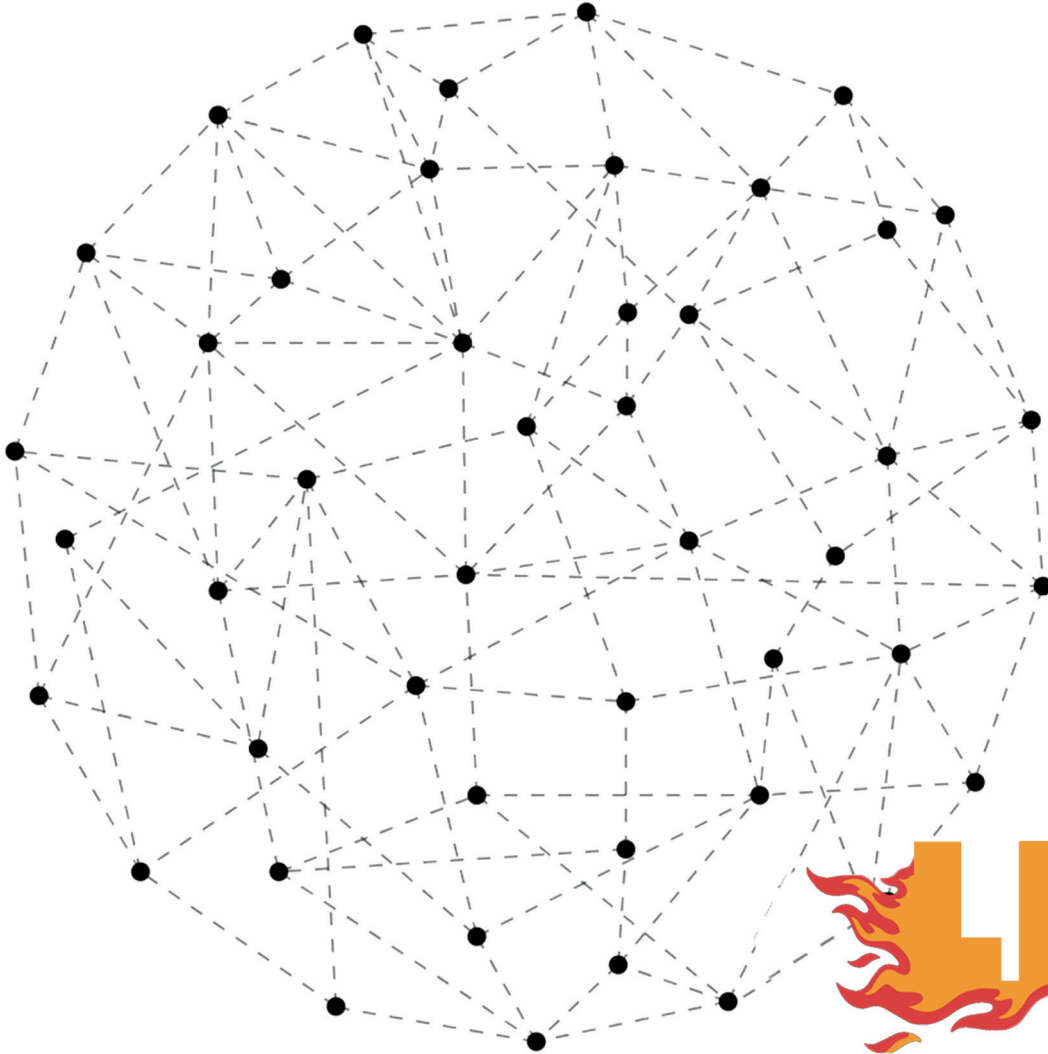


**BARBARA VANNI**



**LE RÉSEAU**

—

01

## INSTALLATION CISCO PACKET TRACER

02

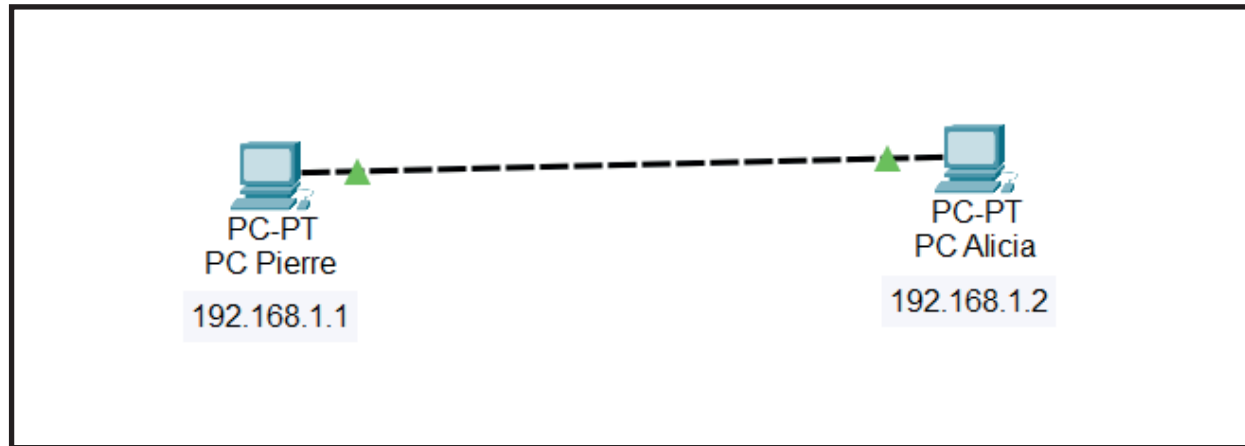
### ●●● Qu'est-ce-qu'un réseau informatique et à quoi ça sert ?

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

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

### ●●● De quoi peut -être composé un réseau ?

- **Serveur** : Ordinateur spécifique pour organiser l'ensemble du réseau. Il gère l'accès aux ressources, aux périphériques et les connexions des différents utilisateurs. Son accès nécessite une identification (identifiant et mot de passe).
- **Poste-client** : Ordinateur connecté au réseau par l'intermédiaire d'une carte réseau (avec ou sans fils) qui peut utiliser les moyens informatiques partagés
- **Commutateur ou Switch** : Boîtier permettant aux équipements du réseau de communiquer.
- **Routeur/Modem** : Permet de communiquer avec d'autres réseaux en faisant transiter des paquets (informations découpées) par les lignes téléphoniques.
- **Concentrateur ou Hub** : Permet de connecter plusieurs équipements du réseau informatique. Le concentrateur est le plus simple de la famille des équipements de connexion réseau, car il connecte des composants LAN ayant des protocoles identiques.
- **Pont (Bridge)** : Les ponts servent à connecter deux ou plusieurs hôtes ou segments de réseau. Le rôle fondamental des ponts dans l'architecture réseau est de stocker et de transférer les trames entre les différents segments qu'ils relient. Ils utilisent les adresses MAC.
- **Répéteur** : Un répéteur est un appareil électronique qui amplifie le signal qu'il reçoit.
- **Point d'accès** : Les points d'accès sans fil (WAP) se composent d'un émetteur et d'un récepteur, qui permettent de créer un réseau local sans fil (WLAN). Les points d'accès sont généralement des équipements réseau distincts dotés d'une antenne, d'un émetteur et d'un adaptateur intégrés.



### ... Quel type de câble pour connecter deux machines?

Il existe 3 types de moyen de communication en ce qui concerne le réseau:

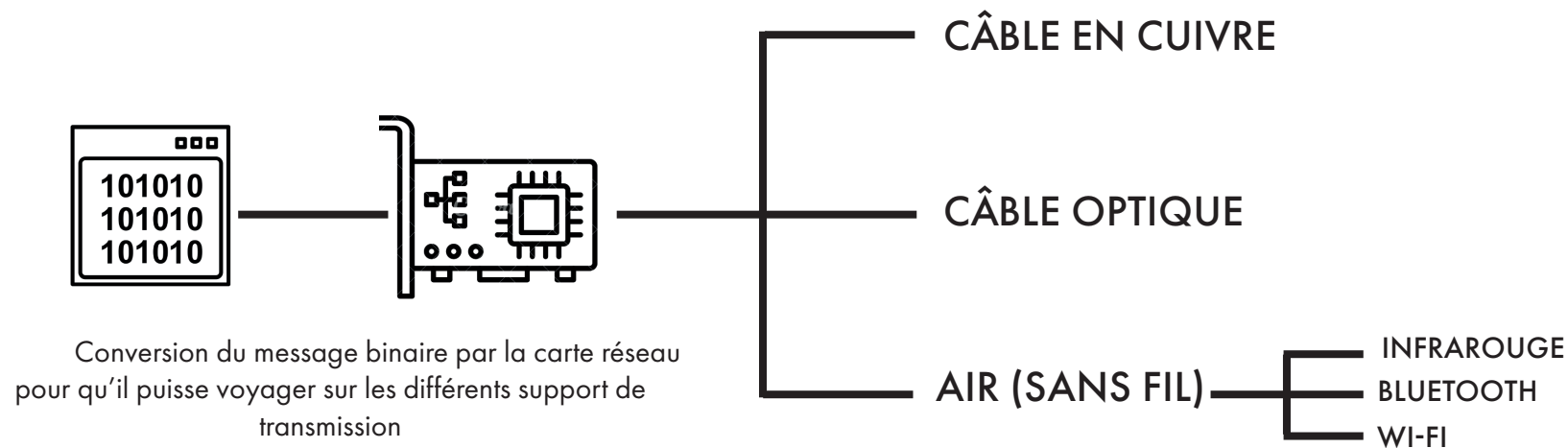
- le **câble en cuivre**, dont le plus utilisé est le câble à paires torsadées (qui peut aussi s'appeler «câble réseau» «câble Ethernet» ou «RJ45»)
- le **câble optique** ou fibre optique
- **l'air**, si on souhaite communiquer sans fil

Dans le cas de notre installation, on peut voir sur la configuration de nos PC qu'ils sont équipés d'une carte réseau en cuivre. On va donc utiliser un **câble en cuivre à paires torsadées (à câbles croisés)** (cooper cross-over ) pour connecter les deux machines entres elles.

Lorsque que l'on utilise des câbles en cuivre à paires torsadées, il faut faire attention car il en existe 2 types : les **câbles droits** et les **câbles croisés**. Leur différence vient simplement du fait que les 8 fils qui composent ces câbles sont organisés dans un ordre différent.

- Un **câble croisé** doit être utilisé pour relier directement 2 équipements terminaux entre eux. Par exemple, un PC avec un PC, un PC avec une imprimante ou un PC avec un serveur.
- Les **câbles droits** seront utilisés dès qu'on a affaire à des réseaux intégrant des équipements d'interconnexion.

Pour déterminer quel câble nous avons besoin il faut connaître la carte réseau sur laquelle on va le brancher. Chaque type de carte réseau est associé à un port et à un support de transmission, tout cela étant régi par des normes.



TYPE CARTE RÉSEAU	PORT ASSOCIÉ (COURAMMENT)	SUPPORT DE TRANSMISSION	NORME GÉNÉRALE
Cuivre	RJ45	Câble cuivre à paire torsadées	IEEE 802.3 (Ethernet)
Optique	GBIC/SFP SFP+/XFP	Fibre optique	IEEE 802.3 (Ethernet)
Sans-fil	X	Air	IEEE 802.11 (WLAN/Wi-Fi)

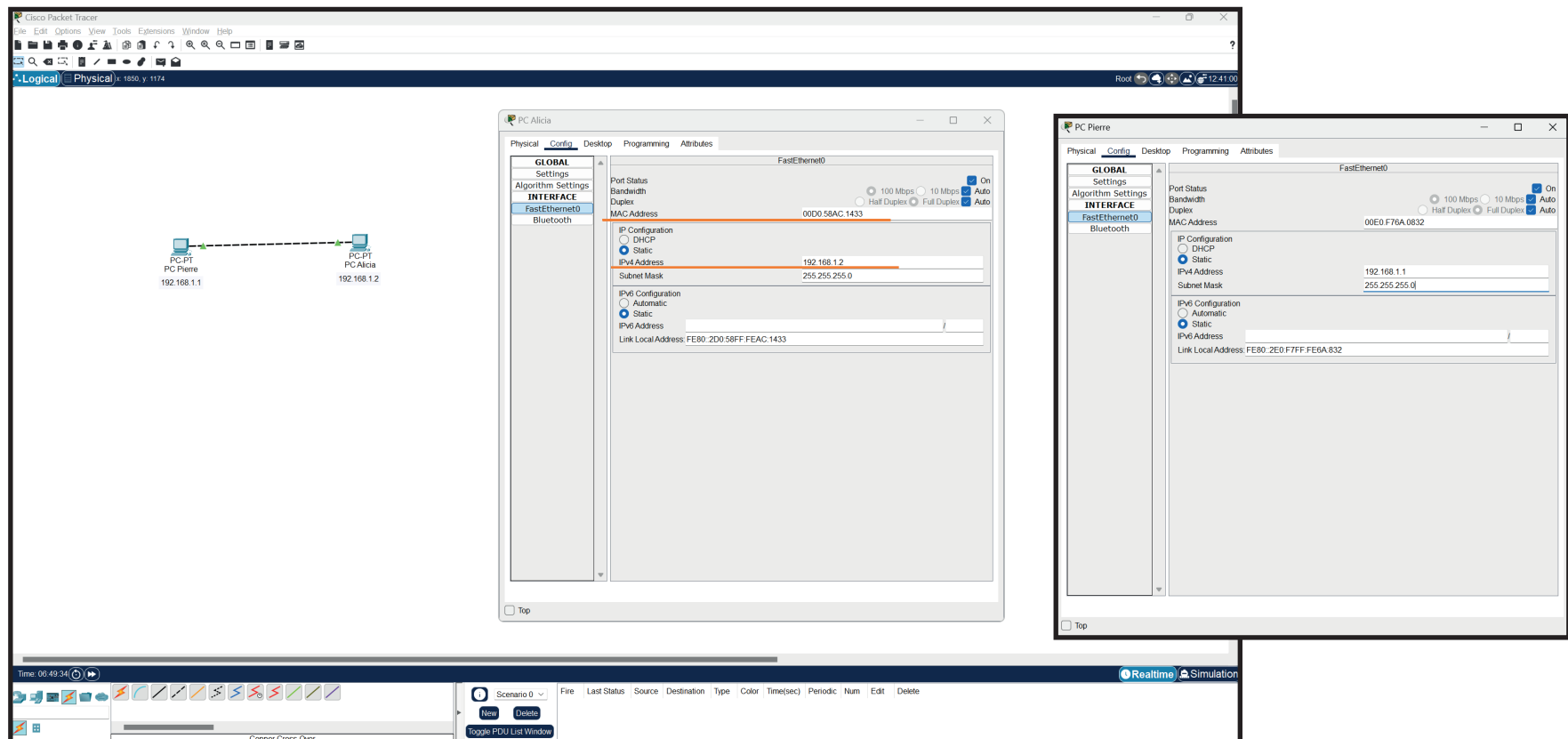
## 04

### ... Qu'est-ce-qu'une adresse IP et à quoi ça sert ?

Adresse Ip (internet protocole) est l'adresse d'identification unique d'une machine sur un réseau informatique (ordinateur, imprimante, routeur,...). C'est une chaîne de chiffre qui fonctionne de la même manière qu'une adresse de domicile et qui garantit que les données correctes sont envoyées/reçu par le bon ordinateur.

### ... Qu'est-ce-qu'une adresse MAC?

L'adresse MAC (pour Media Access Control) est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est sensée être unique au monde. On peut donc considérer qu'elle constitue une sorte de plaque d'immatriculation des appareils électroniques. L'adresse MAC peut être modifiée dans certains cas. Cependant, cela reste assez rare car elle est activée dès la fabrication en usine.



## IPV4 / IPV6

**IPv4** est l'abréviation de Internet Protocol version 4 et est le plus largement utilisé. Il s'agit d'un système numérique de 32 bits divisé en quatre parties (octets) séparées par des points. La valeur de chaque octet varie de 0 à 255. Voici un exemple d'une adresse IPv4 : 169.89.131.246

Tous les types de systèmes gèrent le routage IPv4 sans problème. Mais il existe une version plus récente, destiné à remplacer l'IPv4, c'est l' **IPv6**.

En effet, le nombre de variantes de l'IPv4 est actuellement épuisé, principalement en raison de la rapidité de l'expansion d'internet.

Les adresses IPv6 ont une longueur de 128 bits. Cela signifie qu'il existe environ 340 millions d'adresses IPv6 uniques. Elles sont écrites en huit séries de chiffres hexadécimaux de 16 bits séparés par des deux-points. Il y a donc des lettres de A à F dans une adresse IPv6. Voici un exemple d'une adresse IPv6 : 2001:3FFE:9D38:FE75:A95A:1C48:50DF:6AB8

Le routage est plus efficace avec IPv6 car il permet aux fournisseurs de services Internet de réduire la taille des tables de routage. L'IPv6 utilise également la sécurité du protocole Internet (IPsec), de sorte qu'il n'est pas nécessaire de se préoccuper de l'authentification, de la confidentialité et de l'intégrité des données.

## PRIVE / PUBLIC

Une adresse IP **privée** est l'adresse IP qu'on utilise pour communiquer au sein de réseaux locaux. Ainsi, tous les appareils dotés d'une fonction Bluetooth ou pouvant se connecter à un réseau ont une adresse IP privée. Elle ne fonctionne qu'au sein d'un réseau local (LAN) et non sur internet. Son utilisation est donc gratuite. De l'autre côté, une adresse IP **publique** est l'adresse IP utilisée pour communiquer en dehors des réseaux locaux et pour se connecter à l'internet. Ce type d'adresse IP n'est pas gratuit car il est attribué et contrôlé par les fournisseurs de services Internet. Dans les réseaux publics on retrouve les adresses IP **dynamiques**, qui sont celles qu'un fournisseur de services Internet attribue à ses clients. Et qui donc peuvent changer régulièrement.

En revanche, les adresses IP **statiques** sont considérées comme des adresses IP fixes. Par conséquent, elles restent les mêmes, sauf si l'administration du réseau change.

05

## ADRESSE IP : OÙ LA TROUVER ?

Dans Cisco pour vérifier que l'adresse IP du Pc de Pierre, il nous faut ouvrir un terminal est taper la commande :

ipconfig

The screenshot displays the Cisco Packet Tracer interface. On the left, the 'PC Pierre' configuration window is open, showing a grid of icons. The 'Command Prompt' icon is circled in orange. An orange arrow points from this icon to the 'Command Prompt' window on the right. The 'Command Prompt' window shows the output of the 'ipconfig' command, displaying the IP address 192.168.1.1 and the subnet mask 255.255.255.0. The background shows a network diagram with two PCs connected by a dashed line. The bottom status bar indicates 'Realtime' mode.

```
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::201:C9FF:FE48:1D82
IPv6 Address . . . . .: ::
IPv4 Address. . . . .: 192.168.1.1
Subnet Mask . . . . .: 255.255.255.0
Default Gateway . . . . .: 0.0.0.0

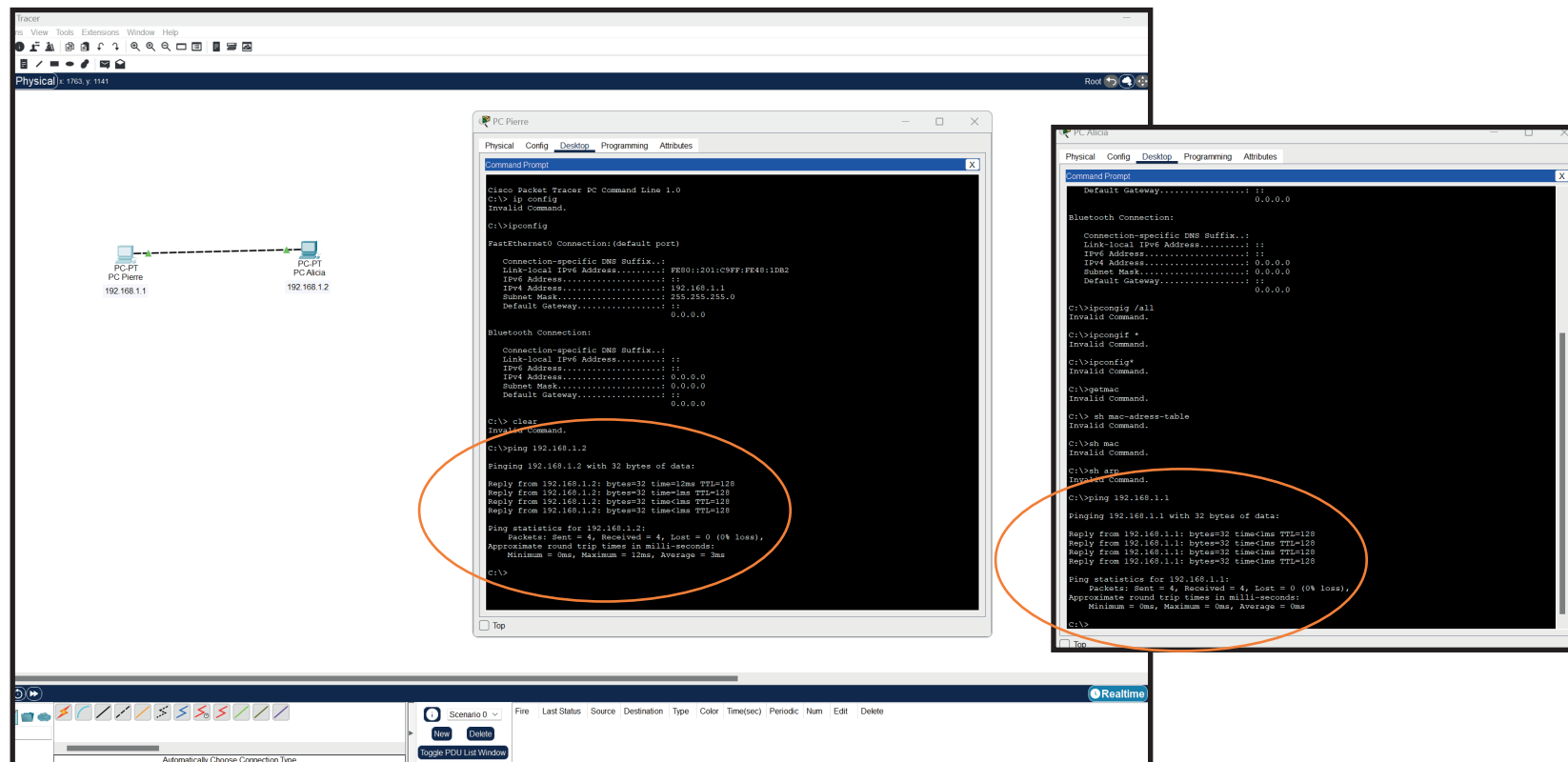
Bluetooth Connection:
Connection-specific DNS Suffix...:
Link-local IPv6 Address . . . . .:
IPv6 Address . . . . .: ::
IPv4 Address . . . . .: 0.0.0.0
Subnet Mask . . . . .: 0.0.0.0
Default Gateway . . . . .: 0.0.0.0

C:\>
```



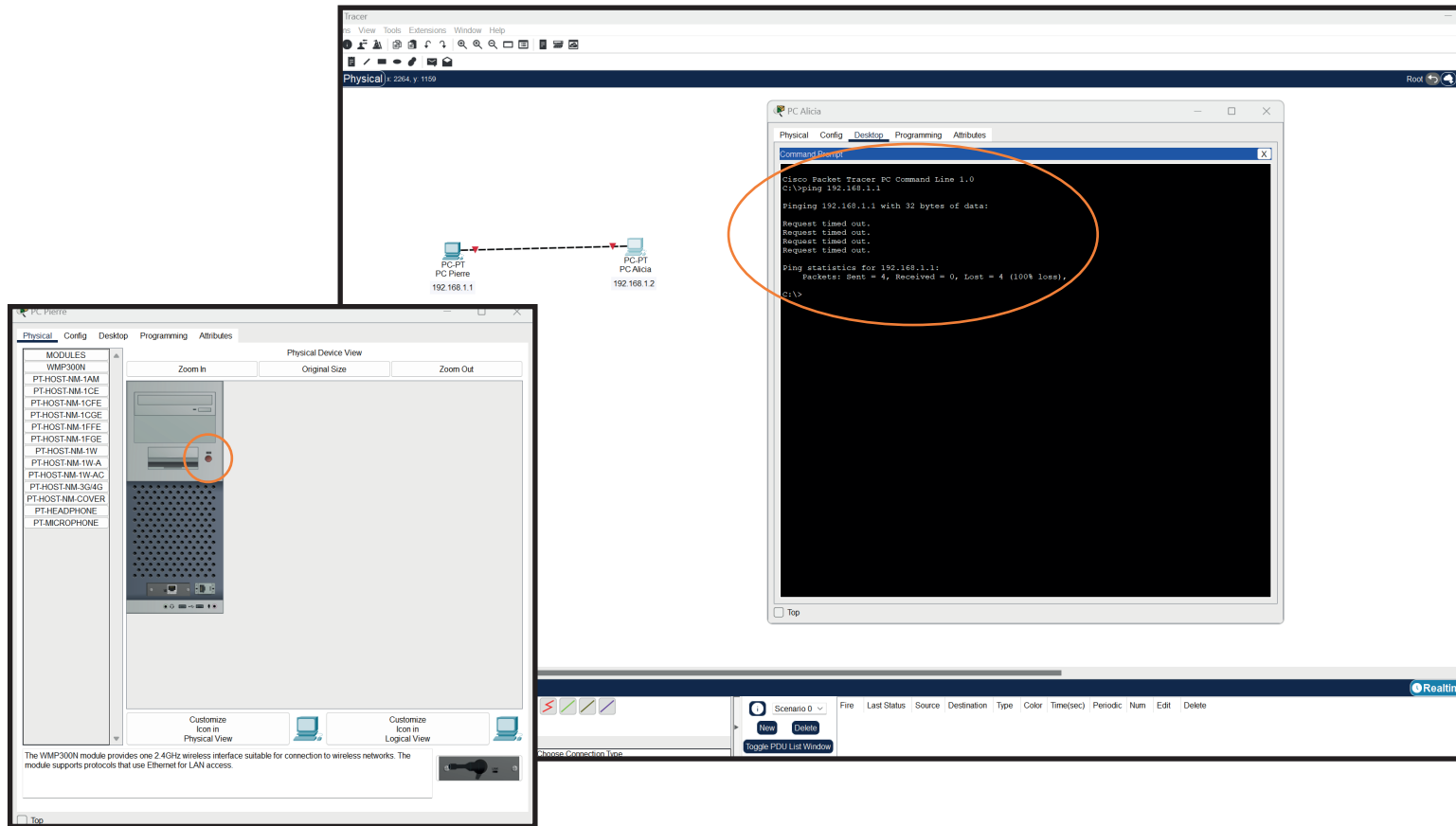
ping [adresse IP ]

- Déterminer l'état du réseau et de divers hôtes étrangers.
- Faire le suivi des incidents matériels et logiciels et les isoler.
- Tester, mesurer et gérer les réseaux.



07

PING NOT FOUND !



On voit que le pc de Pierre ne reçoit pas les paquets envoyés par le pc d'Alicia, tout simplement parceque son Pc est éteint.

## ... SWITCH ou HUB ?

Le **switch** (commutateur) est le premier équipement d'interconnexion que l'on rencontre dans un réseau, c'est celui qui est au plus près des machines. Il va avoir le même rôle qu'un rond-point sur un réseau routier, ou plus précisément qu'un aiguillage sur un réseau ferré. En plus d'être une intersection entre plusieurs directions, il est capable d'orienter les messages dans la bonne direction. C'est vraiment l'élément de base pour relier plusieurs machines. Tous les switches ne se valent pas en termes de caractéristiques, et ils se différencient principalement par :

- le nombre de ports allant de 4 à 96, permettant d'y connecter autant de machines
- le type de port : port RJ45 pour les câbles réseau standard, ou interface optique (type SFP+) pour la fibre optique. Ce sont les plus courants
- le débit possible sur chaque port : de 10 Mbp à 100 Gbp
- les fonctionnalités telles que l'interface de configuration, la compatibilité ou les modes de communication.

Le switch est le grand frère du **hub** (concentrateur). Un hub est un switch non intelligent, c'est-à-dire qu'il n'est pas capable de déterminer vers quelle direction (sur quel port), il doit envoyer un message. Il envoie alors le message sur tous ses ports en partant du principe que de cette manière, le message arrivera bien à destination.

## Différents types de SWITCH:

- administrable
- non administrable
- intelligent (sorte de mix des deux premier)

	SWITCH	HUB
Limite bande passante	Oui	Non
Envoi et reception données en simultané	Non	Oui
Sélection des terminaux individuels	Non	Oui
Diffusion	Oui	Oui
Analyse réseau sans miroir de port	Oui	Non
Modèle de travail OSI	Niveau 1	Niveau 2
Domaine de collision	Pour tous les ports	Pour les ports individuels

## Inconvénients HUB:

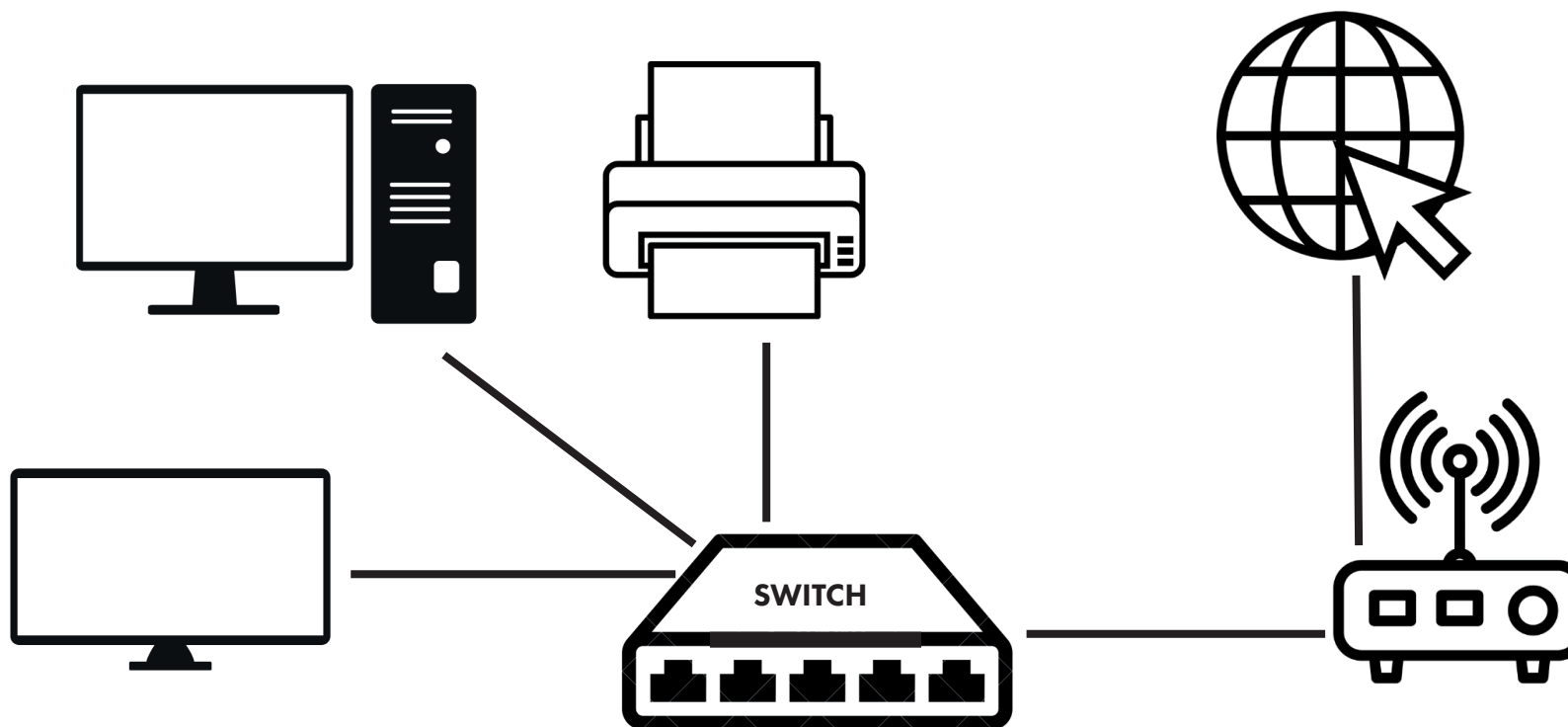
- perte de vitesse
  - faille de sécurité
  - manque de flexibilité
- [!] Obsolète mais peut toujours être utilisé dans le cadre d'une analyse réseau ou de la diffusion de contenu multimédia [!]

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

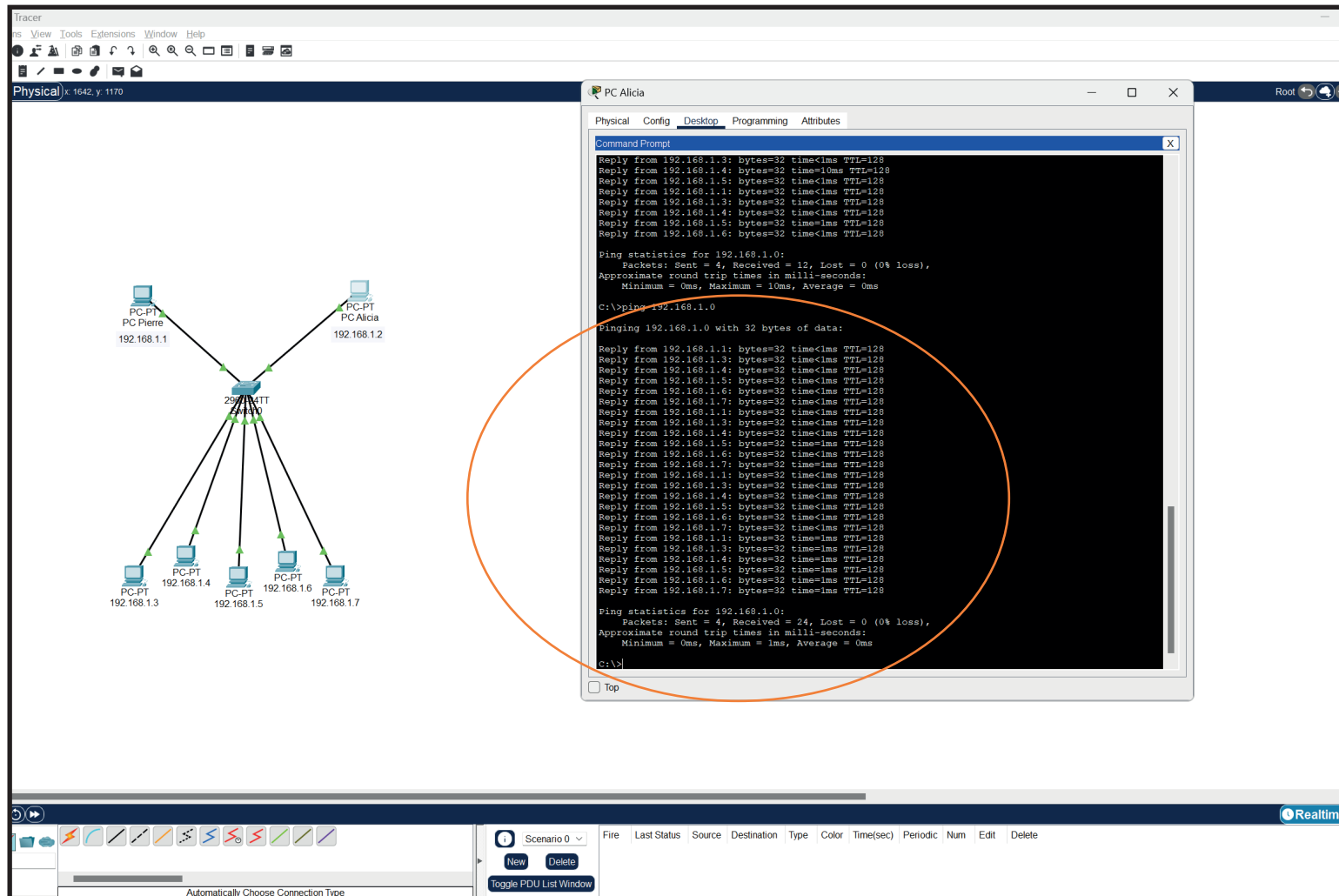
Au lieu de simplement fournir de l'électricité à plusieurs appareils, un switch réseau gère et achemine les données entre ces appareils. Il le fait en utilisant des ports RJ45, qui sont des prises réseau standard utilisées pour connecter des câbles Ethernet.

Il utilise une table d'adresses MAC pour garder une trace de tous les appareils connectés à lui. Lorsqu'il reçoit des données destinées à un appareil spécifique, il sait exactement à quel port envoyer ces données, ce qui réduit le trafic inutile et améliore l'efficacité du réseau.

Le switch réseau est particulièrement utile lorsque vous avez plusieurs périphériques à connecter à Internet. Il pallie les limites d'une mauvaise connexion WiFi en permettant l'installation d'un réseau câblé. C'est un élément essentiel pour créer un réseau informatique domestique ou d'entreprise fiable.



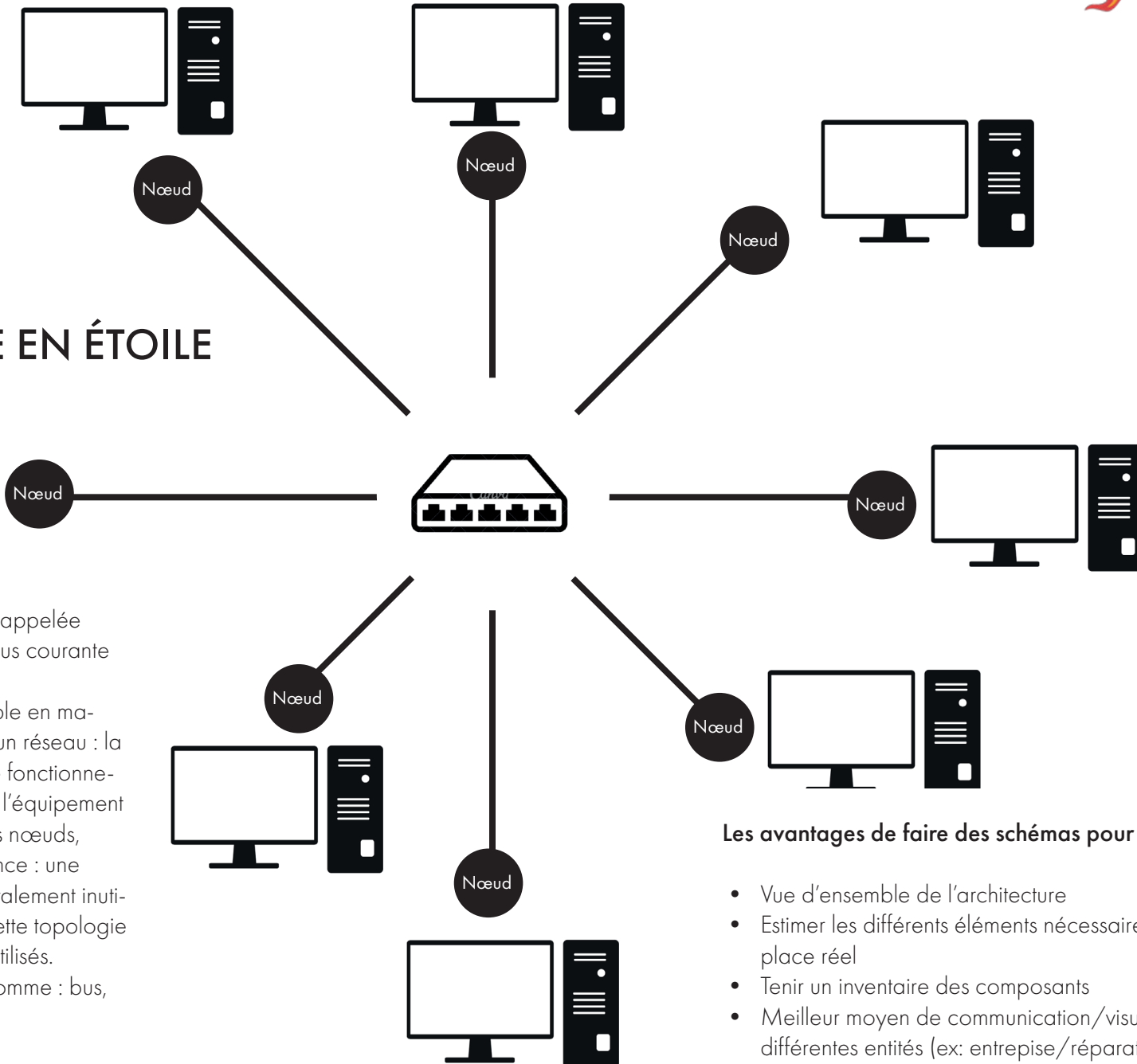
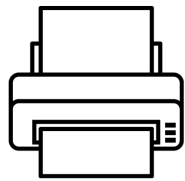
08



Ici on peut voir que tous les ordinateurs sont relié au même commutateur. Ici j'ai choisi d'en mettre un qui possède 24 ports FastEthernet, pour pouvoir accueillir toutes les machines.

Pour le ping, tous les Pc ont été configuré de manière à avoir une adresse IP unique mais qui appartient à la même plage d'adresse et possédant le même masque de sous-réseau.

## TOPOLOGIE EN ÉTOILE



La topologie **Réseau en étoile** aussi appelée Hub and spoke est la topologie la plus courante actuellement.

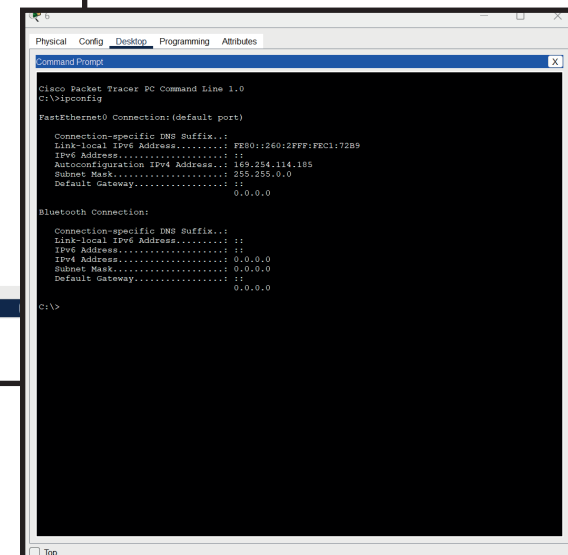
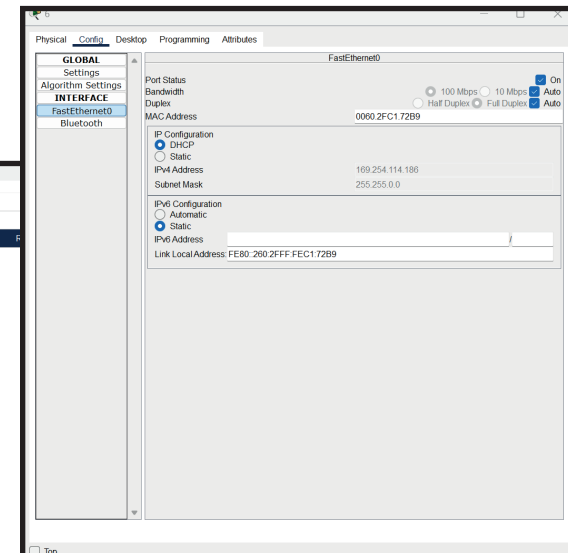
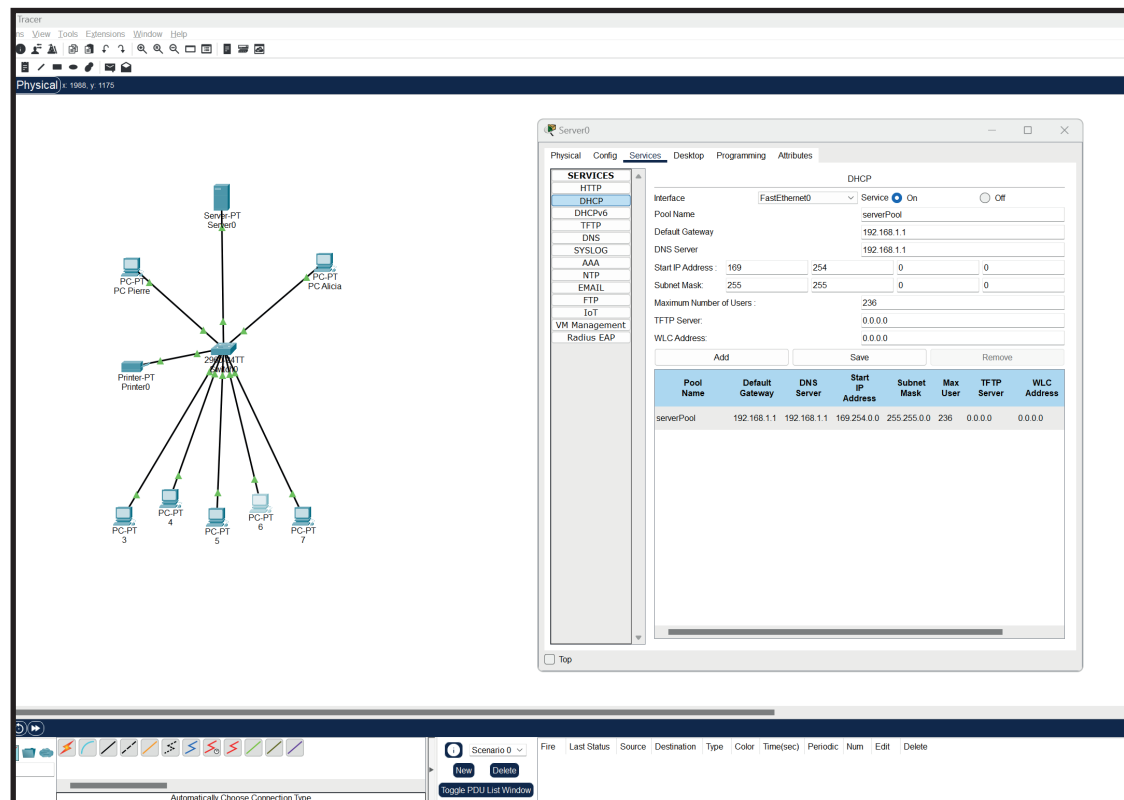
Omniprésente, elle est aussi très souple en matière de gestion et de dépannage d'un réseau : la panne d'un nœud ne perturbe pas le fonctionnement global du réseau. En revanche, l'équipement central, ici un switch) qui relie tous les nœuds, constitue un point unique de défaillance : une panne à ce niveau rend le réseau totalement inutilisable. L'inconvénient principal de cette topologie réside dans la longueur des câbles utilisés.

Il existe d'autres topologies réseau comme : bus, maillée, en anneau.

### Les avantages de faire des schémas pour un réseau :

- Vue d'ensemble de l'architecture
- Estimer les différents éléments nécessaires avant mise en place réel
- Tenir un inventaire des composants
- Meilleur moyen de communication/visualisation entre différentes entités (ex: entreprise/réparateur)

**DHCP** (Dynamic Host Configuration Protocol) signifie “protocole de configuration automatique des hôtes”. Ce mécanisme est très utilisé dans les réseaux LAN car il simplifie l'accès au réseau pour les utilisateurs. Une adresse IP est toujours allouée pour un temps défini par le serveur DHCP. Cela évite que les adresses IP soient affectées indéfiniment à des machines qui ne sont plus dans le réseau. Les grosses différences entre un **IP statique** et le DHCP est que les IP statiques doivent être rentrées manuellement de manière individuelles. Ce qui par exemple pour un administrateur réseau qui a des centaines d'adresses à créer peut être très fastidieux. Comme leurs noms l'indiquent, l'un est statique donc il ne change pas. L'autre est dynamique, elle change donc très régulièrement et évite les manipulations de mise à jour.



1  
1

Adresse Réseau Principal : **CLASS A 10.0.0.0**

T T  
 partie partie  
 réseau hôte  
 (0-127) (1-254)

1

Masque de sous-réseau : **255.255.255.0 (/24)**

SOUS-RÉSEAU 1

Plage d'adresses : **10.0.0.1 - 10.0.0.254**  
Adresse de diffusion : **10.0.0.255**

SOUS-RÉSEAU 2

Plage d'adresses : **10.0.1.1 - 10.0.0.254**  
Adresse de diffusion : **10.0.1.255**

SOUS-RÉSEAU 3

Plage d'adresses : **10.0.2.1 - 10.0.2.254**  
Adresse de diffusion : **10.0.1.255**

SOUS-RÉSEAU 4

Plage d'adresses : **10.0.3.1 - 10.0.3.254**  
Adresse de diffusion : **10.0.3.255**

SOUS-RÉSEAU 5

Plage d'adresses : **10.0.4.1 - 10.0.4.254**  
Adresse de diffusion : **10.0.4.255**

IP demandé : 800 (160/S-R)  
 IP dispo : 1270 (254/S-R)  
 IP restant : 470 (94/S-R)

2

Masque de sous-réseau : **255.255.255.128 (/25)**

SOUS-RÉSEAU 6

Plage d'adresses : **10.0.5.1 - 10.0.5.126**  
Adresse de diffusion : **10.0.5.127**

SOUS-RÉSEAU 7

Plage d'adresses : **10.0.5.129 - 10.0.5.254**  
Adresse de diffusion : **10.0.5.255**

SOUS-RÉSEAU 8

Plage d'adresses : **10.0.6.1 - 10.0.6.126**  
Adresse de diffusion : **10.0.6.127**

SOUS-RÉSEAU 9

Plage d'adresses : **10.0.6.129 - 10.0.6.254**  
Adresse de diffusion : **10.0.6.255**

SOUS-RÉSEAU 10

Plage d'adresses : **10.0.7.1 - 10.0.7.126**  
Adresse de diffusion : **10.0.7.127**

IP demandé : 600 (120/S-R)  
 IP dispo : 630 (126/S-R)  
 IP restant : 30 (6/S-R)



1  
1

3

Masque de sous-réseau : **255.255.255.224 (/27)**

SOUS-RÉSEAU 11 — Plage d'adresses : **10.0.7.129 - 10.0.7.158**  
Adresse de diffusion : **10.0.7.159**

SOUS-RÉSEAU 12 — Plage d'adresses : **10.0.7.161 - 10.0.7.190**  
Adresse de diffusion : **10.0.7.191**

SOUS-RÉSEAU 13 — Plage d'adresses : **10.0.7.193 - 10.0.7.222**  
Adresse de diffusion : **10.0.7.223**

SOUS-RÉSEAU 14 — Plage d'adresses : **10.0.7.225 - 10.0.7.254**  
Adresse de diffusion : **10.0.7.255**

SOUS-RÉSEAU 15 — Plage d'adresses : **10.0.8.1 - 10.0.8.30**  
Adresse de diffusion : **10.0.8.31**

IP demandé : 150 (30/S-R)  
IP dispo : 150 (30/S-R)  
IP restant : 0 (0/S-R)

Il reste  
**502 Hôtes dispo**

4

Masque de sous-réseau : **255.255.255.240 (/28)**

SOUS-RÉSEAU 16 — Plage d'adresses : **10.0.8.33 - 10.0.8.46**  
Adresse de diffusion : **10.0.8.47**

IP demandé : 12 (12/S-R)  
IP dispo : 14 (14/S-R)  
IP restant : 2 (2/S-R)

Pour faire cet adressage réseau, j'ai utilisé une méthode qu'on appelle **VLSM** qui est une technique qui permet de créer des sous-réseaux de différentes tailles à partir d'un réseau IPv4 global. Cette technique est particulièrement utile pour maximiser l'utilisation des adresses IP. Cela permet aussi d'optimiser la gestion du réseau en réduisant le trafic de diffusion. Pour cela je suis partie des sous réseau les plus demandeurs à savoir ceux de 160 hôtes.

### ●●● Pourquoi on à utilisé une IPV4 de classe A?

Les adresses de **classes A** sont généralement utilisé pour les grands réseaux. Elle est découpé de manière à ce que le premier octet (celui à gauche) soit réservé pour le réseau et les 3 octets suivant pour les hôtes . Ce qui permet d'avoir une grande plage d'adresse IP, permettant de créer de nombreux sous réseaux et ipso facto d'accueillir un grand nombres d'hôtes.

Dans le cadre de l'exercices on aurait même pu utilisé une adresse de classe B.

### ●●● Les autres classes ?

- **Classe B** : Les adresses de classe B ont deux octets de réseau et deux octets d'hôte. Elles sont adaptées aux réseaux de taille moyenne.
- **Classe C** : Les adresses de classe C ont trois octets de réseau et un octet d'hôte. Elles sont couramment utilisées pour les réseaux de petite taille, tels que les réseaux domestiques.
- **Classe D** : Les adresses de classe D sont réservées pour les adresses multicast utilisées pour le streaming de données.
- **Classe E** : Les adresses de classe E sont réservées à des fins expérimentales et ne sont généralement pas utilisées dans les réseaux publics.

### ●●● Découpage du sous-réseau ?

En tant que concept, le découpage en sous-réseaux divise le réseau en parties plus petites appelées sous-réseaux. Cette opération est effectuée avec les bits empruntés à la partie hôte de l'adresse IP, ce qui permet une utilisation plus efficace de l'adresse réseau. Un masque de sous-réseau définit la partie de l'adresse utilisée pour identifier le réseau et distinguer les serveurs.

- Un masque de sous-réseau est une suite de bits qui détermine la taille de la partie réseau et la taille de la partie hôte d'une adresse IP.

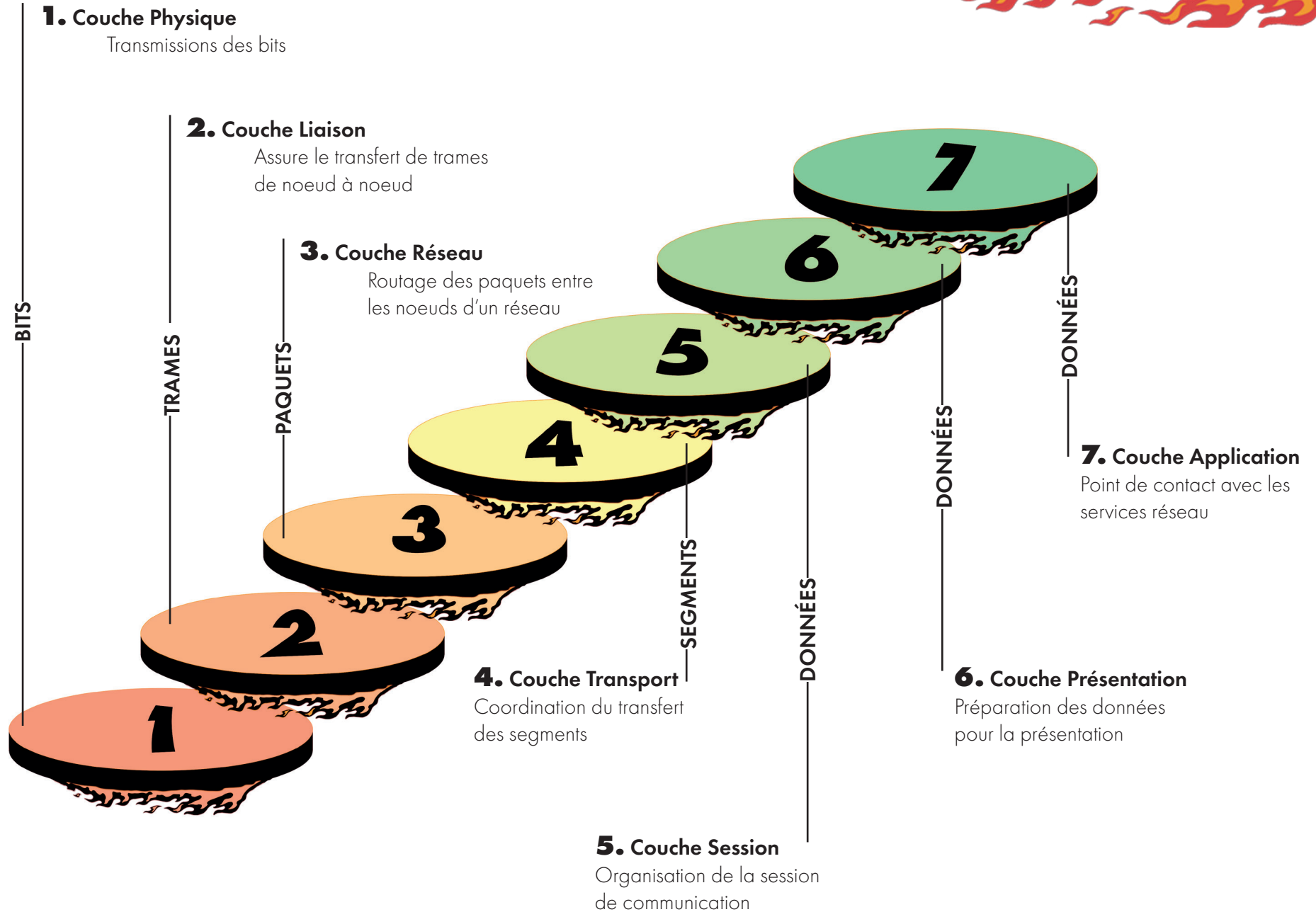
**Un bit à 1 dans le masque représente la partie réseau, tandis qu'un bit à 0 représente la partie hôte.**

- La notation en barre oblique (/X) indique combien de bits dans l'adresse IP sont réservés pour la partie réseau.

Par exemple, pour le sous-réseaux de 120 hôtes :

Besoin de 120 hôtes, ce qui peut être satisfait avec 7 bits ( $2^7 = 128$ , mais 2 adresses sont réservées pour le réseau et la diffusion, il reste donc 126 hôtes). Le masque de sous-réseau est (/25) car 7 bits sont alloués pour la partie hôte.

1  
2



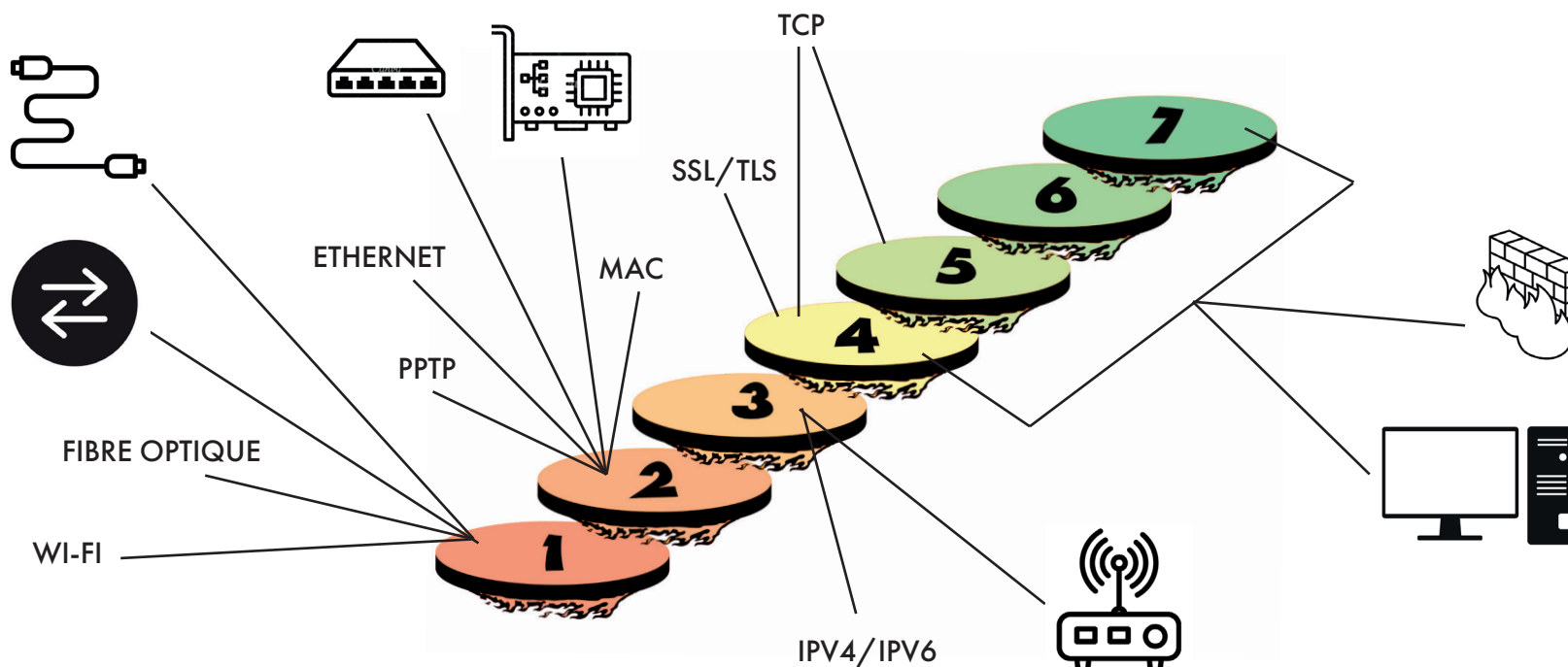
### ... Organisation des couches ?

L'objectif d'un réseau, c'est de permettre aux machines de communiquer entre elles. Pour que ça se passe bien entre les différentes entités, il existe des règles d'uniformisations. On retrouve deux catégories de règles :

- les **normes** qui sont des règles matérielles
- les **protocoles** qui sont des règles logicielles

Le **modèle OSI** propose de classer chacune de ces règles à différents niveaux, sur un total de 7 niveaux qu'on appelle aussi des couches. Chacune de ces couches porte un nom relatif à sa fonction. Chaque acteur ou "élément" du réseau aura besoin des règles d'une couche bien spécifique. Les règles des autres couches ne l'intéresseront pas, et souvent il ne les comprendra même pas.

On peut alors associer chaque élément à une couche :





13

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

## ●●● Architecture du réseau ?

Ici on a une **topologie de réseau en étoile**, tous les périphériques (serveur et ordinateurs) sont connectés au même switch qui agit comme une sorte de point chaud central où toutes les informations circulent et sont accessibles. Il semblerait que ce soit un réseau LAN (local network area)

## ●●● Adresse IP du réseau ?

L'adresse IP du réseau est **192.168.10.0**, car c'est la première adresse possible dans la plage d'adresses IP de classe C (192.168.10.0 à 192.168.10.255) avec le masque de sous-réseau de 255.255.255.0.

## ●●● A combien on peut être sur ce réseau?

Avec un masque de sous-réseau de 255.255.255.0, il a donc 1 octet réservé hôte. Cela signifie que  $2^8 - 2$  adresses sont disponibles, car deux adresses (l'adresse réseau et l'adresse de diffusion) sont réservées. Donc, on peut brancher jusqu'à **254 machines** sur ce réseau.

## ●●● Adresse de diffusion?

L'adresse de diffusion est l'adresse réservée pour envoyer un message à toutes les machines sur le réseau. Dans un réseau avec un masque de sous-réseau de 255.255.255.0, l'adresse de diffusion est celle où tous les bits d'hôte sont définis sur 1. Donc, pour ce réseau, l'adresse de diffusion permettant d'envoyer un message à tous les ordi en même temps est **192.168.10.255**.

14

145.32.59.24

	8 <sup>eme</sup> bit	7 <sup>eme</sup> bit	6 <sup>eme</sup> bit	5 <sup>eme</sup> bit	4 <sup>eme</sup> bit	3 <sup>eme</sup> bit	2 <sup>eme</sup> bit	1 <sup>eme</sup> bit
	$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
	128	64	32	16	8	4	2	1
1 <sup>oct</sup>	1	0	0	1	0	0	0	1
2 <sup>oct</sup>	0	0	1	0	0	0	0	0
3 <sup>oct</sup>	0	0	1	1	1	0	1	1
4 <sup>oct</sup>	0	0	0	1	1	0	0	0

10010001.00100000.00111011.00011000

200.42.129.16

1 <sup>oct</sup>	1	1	0	0	1	0	0	0
2 <sup>oct</sup>	0	0	1	0	1	0	1	0
3 <sup>oct</sup>	1	0	0	0	0	0	0	1
4 <sup>oct</sup>	0	0	0	1	0	0	0	0

11001000.00101010.10000001.00010000

14.82.19.54

1 <sup>oct</sup>	0	0	0	0	1	1	1	0
2 <sup>oct</sup>	0	1	0	1	0	0	1	0
3 <sup>oct</sup>	0	0	0	1	0	0	1	1
4 <sup>oct</sup>	0	0	1	1	0	1	1	0

00001110.01010010.00010011.00110110



# 15

## ●●● Qu'est-ce que le routage ?

Le routage est le processus de transmission de données d'un point à un autre à travers un réseau ou entre différents réseaux. Il implique la prise de décisions sur la manière de faire passer ces données d'un nœud à un autre, en utilisant les chemins les plus efficaces et les plus appropriés. Le routage est essentiel pour l'acheminement du trafic sur Internet et dans tout réseau informatique. Les routeurs sont les dispositifs clés du routage, car ils déterminent les chemins que les données doivent emprunter en fonction des adresses IP, des tables de routage et des protocoles de routage.

## ●●● Qu'est-ce qu'un gateway ?

Une passerelle (gateway) est un dispositif ou un logiciel qui relie deux réseaux informatiques hétérogènes, permettant la communication entre eux. Les passerelles servent de points d'entrée ou de sortie entre les réseaux et sont souvent responsables de la traduction des protocoles, de la conversion des données ou de la gestion des règles de sécurité pour assurer une communication fluide entre les réseaux. Par exemple, une passerelle peut être utilisée pour connecter un réseau local (LAN) à Internet ou pour relier des réseaux utilisant différents protocoles de communication.

## ●●● Qu'est-ce qu'un VPN ?

Un VPN (Virtual Private Network, ou réseau privé virtuel) est une technologie qui permet de créer un réseau sécurisé en utilisant une infrastructure de réseau public, généralement Internet. Les VPN utilisent des protocoles de chiffrement pour sécuriser les données transitant entre un utilisateur et un réseau distant. Cela garantit la confidentialité et la sécurité des données, ce qui est particulièrement utile pour les communications à distance. Les VPN sont couramment utilisés pour accéder à distance à des ressources d'entreprise, protéger la vie privée en ligne, contourner la censure, ou relier des sites distants de manière sécurisée.

## ●●● Qu'est-ce qu'un DNS ?

Le DNS (Domain Name System, ou système de noms de domaine) est un service essentiel sur Internet qui traduit les noms de domaine en adresses IP compréhensibles par les ordinateurs. Les ordinateurs utilisent des adresses IP pour identifier et atteindre d'autres ordinateurs sur un réseau, mais les humains préfèrent utiliser des noms de domaine pour accéder aux sites Web. Le DNS sert de système d'annuaire qui associe les noms de domaine à des adresses IP, permettant ainsi de localiser des ressources sur Internet. Le DNS facilite la navigation sur le Web, l'envoi de courriels et d'autres opérations en ligne en convertissant des noms de domaine en adresses IP.