

# Sécurité IP et administration réseau

BLOC 1 - BLOC 3 - BTS SIO  
A.BRES



# Sommaire

**01**

## Pourquoi Internet ?

Retour dans les années 1960 en pleine Guerre Froide.

**02**

## Le fonctionnement d'Internet

Le fonctionnement d'Internet et des réseaux de communications.

**03**

## La notion de réseau

Point de situation sur les différents environnements.

**04**

## Modèle OSI

Gestion des couches OSI, des équipements et protocoles associés.



# 01

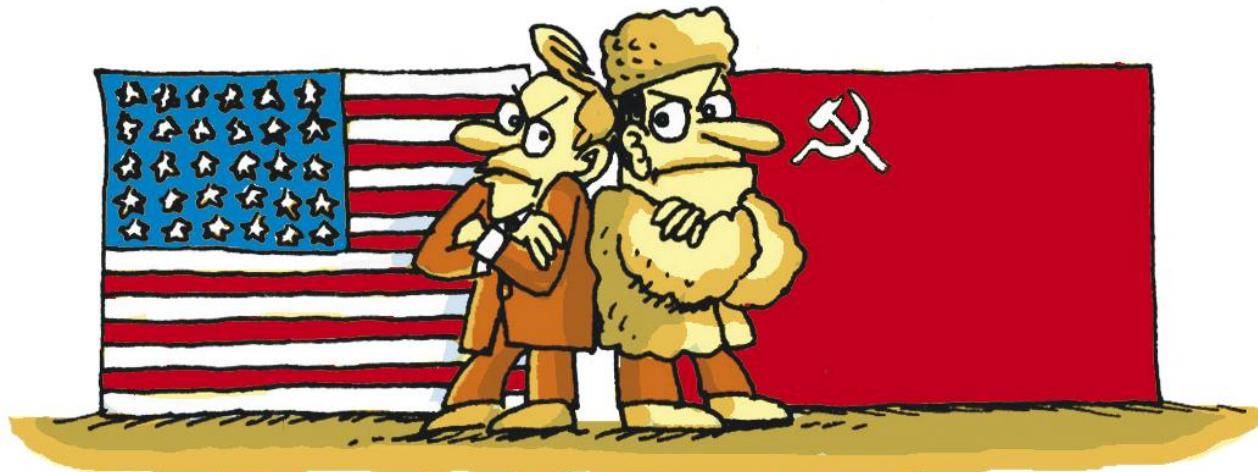
## Pourquoi Internet ?

Back to 1962 !



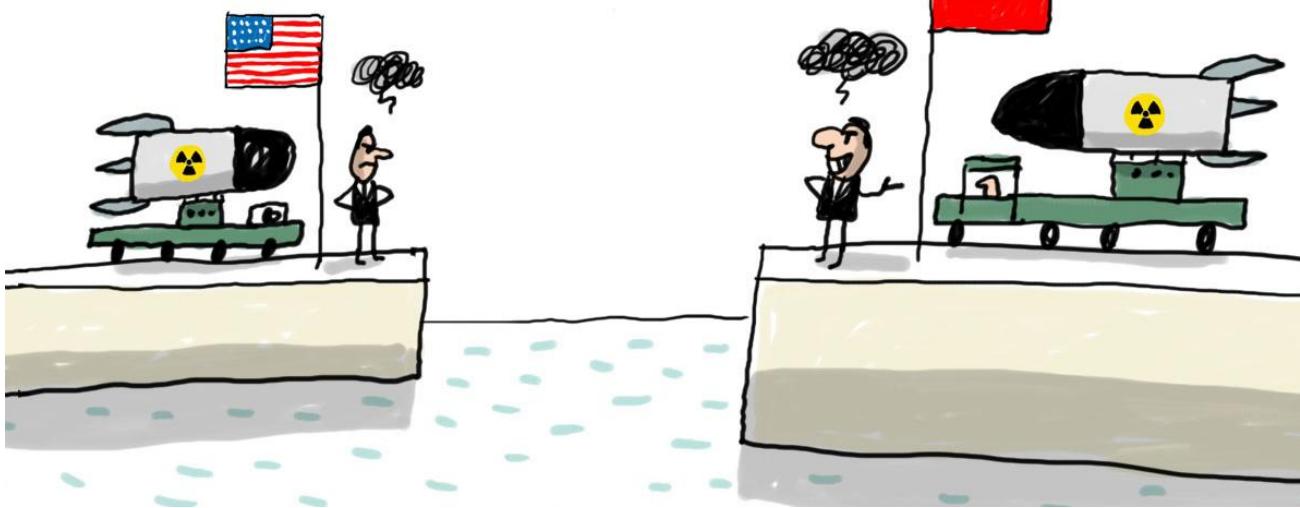
# La Guerre Froide...

La [Guerre Froide \(1947-1991\)](#) fut une période tendue de tensions géopolitiques entre les États-Unis et l'Union Soviétique, sans conflit militaire direct, au lendemain de la capitulation de l'Allemagne Hitlérienne. Les deux superpuissances ont rivalisé pour l'influence mondiale, adoptant des idéologies opposées (capitalisme vs communisme). Les confrontations indirectes ont eu lieu à travers des alliances et [des compétitions technologiques \(course à l'espace, guerre nucléaire\)](#). Cette période s'est conclue avec l'effondrement de l'Union Soviétique, marquant la fin de la bipolarité mondiale.

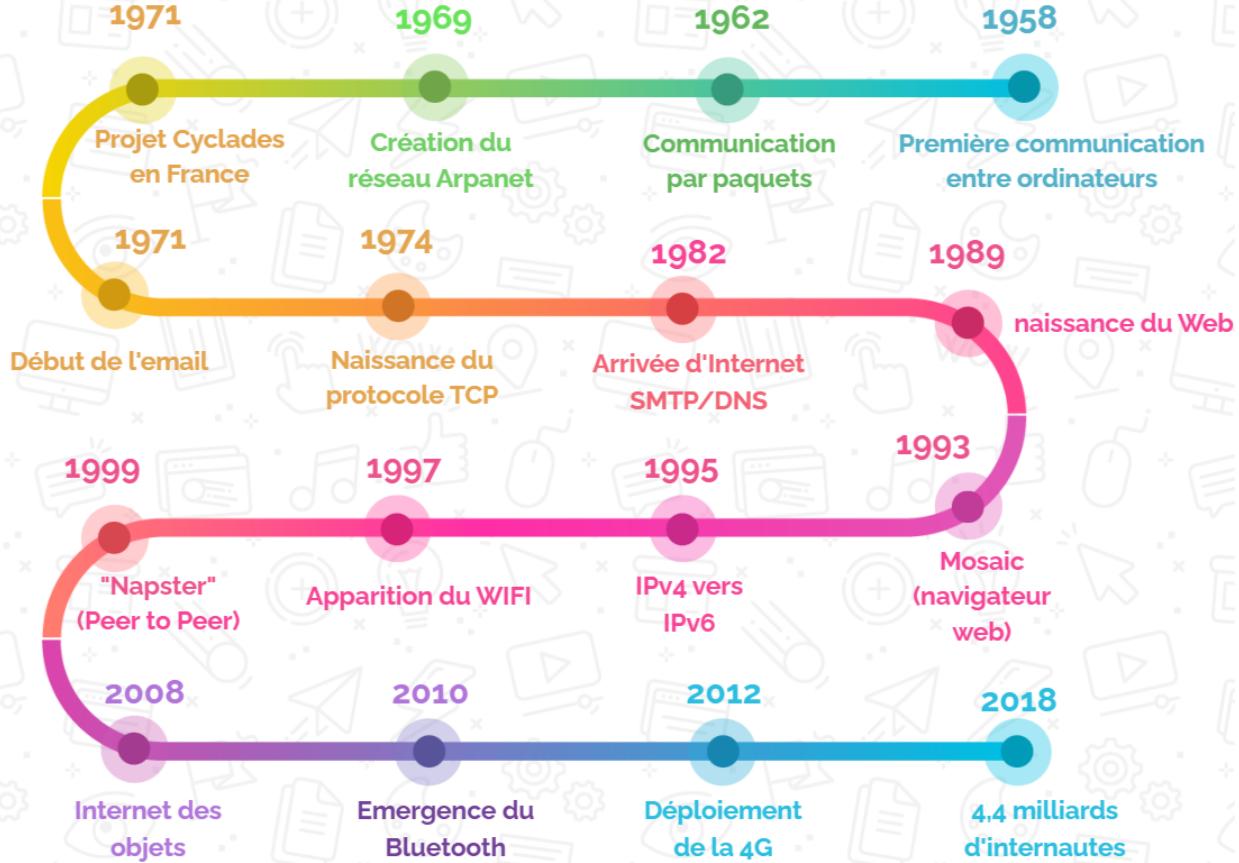


# La Guerre Froide...

En 1969, en pleine Guerre Froide, l'US Air Force charge un ingénieur, Paul BARAN, de créer un réseau de communication militaire **pouvant résister à une attaque nucléaire**. C'est alors que naît l'idée d'**ARPANET**, ... un réseau constitué d'une multitude de réseaux. En 1983, ARPANET devient **Internet** (démilitarisé).



# FRISE CHRONOLOGIQUE HISTOIRE D'INTERNET





Un téléphone mobile



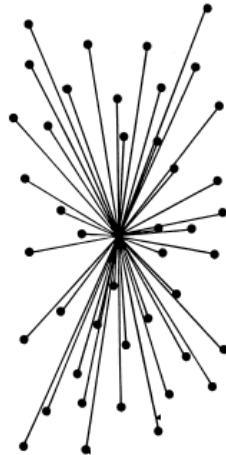
Un téléphone fixe



La radio



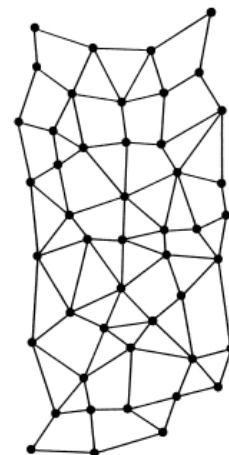
Un télégraphe



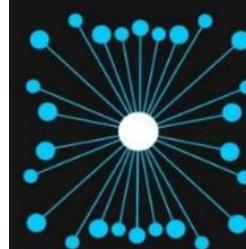
Centralisé



Décentralisé

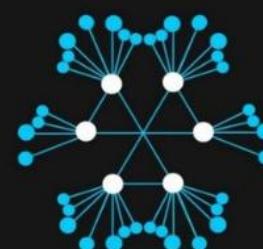


Distribué



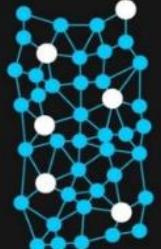
Centralized Network

All the nodes are connected under a single authority



Decentralized Network

No single authority server controls the nodes, they all have individual entity



Distributed Network

Every node is independent and interconnected with each other



La cybersécurité a commencé à être une préoccupation dès les premiers jours de l'informatique, lorsque les premiers ordinateurs ont été utilisés à des fins militaires et gouvernementales. La préoccupation initiale était la protection des informations sensibles.

# Cybersécurité

Le virus « Creeper » est l'un des premiers exemples de logiciel malveillant. Il a été créé en 1971 par Bob THOMAS. Creeper n'était pas un virus au sens moderne du terme, mais plutôt un programme expérimental qui se propageait au travers d'ARPANET.

Il était conçu pour s'exécuter sur les ordinateurs hôtes d'un réseau ARPANET et affichait le message « I'm the creeper, catch me if you can! ». Une fois exécuté, il utilisait le réseau pour se déplacer entre les ordinateurs. Il se copiait sur différents postes. Un programme appelé « Reaper » a été conçu pour traquer et supprimer Creeper des ordinateurs infectés.

« Creeper » était plus une expérience et une démonstration de la capacité d'un programme à se déplacer et « Reaper » un antivirus précoce. Creeper n'a pas causé de dommages graves, mais il a marqué le début de la réflexion sur la sécurité informatique et la nécessité de développer des mécanismes pour protéger les systèmes informatiques contre les menaces potentielles.



# Cybersécurité

Les attaques informatiques sont devenues de plus en plus sophistiquées, avec l'émergence de groupes de cybercriminels et d'acteurs étatiques impliqués dans le **cyberespionnage** et la **cybercriminalité**.

Les gouvernements ont commencé à mettre en place des **réglementations** sur la cybersécurité pour protéger les données **personnelles** et **financières**. De plus, la sensibilisation accrue du public aux questions de cybersécurité a renforcé l'importance de la protection en ligne.

Des cyberattaques notables telles que [Stuxnet](#) en 2010, qui a ciblé les infrastructures industrielles en Iran, et les attaques de ransomware ([WannaCry](#) en 2017) ont attiré l'attention mondiale sur les implications graves des cyberattaques.

La cybersécurité reste un domaine **en constante évolution** en réponse aux nouvelles menaces et aux avancées technologiques. Les entreprises et les gouvernements continuent d'investir dans la prévention, la détection et la réponse aux cyberattaques pour protéger leurs systèmes et leurs données.



# Micode – Wanna Cry - 2017



# TP !

Effectuez un travail de comparaison entre  
**WannaCry** et **Stuxnet** sur les points :

Origine & contexte ; mécanismes de propagation  
; cibles & impacts ; caractéristiques techniques ;  
réponses et contre-mesures.

# Internet aujourd'hui ?

Chiffres OpenClassrooms

- 42% internautes sont Asiatiques ;
- 1,6% internautes sont Français ;
- 78% des Américains ont Internet ;
- 10% des Africains ont Internet ;
- 1/3 personnes ont accès à Internet ;
- Pays avec le plus de connexions Internet : **Corée du Sud** ;
- Le nombre d'internautes a été multiplié par **4,5 entre 2000 et 2010**.
- Aller plus loin : [ARPANET](#)
- Aller plus loin : [World Wide Web](#)



# 02



# Fonctionnement d'Internet

Comment ça marche ?



# Idée de fonctionnement générale



Afin de **ne pas surcharger les réseaux** et limiter le temps d'attente en cas de perte d'informations, les messages sont **découpés en plusieurs paquets** partant vers leur destination, avant de se **recomposer** chez le destinataire final.

# Idée de fonctionnement générale



## Génération d'un requête

Une **requête** est générée par le **client** pour le **serveur**.



## Envoie sur Internet

La requête sort du **LAN** vers le **WAN** après encapsulation.



## Réception de la requête

La requête arrive dans le **LAN** ou la **DMZ** et est **décapsulée**.

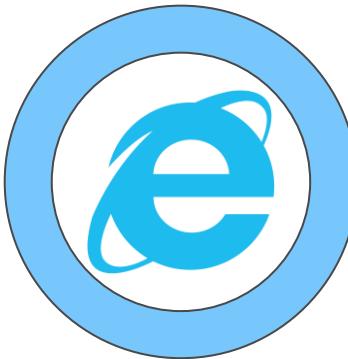


## Traitement

Le **serveur** final reçoit la requête et la **traite**.

Sur l'ensemble du chemin, il est possible que la **requête** parcoure des **centaines**, voire des **milliers** de kilomètres de **câbles** en tous genres et **d'équipements** réseaux. Cette requête va également être convertie, amplifiée, chiffrée, déchiffrée, atténuee...Bref, elle va vivre !





## Définition d'Internet.

Définition Insee

Ensemble de réseaux mondiaux interconnectés qui permettent à des ordinateurs et à des serveurs de communiquer efficacement au moyen d'un protocole de communication commun : Internet Protocol. Ses principaux services sont le Web, le FTP, la messagerie et les groupes de discussion.

...



# Question !

Selon vous, *si elle existe*, quelle est la différence entre **Web** et **Internet** ?

# Différence entre Web et Internet

## Internet

Internet peut exister sans le web, mais pas l'inverse !  
Internet peut être défini comme **le contenant** et le web comme **le contenu**. Internet est le **réseau informatique mondial** sur lequel s'appuient de nombreux **autres services**, dont le Web.

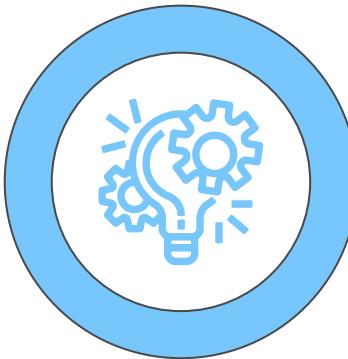
## Le web

Le web n'est qu'une application d'Internet **distincte des autres applications** comme la messagerie électronique, les transferts de fichiers, les messageries instantanées, les jeux en ligne etc... Son rôle est d'afficher **des pages HTML**. Son abréviation est **WWW**.

**Internet = Interconnected Network** (soit le réseau informatique mondial qui interconnecte tous les serveurs du monde entre eux).

# Captain Gizmo - Most Popular Websites 1993 - 2023





## Définition d'un SI.

Définition Gendarmerie

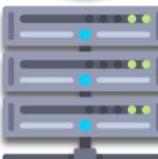
Un **Système d'Information** est un ensemble organisé de ressources (techniques, organisationnelles, humaines) qui permettent d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire l'Information. Le SI est géré par la DSI, **Direction des Systèmes d'Informations**.

# Comment accéder aux serveurs reliés ?



Protocoles

**HTTP  
SMTP  
FTP  
POP3  
IMAP**



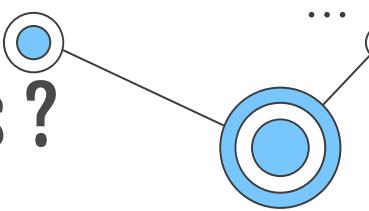
Adresse IP

IP: 194.250.250.01

IP: 194.250.250.02

IP: 195.250.250.03

IP: 195.250.250.04



# TD !

À l'aide de la [commande nslookup](#) sur votre terminal Windows et du site [mon-adresse-ip.fr](#), localisez votre Data-Center de [facebook.com](#) France.



Routeur CISCO 7201



Switch Extreme Network 4950



Access Point Wifi UnFi AC Lite



Pare-Feu Stormshield SN710

\* Document Annexe : Les différents supports et câbles réseau



Courants Porteurs en Ligne (CPL)



Module SFP+



Fibre optique

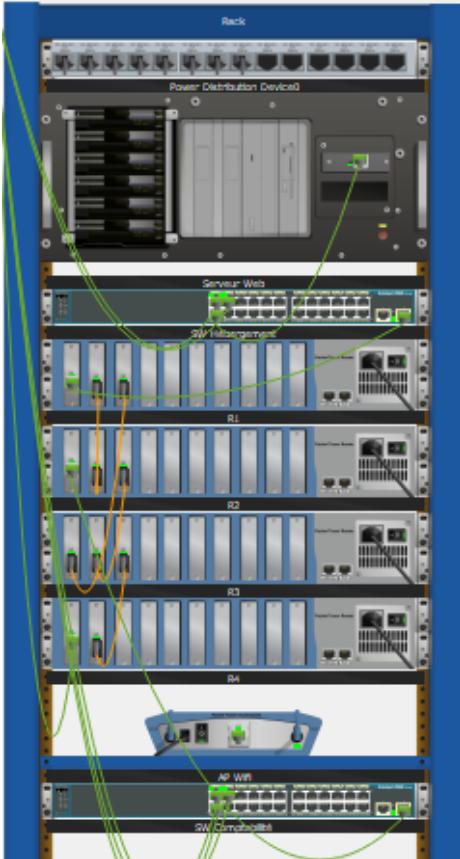


Câble cuivre RJ45



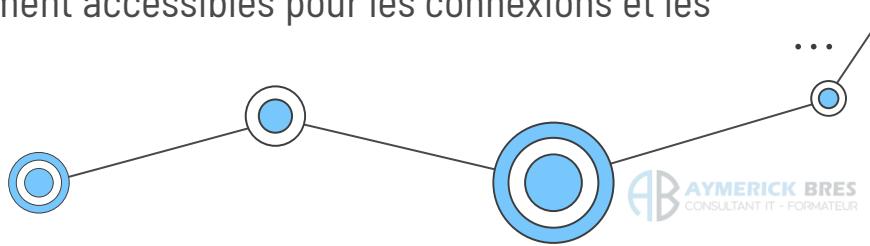
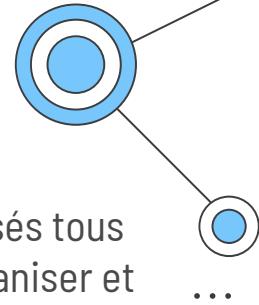
Câble coaxial

# Baie et Bandeau



Une **baie de brassage** est une armoire où sont centralisés tous les câbles réseau de votre entreprise. Elle permet d'organiser et de connecter facilement les câbles qui relient vos ordinateurs, serveurs, routeurs et autres équipements. En gardant tous les câbles bien rangés et accessibles, la baie de brassage facilite la gestion du réseau et la résolution des problèmes.

Un **bandeau optique** est un panneau utilisé pour organiser et connecter les câbles à fibres optiques. Ces câbles transportent des données à très haute vitesse et sur de longues distances. Le bandeau optique assure que les fibres optiques sont bien protégées et facilement accessibles pour les connexions et les modifications.





# 402 Tbit/s

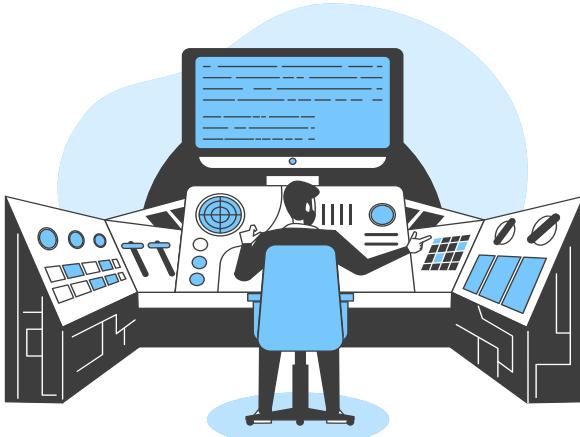
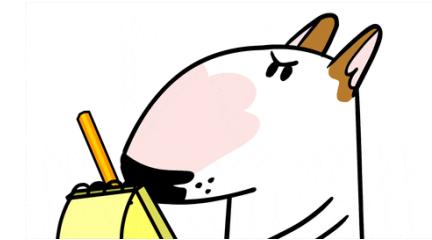
Record de vitesse de transfert  
établi sur une fibre optique  
commerciale. 27/06/2024

[Source.](#)

# Résumons la situation



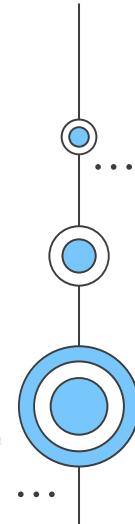
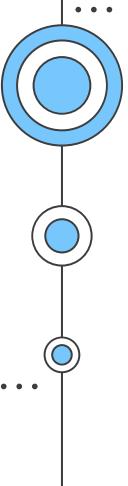
- La Guerre Froide est l'élément déclencheur de la course aux communications mondiales ;
- Il aura fallu seulement 60 ans pour passer d'un PoC à l'Internet d'aujourd'hui ;
- Internet est et reste une notion complexe à définir ;
- Plusieurs équipements sont nécessaires pour faire fonctionner une chaîne de connexion ;
- Pour raccorder plus de 2 machines entre elles, vous devez intégrer un équipement réseau ;
- Le choix du support physique a un impact sur les performances de votre réseau ;
- Une baie de brassage est l'armoire centralisant vos connexions réseaux physiques.



# 03

## La notion de réseaux...

Plusieurs  
environnements  
possibles.



# Différents environnements de réseaux



## Local Area Network (LAN)

Les LAN sont les réseaux à l'échelle locale (réseaux domestiques, réseaux d'entreprises). Ce type de réseau utilise généralement un **adressage IP non routable** sur Internet.

Il est généralement **possible d'intervenir** sur la **commutation** des trames ou sur le **routage** des paquets.



## Wide Area Network (WAN)

Les WAN sont des réseaux de réseaux à l'échelle mondiale (couverture par pays, continent ou planète entière), dont le plus connu est **Internet**. Ce dernier est lui-même composé de MAN, de LAN et de DMZ.

Il **n'est plus possible d'intervenir** sur le **routage** ou la **commutation**. Ces points sont désormais à la charge des opérateurs.

# Différents environnements de réseaux



## Personal Area Network (PAN)

Les PAN sont des réseaux utilisés pour la communication entre les dispositifs à proximité immédiate d'une personne, typiquement dans un rayon de quelques mètres, comme, par exemple, le NFC ou le Bluetooth pour effectuer des paiements sans contact, ou pour connecter des équipements sans fil.

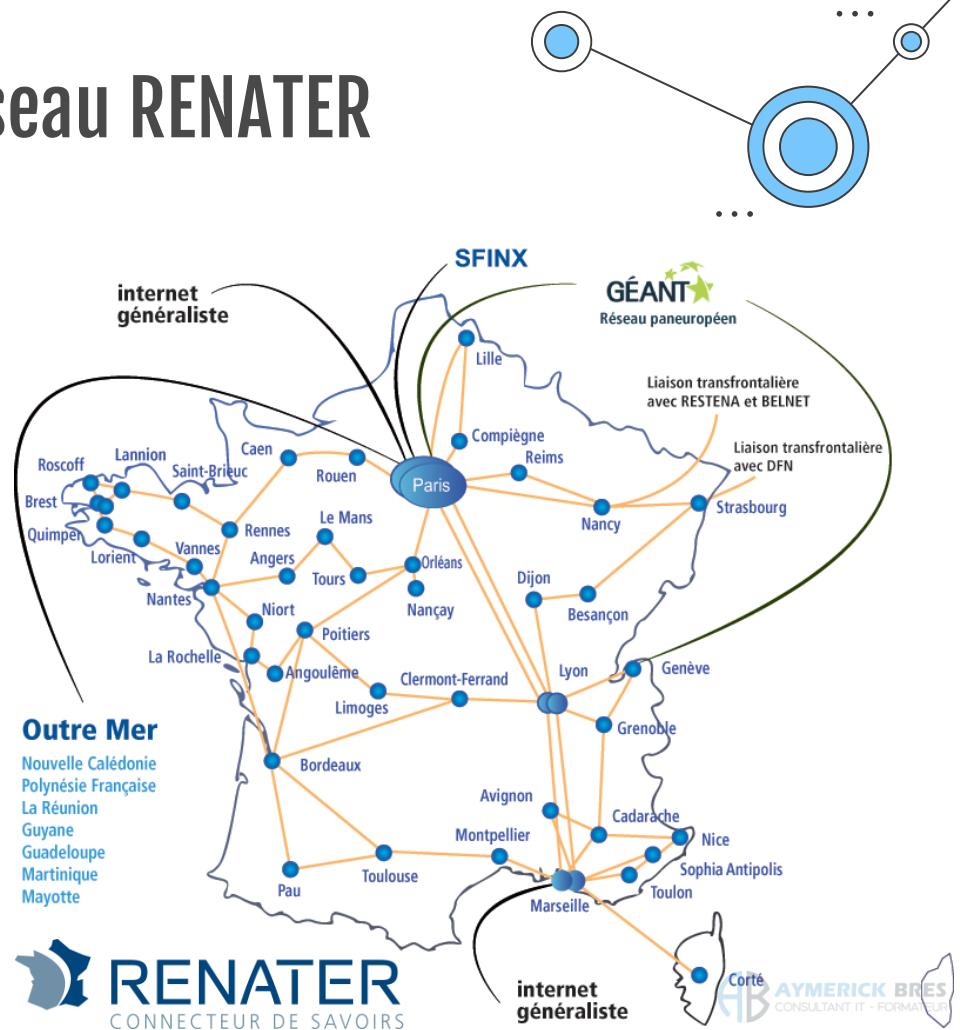


## Storage Area Network (SAN)

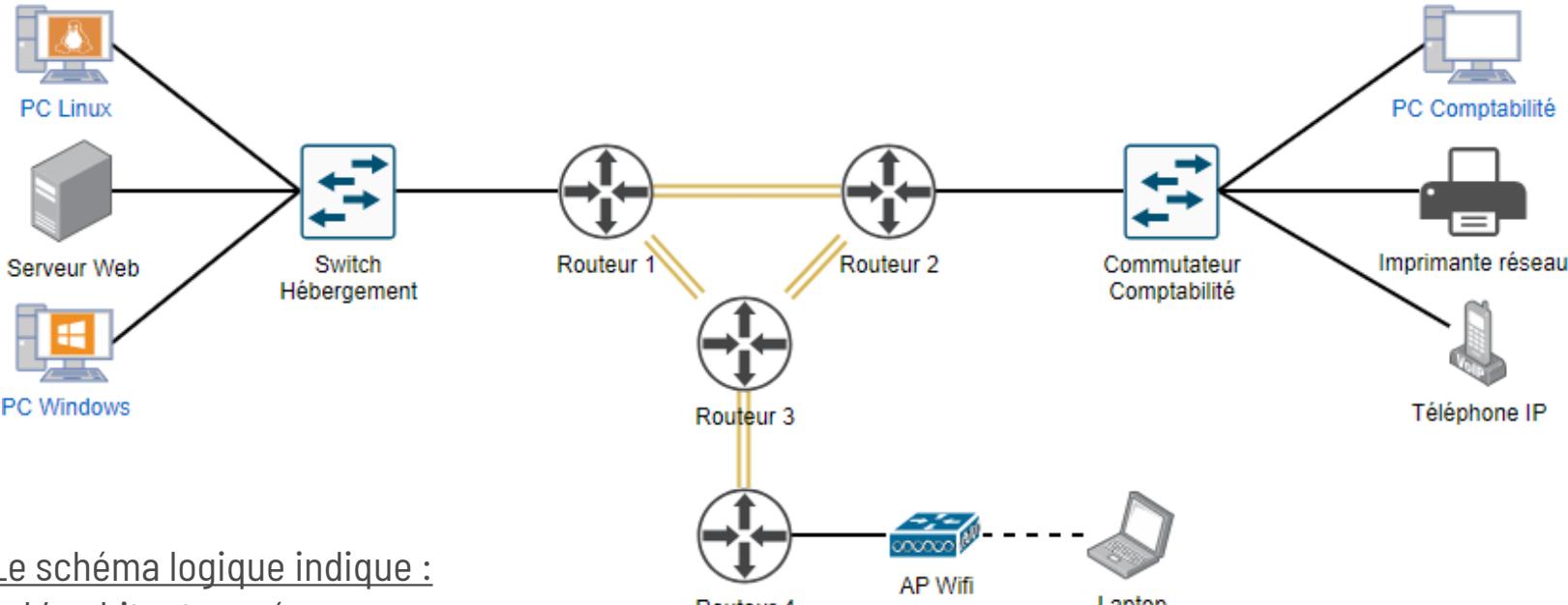
Les SAN sont des réseaux dédiés au stockage des données. Il permet de relier des serveurs à des baies de stockage (disques durs, bandes, etc.) de manière centralisée. Il est généralement limité à un site unique mais optimisé pour les transferts de données rapides et le stockage de grandes quantités de données.

# MAN : Le réseau RENATER

Les **Metropolitan Area Network** sont déployés à l'échelle d'une ville (réseaux universitaires, service public). Il peut être composé de plusieurs LAN. Ainsi, on peut retrouver un **plan d'adressage public comme privé**. Il commence à être difficile d'intervenir sur le routage ou la commutation.



# La schématisation logique d'un réseau



Le schéma logique indique :

- L'architecture réseau,
- Le plan d'adressage IP,
- Le type d'équipement,
- Éventuellement certains aspects de la configuration logicielle.

# TD !

Reproduisez le **schéma logique** de la slide  
précédente sur le logiciel **CISCO PACKET  
TRACER**.

# La schématisation physique d'un réseau

Schéma physique

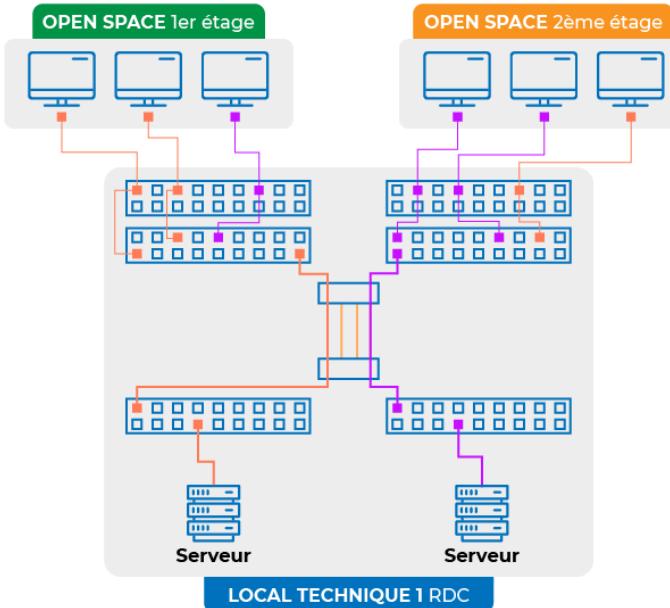
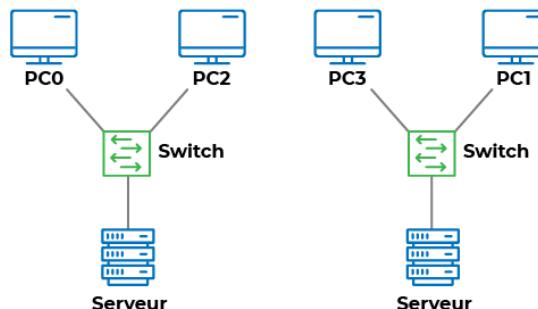


Schéma logique

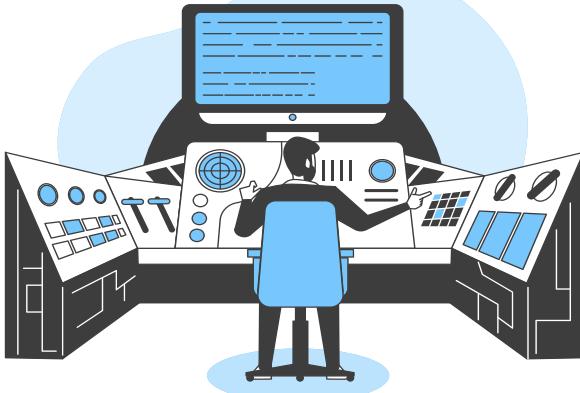


Le schéma physique indique :

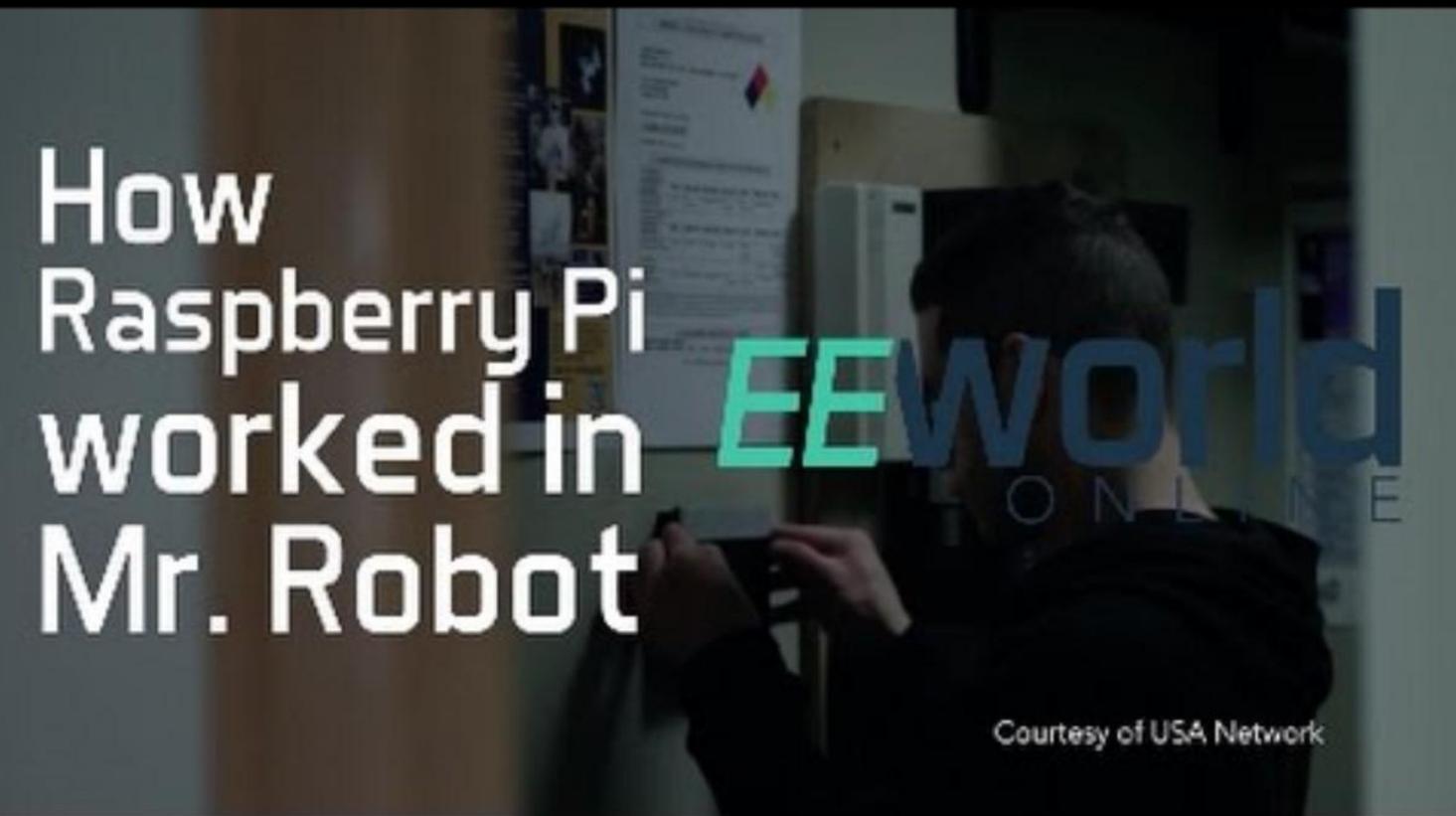
- La localisation physique des équipements,
- Le nombre de câbles utilisés,
- Le nombre de machines sur le réseau,
- Une vue plus détaillée des équipements d'interconnexion.

# Résumons la situation

- Les réseaux informatiques existent depuis longtemps sous différentes formes ;
- Les réseaux permettent l'échange de données entre différents équipements informatiques ;
- Il existe différents types de réseaux en fonction de leur taille ;
- Il est possible de représenter l'architecture à l'aide de plusieurs schémas ;
- Pour raccorder plus de 2 machines entre elles, vous devez intégrer un équipement réseau ;
- Pour faire communiquer plusieurs réseaux entre eux, il faut obligatoirement passer par un routeur ;
- Il est possible de créer une maquette virtuelle d'un réseau grâce à un outil de simulation.



# Possible Hack Mr ROBOT ? – EE World Online - 2017



How  
Raspberry Pi  
worked in  
Mr. Robot

Courtesy of USA Network

# 04

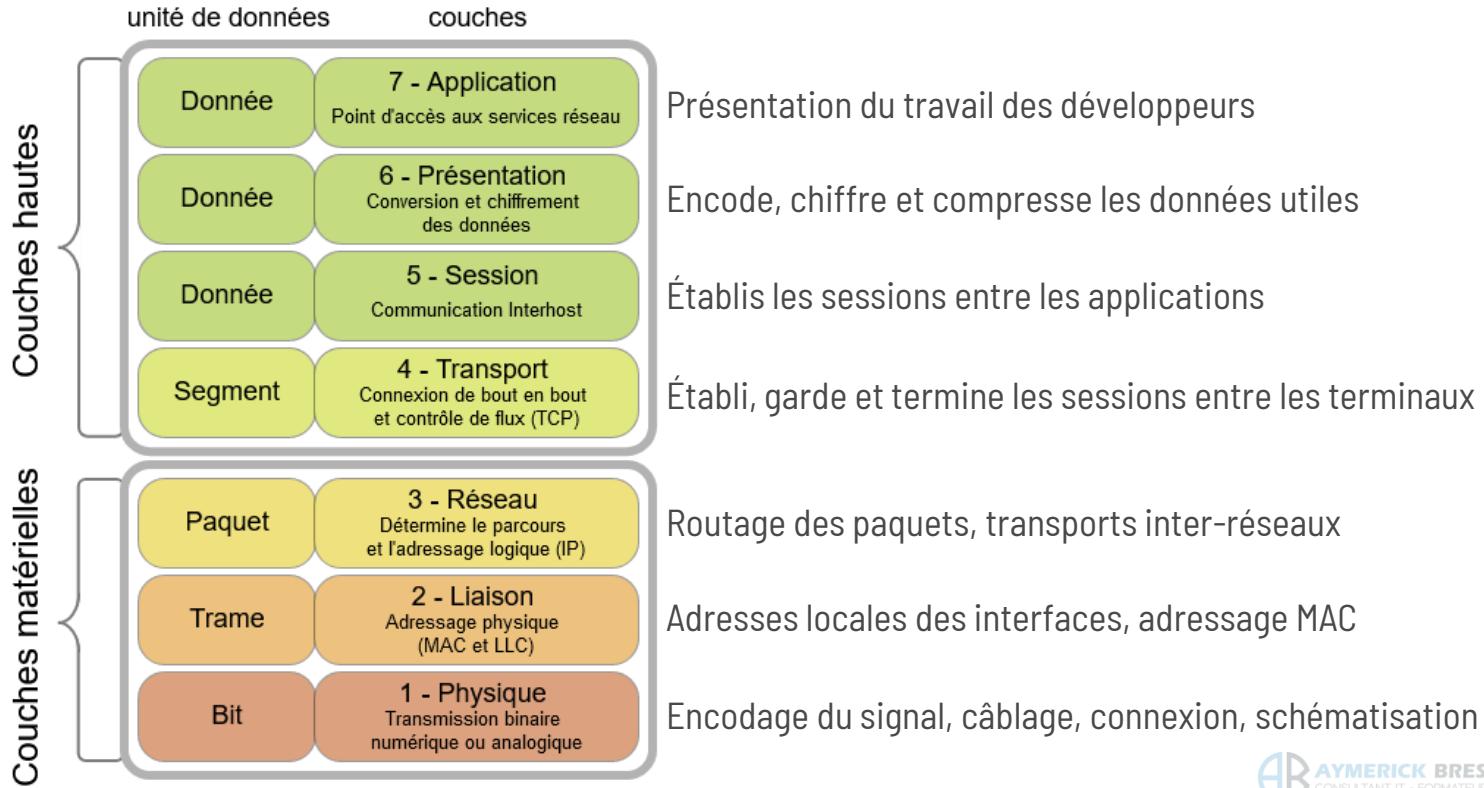
## Gestion des couches

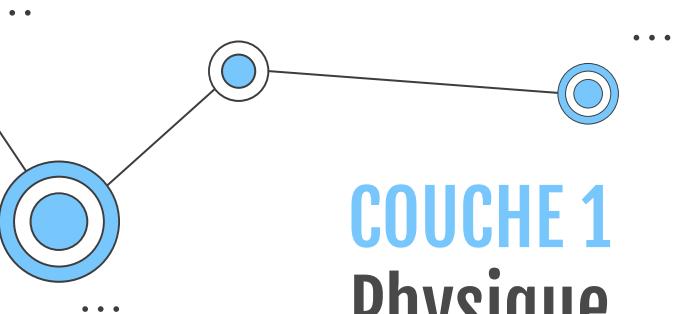
Couches par couches...



# Les 7 couches du modèle OSI

## Open Systems Interconnection





## COUCHE 1 Physique

Choix du support physique pour transmettre l'énergie électrique ou lumineuse sous forme de **bits**, soit, la présence ou l'absence d'énergie sur un espace temps : **0 ou 1.**



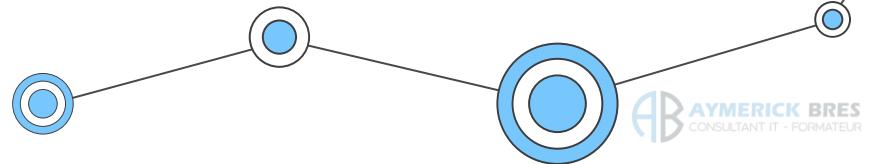
## COUCHE 2 Adressage MAC



Une adresse MAC ([Media Access Control](#)) est un identifiant unique [assigné à une interface réseau](#). Il y a autant d'adresses MAC que d'interfaces (cartes) réseau sur l'équipement. Elle est utilisée au niveau de la couche de liaison de données (2) du modèle OSI. Chaque périphérique réseau (comme une carte réseau, un routeur, ou un point d'accès Wi-Fi) possède une adresse MAC [unique](#) par interface.

Une adresse MAC est une [séquence de 48 bits](#) réparties sur [6 octets](#).  
Elle est représentée sous la forme de [12 chiffres hexadécimaux](#) :

**00:1A:2B:3C:4D:5E**





# Nombres hexadécimaux / binaires...

Décimal	Hexadécimal	Binaire	Décimal	Hexadécimal	Binaire
---------	-------------	---------	---------	-------------	---------

0	0	0000	8	8	1000
---	---	------	---	---	------

1	1	0001	9	9	1001
---	---	------	---	---	------

2	2	0010	10	A	1010
---	---	------	----	---	------

3	3	0011	11	B	1011
---	---	------	----	---	------

4	4	0100	12	C	1100
---	---	------	----	---	------

5	5	0101	13	D	1101
---	---	------	----	---	------

6	6	0110	14	E	1110
---	---	------	----	---	------

7	7	0111	15	F	1111
---	---	------	----	---	------

```
C:\Users\Aymeric BRES>ipconfig /all
```

#### Configuration IP de Windows

```
Nom de l'hôte . . . . . : Helios500
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: home
```

#### Carte inconnue Connexion au réseau local :

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : TAP-Windows Adapter V9 for OpenVPN Connect
Adresse physique . . . . . : 00-FF-07-41-38-3E
DHCP activé. . . . . : Non
Configuration automatique activée. . . . . : Oui
```

#### Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . . . : home
Description. . . . . : Killer E2500 Gigabit Ethernet Controller
Adresse physique . . . . . : D8-C4-97-9C-FD-C3
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
Adresse IPv4. . . . . : 192.168.1.50(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : mercredi 20 octobre 2021 18:30:19
Bail expirant. . . . . : jeudi 21 octobre 2021 19:34:15
Passerelle par défaut. . . . . : 192.168.1.254
Serveur DHCP . . . . . : 192.168.1.254
Serveurs DNS. . . . . : 192.168.1.254
NetBIOS sur Tcpip. . . . . : Activé
```

#### Carte réseau sans fil Connexion au réseau local\* 2 :

```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Adresse physique . . . . . : 0C-54-15-73-CB-99
DHCP activé. . . . . : Oui
Configuration automatique activée. . . . . : Oui
```

#### Carte réseau sans fil Connexion au réseau local\* 1 :

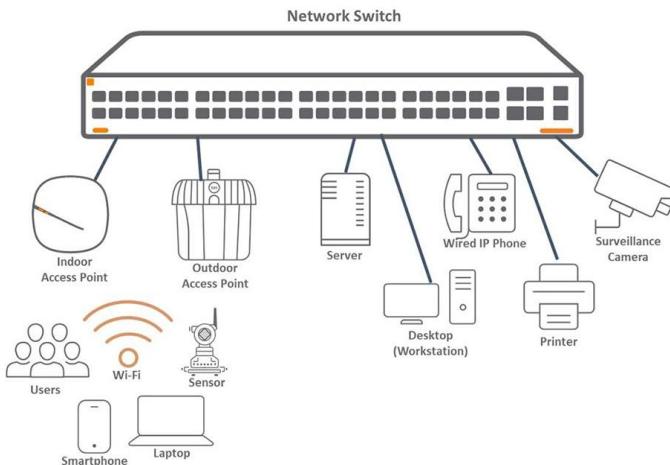
```
Statut du média. . . . . : Média déconnecté
Suffixe DNS propre à la connexion. . . . . :
Description. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Adresse physique . . . . . : 0E-54-15-73-CB-98
DHCP activé. . . . . : Non
Configuration automatique activée. . . . . : Oui
```

# COUCHE 2 : L'adresse Media Access Control (MAC)

## Les caractéristiques importantes de l'@ MAC

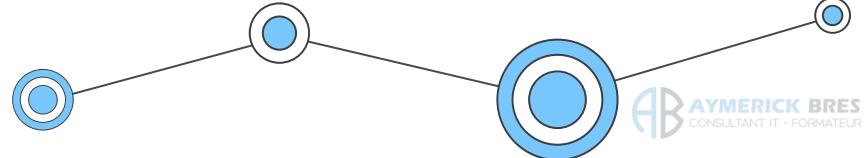
- Elle est construite sur **48 bits** ;
- Elle est composée de **6 octets hexadécimaux** ;
- Généralement, un double point « : » sépare les octets ;
- Non modifiable car associé à la carte réseau lors de la conception en usine ;
- Elle est unique dans le monde ;
- Il existe **281 000 milliards** de possibilités ;
- Les **3 premiers octets** représentent le constructeur ;
- Les **3 derniers octets** représentent la carte réseau ;
- Il est possible de vérifier sur [ce site](#) quel est le fabricant de la carte réseau ;
- Elle agit similairement à un numéro de série ;
- Permet de faire transiter les **TRAMES**.

# Le commutateur (Switch)



Un **switch**, ou **commutateur**, est un appareil réseau qui connecte plusieurs appareils au sein d'un réseau local (LAN). Contrairement à **un hub**, un switch envoie les données uniquement à l'appareil destinataire, améliorant ainsi les performances du réseau.

Le switch utilise une **table CAM (Content Addressable Memory)** pour fonctionner efficacement. Cette table **enregistre les adresses MAC des appareils connectés à chaque port physique**. Lorsqu'un appareil envoie des données, le switch consulte la table CAM pour déterminer à quel port envoyer les données. Si l'adresse n'est pas dans la table, le switch envoie les données à tous les ports jusqu'à ce qu'il identifie le destinataire, puis met à jour la table pour des transmissions futures plus rapides.



# TD !

Identifiez l'adresse MAC de vos postes du schéma logique précédent sur le logiciel **CISCO PACKET TRACER**.

Commande **show interfaces** pour les équipements réseau.

# COUCHE 3

## Adressage IP

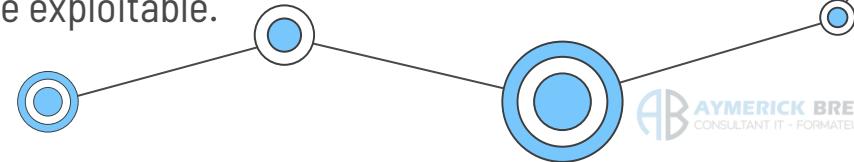
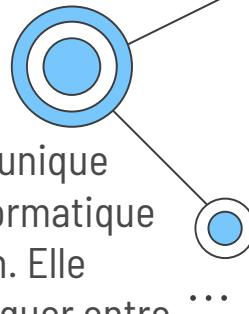


Une **adresse IP** (Internet Protocol) est un identifiant unique assigné à chaque **appareil connecté à un réseau** informatique utilisant le protocole Internet pour la communication. Elle permet aux dispositifs de s'identifier et de communiquer entre eux sur un réseau, qu'il soit local (LAN) ou global (Internet).

Il existe principalement deux versions d'adresses IP : **IPv4** et **IPv6**.

Une adresse **IPv4** est composée de **32 bits**, généralement représentée sous forme de **4 octets** (groupes de huit bits) en notation décimale pointée.

L'adresse IP doit toujours être **associée à un masque de sous-réseau** pour être exploitable.





## COUCHE 2-3

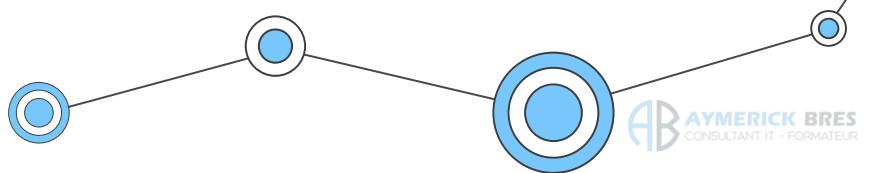
# Résolution ARP



Le protocole **ARP** (Address Resolution Protocol) est un protocole réseau qui sert à faire le lien entre une **adresse IP (logique)** et une adresse **MAC (physique)**.

Concrètement, lorsqu'un ordinateur veut communiquer sur un réseau local avec une machine dont il connaît l'IP, il doit d'abord découvrir quelle est l'adresse MAC associée. Il envoie alors une requête ARP : « Qui a cette adresse IP ? » en diffusion (broadcast).

La machine concernée répond avec sa MAC, et cette correspondance est enregistrée dans **une table ARP** pour éviter de redemander à chaque fois.



# Cybersécurité – Attaques connues

**ARP Spoofing** : Falsification de la table ARP. L'attaquant envoie de fausses réponses ARP pour lier leur propre adresse MAC à l'adresse IP d'un autre périphérique, ce qui leur permet de rediriger le trafic réseau.

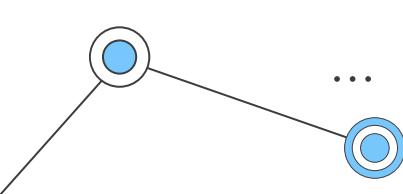
Attaque couramment utilisée dans le cadre « Man-in-the-middle ».

**VLAN Hopping** : Attaque consistant à tromper un commutateur pour qu'il achemine du trafic sur un VLAN auquel un périphérique n'est normalement pas autorisé à accéder.

**Attaque Spanning Tree Protocol** : Le STP est utilisé pour éviter les boucles dans les réseaux Ethernet. Cependant, l'attaquant peut exploiter des vulnérabilités du STP pour perturber la topologie du réseau ou causer des pannes.

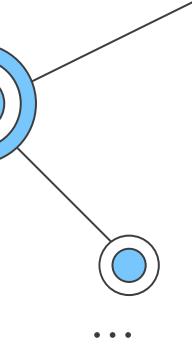
**MAC Flooding** : Inondation du cache CAM d'un commutateur en envoyant un grand nombre de trames avec différentes adresses MAC entraînant une surcharge de cache, provoquant un ralentissement, une interruption du service ou un envoi par broadcast.

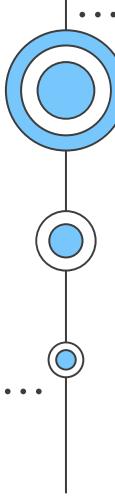




# **COUCHE 3 : Fonctionnement d'une adresse IPv4**

(Prise de note)





# COUCHE 3 : Masque adressage IP

Composition d'un octet, soit 8 bits binaires

1	2	3	4	5	6	7	8
$2^7$	$2^6$	$2^5$	$2^4$	$2^3$	$2^2$	$2^1$	$2^0$
128	64	32	16	8	4	2	1
128	192	224	240	248	252	254	255

Notation **Classless Interdomain Routing** (CIDR) : permet d'écrire un slash accompagné du nombre de bits à 1 dans le masque. Par exemple, le masque **255.255.255.0** aura comme notation **CIDR /24**. En effet, dans le masque pris en exemple, **24 bits sont à la position 1**.

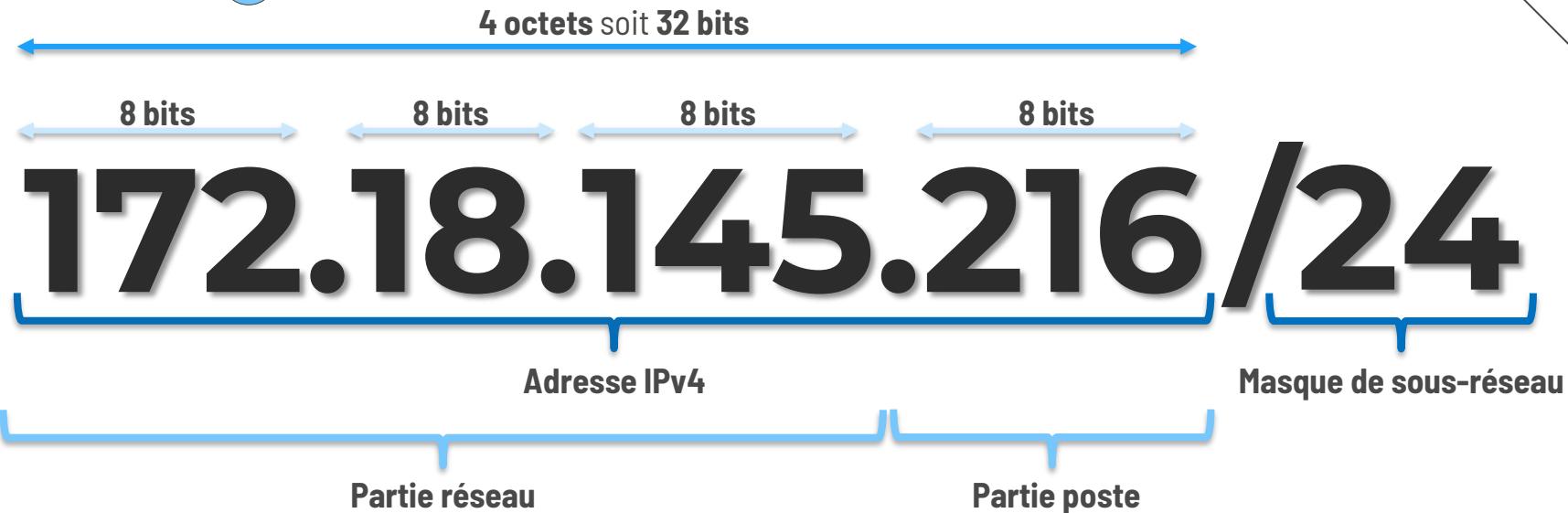


## COUCHE 3 : Classes d'adressage IP

Classe	Début	Fin	Masque par défaut	Plage privée
A	0.0.0.1	126.255.255.255	/8	10.0.0.0
B	128.0.0.0	191.255.255.255	/16	172.16.0.0 à 172.31.255.255
C	192.0.0.0	223.255.255.255	/24	192.168.1.0
D	224.0.0.0	239.255.255.255	-	-
E	240.0.0.0	255.255.255.254	-	-

Le réseau [127.0.0.0](#) et les classes D et E représentent respectivement des réseaux de tests, de multicast et de tests IETF. [Ils ne sont pas utilisables](#) en privé comme en public.

# COUCHE 3 : Récap. adressage IP

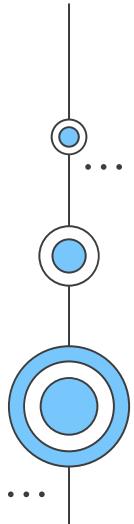
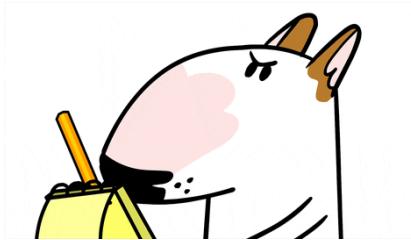
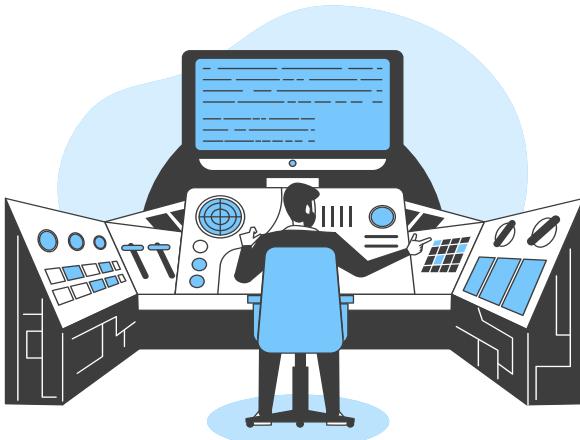


- ✓ Adresse de réseau : **172.18.145.0**
- ✓ Adresse de diffusion : **172.18.145.255**
- ✓ Première adresse hôte : **172.18.145.1**
- ✓ Dernière adresse hôte : **172.18.145.254** (par convention passerelle)
- ✓ Nombre d'hôtes possibles  $2^n - 2 \Leftrightarrow 2^8 - 2 = 254$  hôtes possibles (n = nombre de bits hôtes disponibles)

# Résumons la situation

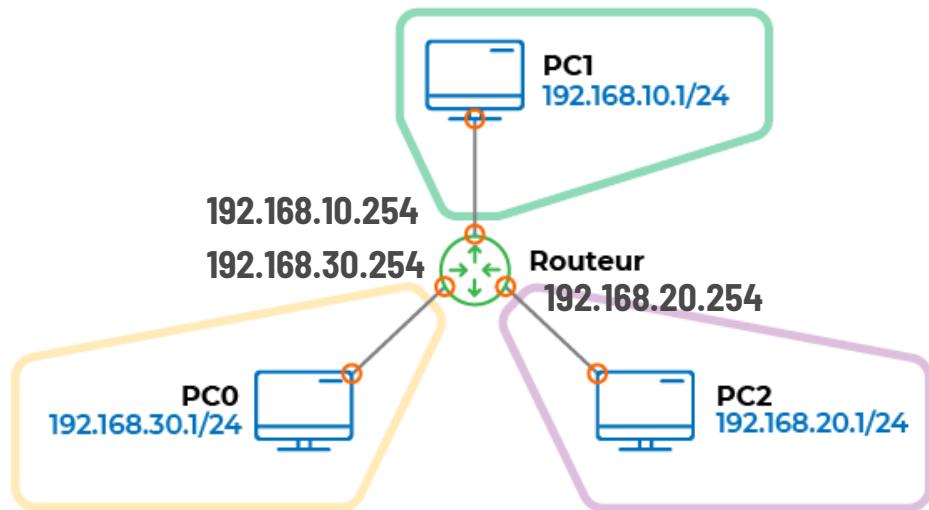


- L'adresse IP est nécessaire pour acheminer des messages entre des réseaux différents ;
- Une adresse IPv4 est écrite sur **32 bits**, soit **4 octets**,
- Une adresse IP est « découpée » en 2 parties grâce au masque de sous-réseau,
- L'IPv6 va peu à peu prendre la place de l'IPv4 dû au manque d'adresses disponibles,  
*Exemple d'adresse IPv6 :*  
**2001:0db8:0000:85a3:0000:0000:ac1f:8001**
- Un plan d'adressage cohérent doit être élaboré lors de la création du réseau,
- Les masques de sous réseaux **/8** ; **/16** ; **/24** ; **/30** sont les plus utilisés.

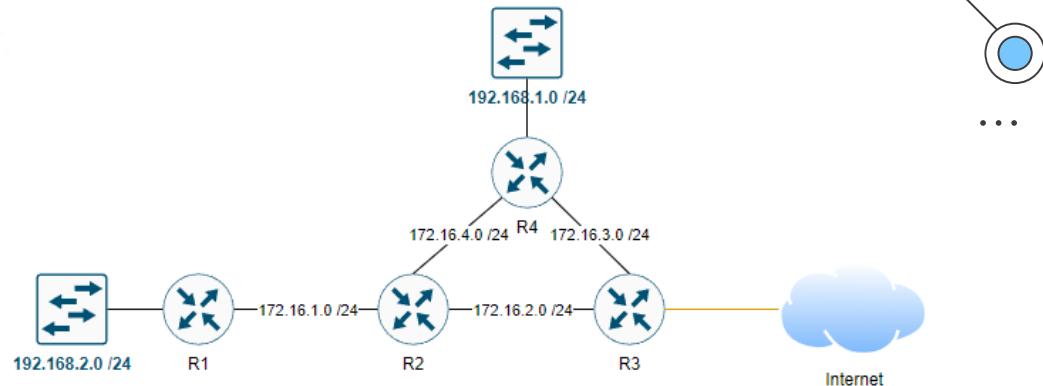
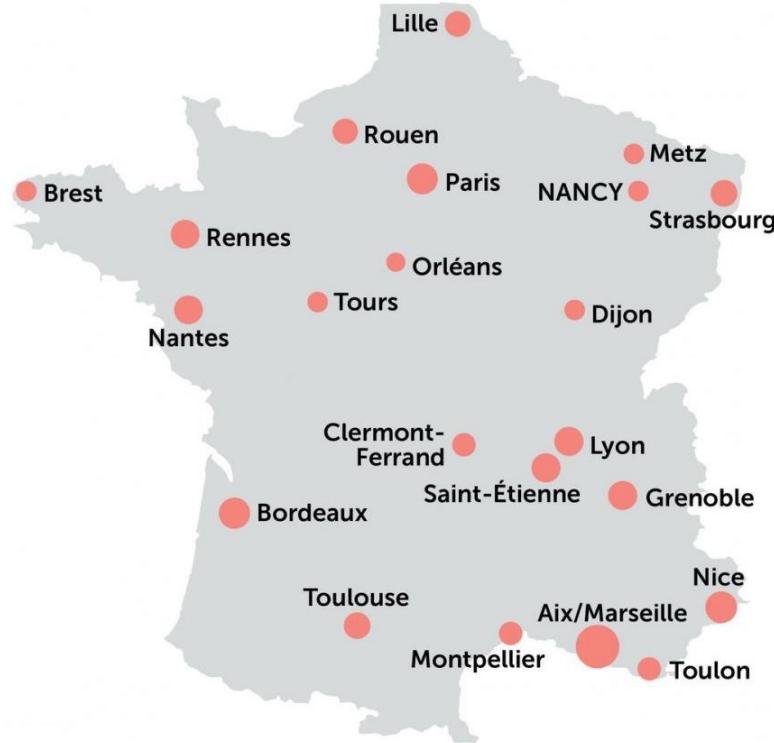


# COUCHE 3 : Le routage IP

Un **routeur** est un équipement particulier. En effet, contrairement à tous les autres équipements, il est le seul à avoir autant d'adresses IP que de réseaux connectés. Le rôle du routeur est de faire passer les paquets de réseau en réseau à la manière d'un poste de douane présent aux frontières d'un pays. Par convention, l'adresse IP d'un routeur dans un réseau est toujours la dernière adresse IP adressable.



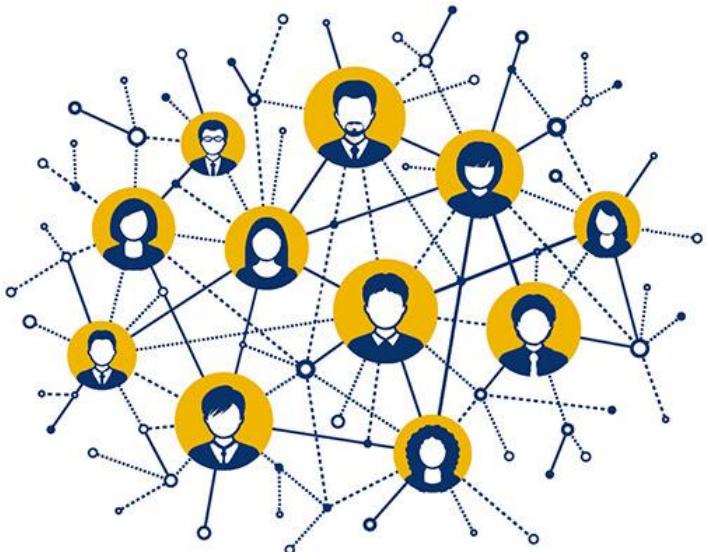
# COUCHE 3 : Le routage IP



Connection de 192.168.1.0 à 192.168.2.0

Routeur	Net. Dest.	Mask Dest.	Next-OP
R4	192.168.2.0	255.255.255.0	172.16.4.2
R2	192.168.2.0	255.255.255.0	172.16.1.1
R1	192.168.2.0	255.255.255.0	DC

# Le routeur



Un routeur est un appareil réseau essentiel qui permet de connecter plusieurs réseaux entre eux, comme un réseau local (LAN) à Internet. Il dirige les paquets de données entre ces réseaux, en choisissant le chemin le plus efficace pour chaque paquet.

Le routeur utilise une table de routage pour fonctionner. Cette table contient des informations sur les différentes routes disponibles pour atteindre diverses destinations. Les routes possèdent des poids pour définir leur priorité. Lorsqu'un paquet de données arrive, le routeur examine l'adresse IP de destination et consulte sa table de routage pour déterminer la meilleure route à suivre. Si le chemin optimal est trouvé, le routeur transmet le paquet à son prochain point de passage, qu'il s'agisse d'un autre routeur ou du dispositif de destination final.

# Cybersécurité – Attaques connues

**Déni de service (DoS) :** Inondation d'un réseau ou d'un serveur en envoyant un grand nombre de demandes de trafic légitime, ce qui entraîne une congestion ou une indisponibilité du service.

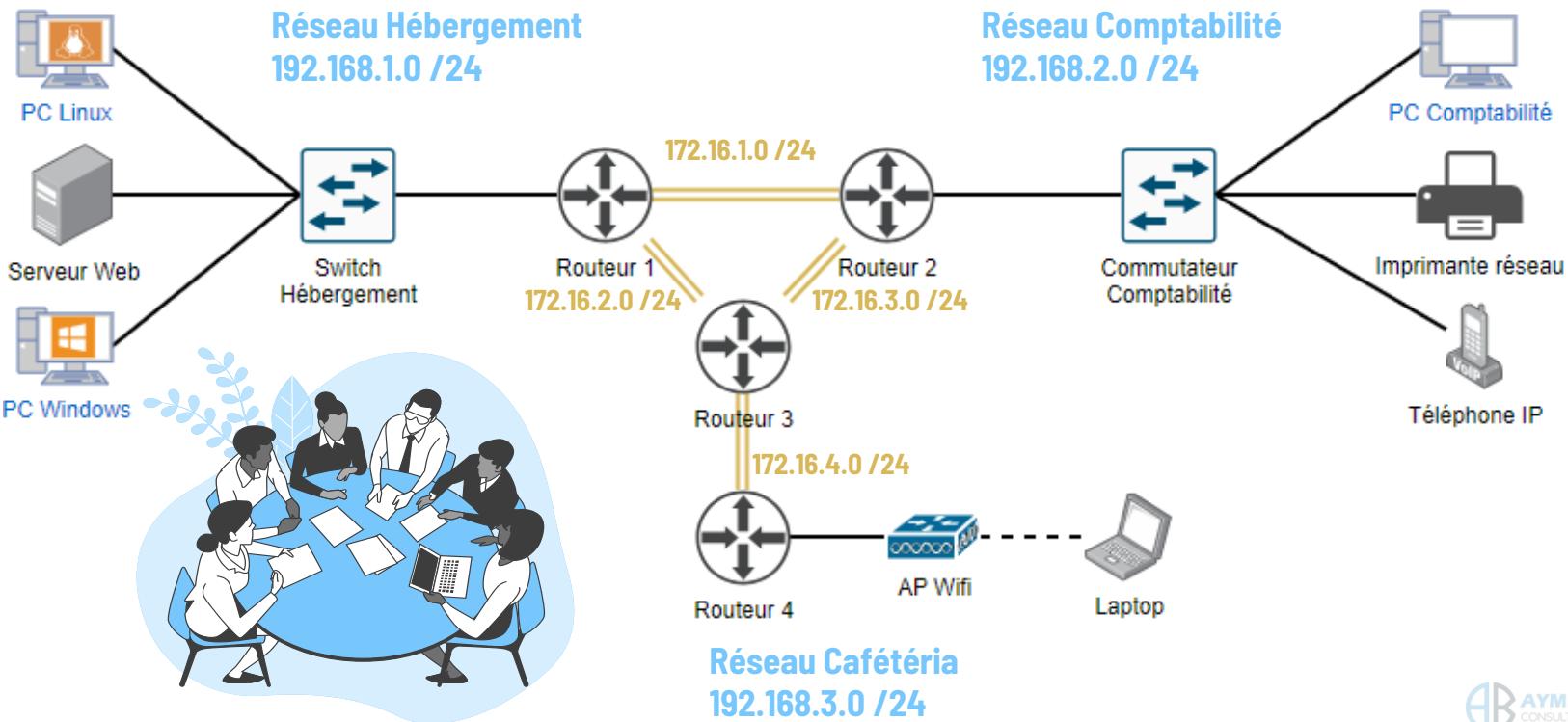
**Route Hijacking :** L'attaquant tente de détourner le trafic réseau en annonçant de fausses informations de routage sur Internet. Cela peut rediriger le trafic vers des serveurs compromis contrôlés par l'attaquant.



# TD !

Sur le logiciel **CISCO PACKET TRACER**. Reprenez le schéma logique suivant, et mettez en place le plan d'adressage IP.

# La schématisation logique d'un réseau



# TD !

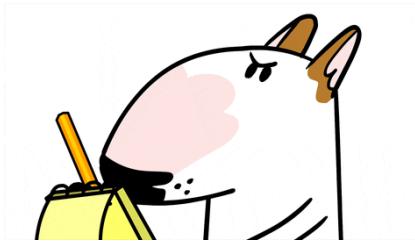
Sur le logiciel **CISCO PACKET TRACER**. Reprenez le schéma logique précédent, et mettez en place le routage pour que tous les hôtes se pinguent.

# TD !

Identifiez la [résolution ARP](#) s'effectuer lors d'un ping sur le logiciel [CISCO PACKET TRACER](#).

# Résumons la situation

- Lorsqu'un paquet est envoyé d'un réseau IP vers un autre, il passe obligatoirement **par un routeur**. Ce dernier est appelé « **la passerelle par défaut** » ou « **Gateway** » en anglais ;
- Chaque interface réseau du routeur doit être **activée** et avoir **une adresse IP** de configurée ;
- Il y a autant d'adresses IP que de réseaux connectés au routeur ;
- La **table de routage** enregistrée dans un routeur permet à celui-ci de router les paquets vers les destinations mentionnées ;
- La résolution **ARP** fait le lien entre **l'adressage MAC** et **l'adressage IP** (entre la couche 2 et la couche 3 du modèle OSI).



# COUCHE 4 : Transport TCP / UDP

TCP ( Connection oriented )



UDP ( Connectionless )



## Typical Applications

- File Transfer Protocol ( FTP )
- Web Browsing
- Email



unicast

## Typical Applications

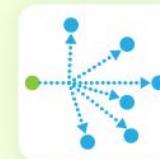
- Live Streaming
- VoIP



unicast



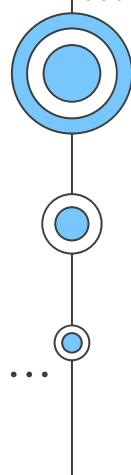
multicast



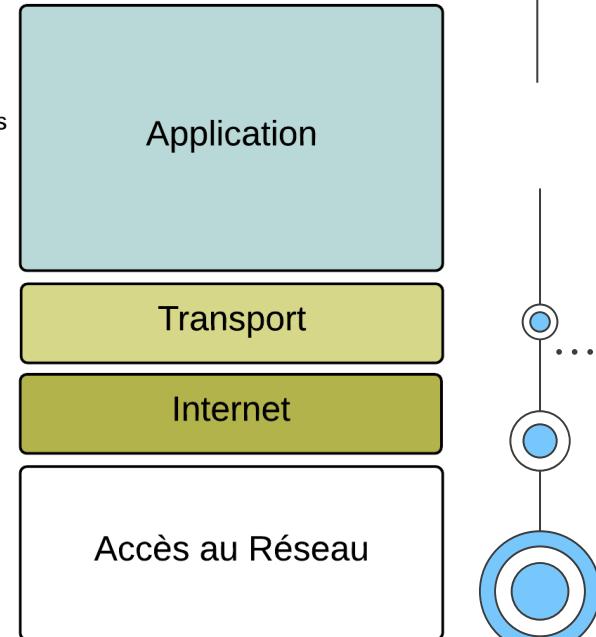
broadcast

# Les 7 couches du modèle OSI

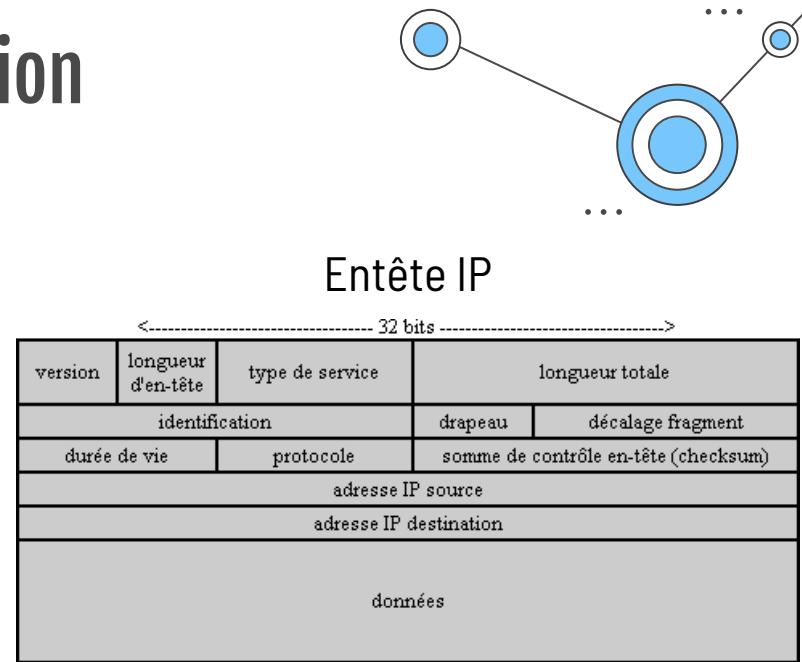
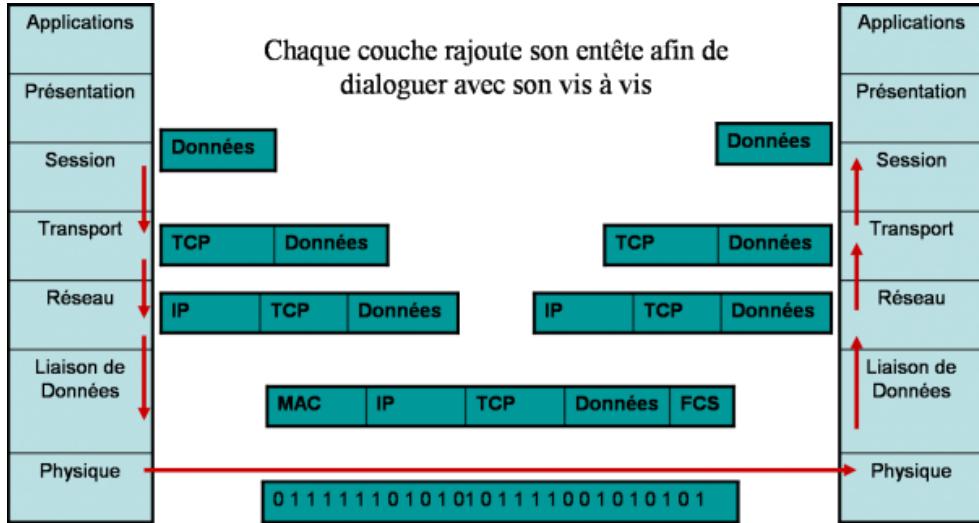
## Open Systems Interconnection

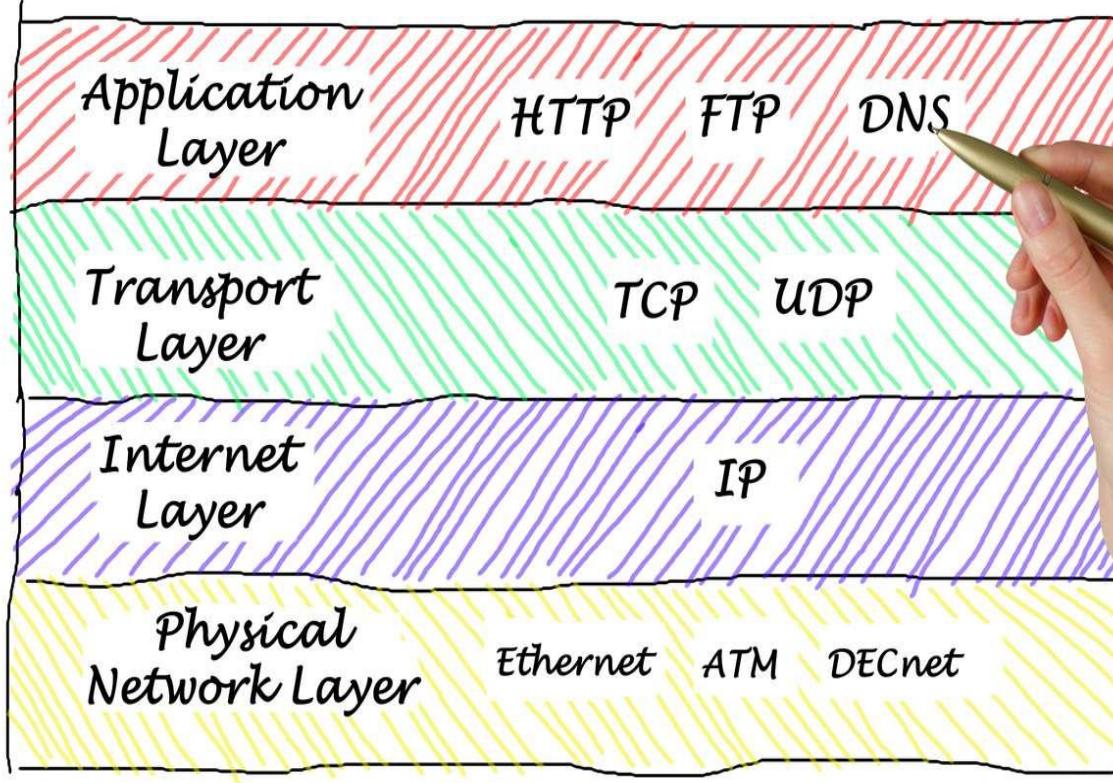


Modèle OSI	Périphérique / Description
7 Application	 Services applicatifs au plus proche des utilisateurs
6 Présentation	 Encode, chiffre, compresse les données utiles
5 Session	 Etablit des sessions entre des applications
4 Transport	 Etablit, maintien et termine des sessions entre des périphériques terminaux
3 Réseau	 Adresse les interfaces globalement et détermine les meilleurs chemins à travers un inter-réseau
2 Liaison de Données	 Adresse localement les interfaces, livre les informations localement, méthode MAC
1 Physique	 Encodage du signal, câblage et connecteurs, spécifications physiques



# Encapsulation





# Résumons la situation

- Le modèle OSI permet de classer, sur plusieurs niveaux, les règles, les protocoles et rend possible la communication sur les réseaux ;
- Ce modèle est composé de 7 couches ;
- Chaque protocole et chaque élément réseau sont associés à une couche précise ;
- Le modèle TCP/IP est un modèle similaire en 4 couches, plus proche de la réalité ;
- Lorsqu'un message est envoyé, il est découpé en plusieurs morceaux s'il est trop grand ;
- Lorsqu'un message est envoyé, chaque couche rajoute son information, on appelle cela l'**encapsulation**.



# Merci !

Avez-vous des dernières questions ?

Chapitre à relire pour le contrôle de connaissances.

[Lire ce cours sous une autre approche.](#)

# Kahoot!

**CREDITS:** This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

Please keep this slide for attribution