

Chapitre (TCP/IP)



1. Objectifs



À la fin de ce chapitre, on sera capable de :

1. Expliquer le rôle du protocole ARP dans la communication réseau.
2. Effectuer des calculs de sous-réseaux (subnetting) statiques et dynamiques.
3. Identifier le nombre d'hôtes, l'adresse réseau et broadcast pour un sous-réseau donné.
4. Manipuler ces notions sur des exemples concrets (Packet Tracer, simulation).

2. Modèle OSI

Du Modèle OSI



Le modèle *OSI* (Open Systems Interconnection): a été créé pour standardiser les communications réseau entre ordinateurs. Il divise la communication en **7 couches**, chacune ayant un rôle spécifique.

- **But** : permettre à tous les équipements et logiciels de parler le même langage.
- **Idée** : chaque couche s'occupe d'une tâche et passe les données à la suivante

N°	Couche OSI	Rôle principal	Exemples / Protocoles / Unité
7	Application	Interface entre l'utilisateur et le réseau. Permet aux applications d'accéder aux services réseau.	HTTP, SMTP, FTP, DNS Unité : Données
6	Présentation	Assure la traduction, la compression et le chiffrement des données pour la couche application.	JPEG, MPEG, SSL/TLS Unité : Données
5	Session	Gère les sessions de communication entre deux machines (ouverture, maintien, fermeture).	RPC, NetBIOS, PPTP Unité : Données
4	Transport	Garantit la transmission fiable des données entre deux hôtes (segmentation, contrôle d'erreur).	TCP, UDP Unité : Segments
3	Réseau	Gère l'adressage logique et le routage des paquets à travers le réseau.	Routeurs, IP, ICMP Unité : Paquets
2	Liaison de données	Transmet les trames entre deux machines reliées physiquement. Gère les adresses MAC et la détection d'erreurs.	Switchs, Ponts, Ethernet, PPP Unité : Trames
1	Physique	Transmet les bits bruts sur le support physique (câble, fibre, ondes). Spécifie les caractéristiques électriques et mécaniques.	Répéteurs, Hubs, Câbles RJ45 Unité : Bits

Couche OSI

Sur Modèle OSI

Fonctionnement global:

- **À l'envoi (encapsulation)**: Les données descendent de la couche 7 vers la 1; Chaque couche ajoute son propre en-tête (informations de contrôle).
- **À la réception (décapsulation)**: Les couches du destinataire retirent les en-têtes une à une jusqu'à retrouver le message original.



Imaginons que vous ouvrez votre navigateur et que vous tapez : **www.example.com**.

Voyons comment **les couches du modèle OSI** interviennent étape par étape:

- Couche Application (HTTP): C'est ici que tout commence. Le navigateur envoie une demande de page web au serveur via le protocole HTTP. C'est la couche qui permet la communication entre l'utilisateur et le réseau.
- Couche Présentation: Assure la traduction, la compression et le chiffrement des données pour la couche application.
- Couche Session: Assure la traduction, la compression et le chiffrement des données pour la couche application.
- Couche Transport (TCP): Cette couche s'occupe de la fiabilité de la transmission. Elle découpe la requête en plusieurs segments et ajoute des numéros pour que le serveur puisse les remettre dans le bon ordre. Si un segment est perdu, TCP le renvoie automatiquement.
- Couche Réseau (IP): Chaque segment est ensuite placé dans un paquet IP. Cette couche ajoute les adresses IP source et destination, puis cherche le meilleur chemin pour atteindre le serveur sur Internet.
- Couche Liaison de données (Ethernet ou Wi-Fi): Les paquets IP sont ensuite encapsulés dans des trames. Cette couche gère la communication au niveau local, c'est-à-dire à l'intérieur du réseau de votre université ou de votre maison.
- Couche Physique: Enfin, les trames deviennent des signaux électriques, optiques ou radio, qui voyagent dans les câbles ou par ondes Wi-Fi. Ce sont les bits (0 et 1) qui circulent physiquement sur le support. Et maintenant, de l'autre côté, le serveur reçoit ces bits et effectue le chemin inverse (ce qu'on appelle la décapsulation) : il reconstitue les trames, les paquets IP, les segments TCP, et enfin la requête HTTP.
- Le serveur traite cette requête et renvoie la page web au navigateur, qui l'affiche à l'écran.¹

3. Le modèle TCP / IP

Modèle OSI vs modèle TCP/IP

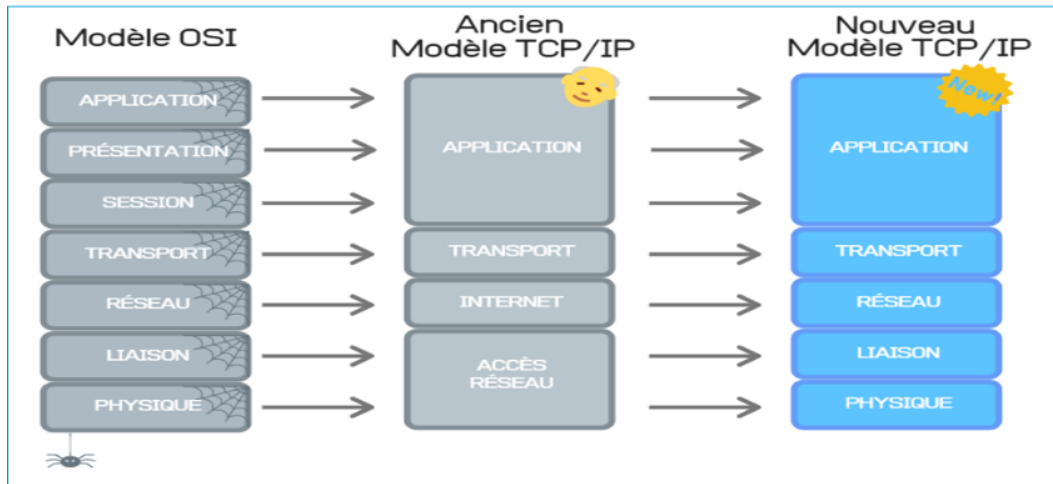


Le modèle OSI :

1. Obsolète
2. Possède
3. 7 couches hiérarchisées

Le modèle TCP/IP(Transmission Control Protocol / Internet Protocol) :

1. En cours d'utilisation
2. Le modèle TCP/IP existe sous deux versions : L'ancienne et la nouvelle.
3. Possède 5 couches hiérarchisées
4. Le modèle TCP / IP spécifie les protocoles utilisés.
5. Ce modèle est devenu le standard pour la communication sur Internet.¹



Modèle OSI vs Modèle TCP/IP

Le modèle TCP / IP



Le modèle TCP / IP est très similaire au modèle OSI:

Couche Application (Fusion de couches Application, Session et Présentation du modèle OSI)

Couche Transport

Couche Internet (Ancienne couche Réseaux du modèle OSI)

Couche d'Accès Réseaux (Fusion de deux couches Physique et Liaison de Données du modèle OSI)

Application	7	Application
	6	Presentation
	5	Session
Transport	4	Transport
Internetwork	3	Network
Link/Network	2	Data Link
Physical	1	Physical

Principe de fonctionnement



Le modèle OSI et le modèle TCP/IP ont le même principe de fonctionnement.

BOB veut envoyer un message à **ALICE**.

- Étape 1 : **BOB** fragmente la donnée.
- Étape 2 : Chaque fragment de donnée va passer par chaque couche du modèle TCP/IP.

- 1) La couche APPLICATION ajoute des informations à la donnée.
- 2) La couche TRANSPORT ajoute des informations à la donnée afin de créer un SEGMENT.
- 3) La couche RÉSEAU ajoute des informations à la donnée afin de créer un PAQUET.
- 4) La couche LIAISON ajoute des informations à la donnée afin de créer une TRAME.
- 5) La couche PHYSIQUE adapte l'information au support de transmission.



fragmentation des données(TCP/IP)

clés pour comprendre le réseau



Le modèle **TCP/IP** désigne une suite de protocoles de communication qui forment la base d'Internet et de la majorité des réseaux informatiques modernes.

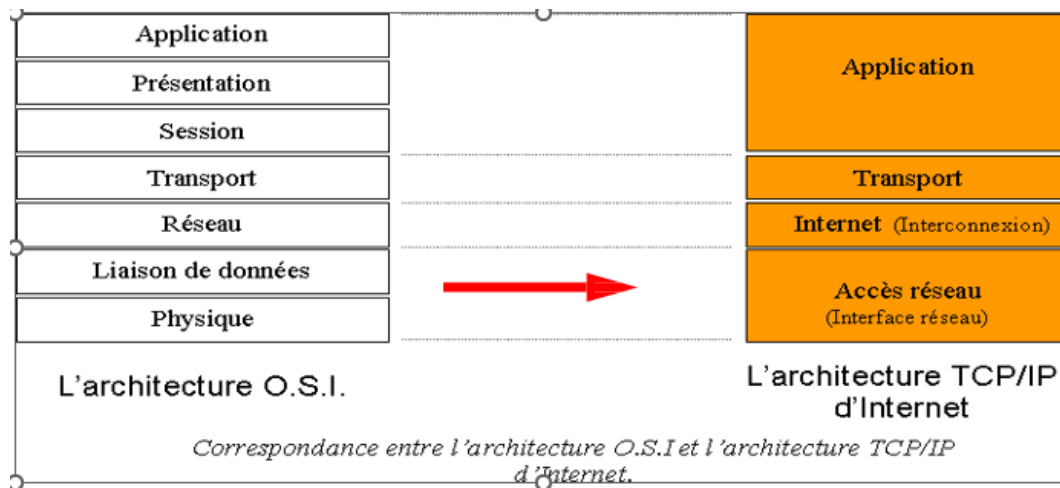
Bien qu'il soit souvent comparé au modèle **OSI**, **TCP/IP** n'est pas un modèle théorique.

C'est une architecture de protocoles pensée pour la mise en œuvre pratique.

TCP/IP permet d'assurer l'interopérabilité entre différents types de réseaux et d'appareils, garantissant que des milliards de dispositifs peuvent communiquer efficacement et de manière standardisée. C'est ainsi le fondement des communications en réseau, que ce soit pour les réseaux locaux d'entreprises ou pour Internet lui-même

Le modèle TCP / IP Couche TCP/IP	Équivalent OSI	Exemples de Protocoles
Couche 4 : Application	Couche Application	Web (HTTP/HTTPS), email (SMTP, IMAP, POP3), transfert de fichiers (FTP), etc
Couche 3 : Transport	Couche Transport	TCP, UDP
Couche 2 : Internet	Couche Réseau	IP (IPv4, IPv6)
Couche 1 : Accès Réseau	Couche Liaison de données + Couche Physique	Ethernet, Wi-Fi, ARP

Le modèle vs



4. Couche- Accès Réseau



Définition

La couche physique va adapter le message en fonction du support. C'est elle qui est responsable de l'envoi de **nos 0 et 1**.

Quelques protocoles de la couche physique :

- ADSL
- bluetooth
- câble coaxial
- CSMA/CA
- CSMA/CD
- paire torsadée
- USB
- wireless

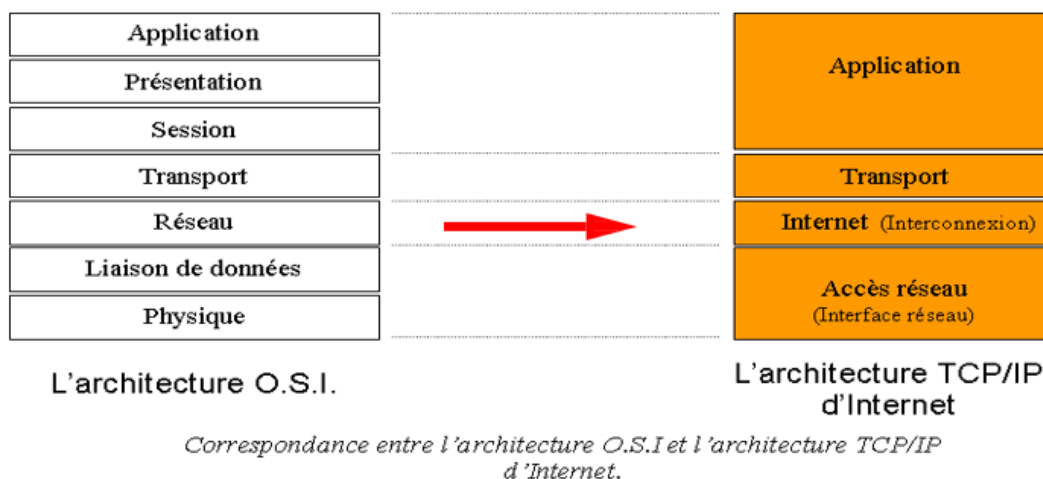
5. Couche-Internet

5.1. Couche-Internet

Couche-Internet



Définition



Correspond à la **couche 3** réseau du modèle **OSI \ nv.TCP/IP**

Principale couche de cette architecture

- Réalisé l'interconnexion des réseaux distants en mode non connecté.
- Se base sur le protocole IP: a pour but d'acheminer les paquets indépendamment les uns des autres jusqu'à leur destination, routage individuel des paquets.

Le protocole IP ne prend pas en charge ni la détection de paquets perdus ni la possibilité de reprise sur erreur.

Qui utilise les données de la couche 3 ?

- Les routeurs.

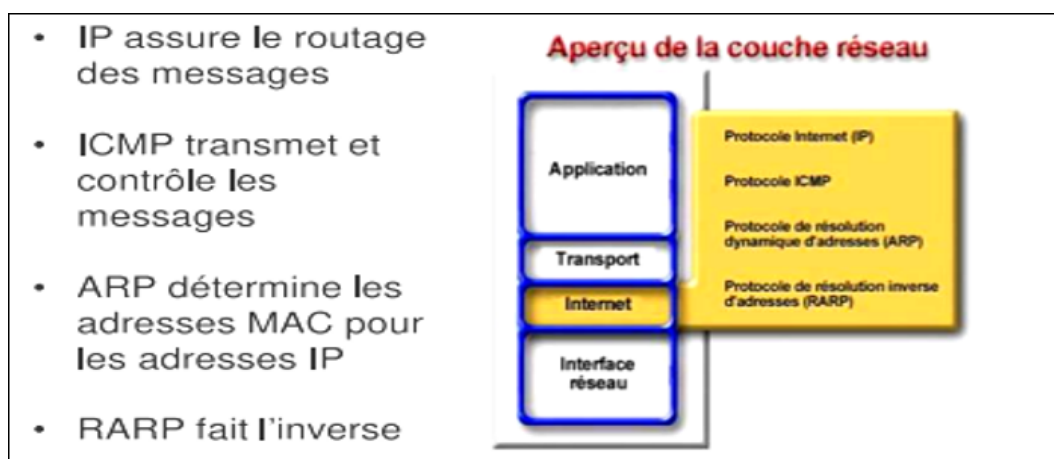
Que trouve-t-on comme informations dans la couche 3 ?

- Les adresses **IP** de notre émetteur et de notre destinataire.

La couche réseau permet de livrer un paquet au travers d'un réseau.

- **Unité:** Paquet.

Protocoles



Protocoles IP

La Communication hors du réseau local : Lorsqu'un hôte souhaite contacter une machine extérieure à son LAN (Local Area Network), il a besoin de connaître son **adresse IP**. C'est le protocole IP (Internet Protocol), propre à la couche Internet, qui permet de définir et d'utiliser cette adresse.

La communication dans le réseau local : À l'intérieur d'un LAN, les échanges ne se font pas directement avec les adresses IP, mais avec les adresses physiques (MAC) propres à chaque carte réseau. **Pour établir la correspondance entre l'adresse IP et l'adresse MAC, le protocole ARP (Address Resolution Protocol)** est utilisé au niveau de la couche Liaison.

Le protocole IP: le langage universel d'Internet. Le **protocole IP** est la base des communications sur Internet. Chaque machine connectée possède une adresse IP unique, qui permet de l'identifier dans le réseau mondial.

5.2. L'entête IP

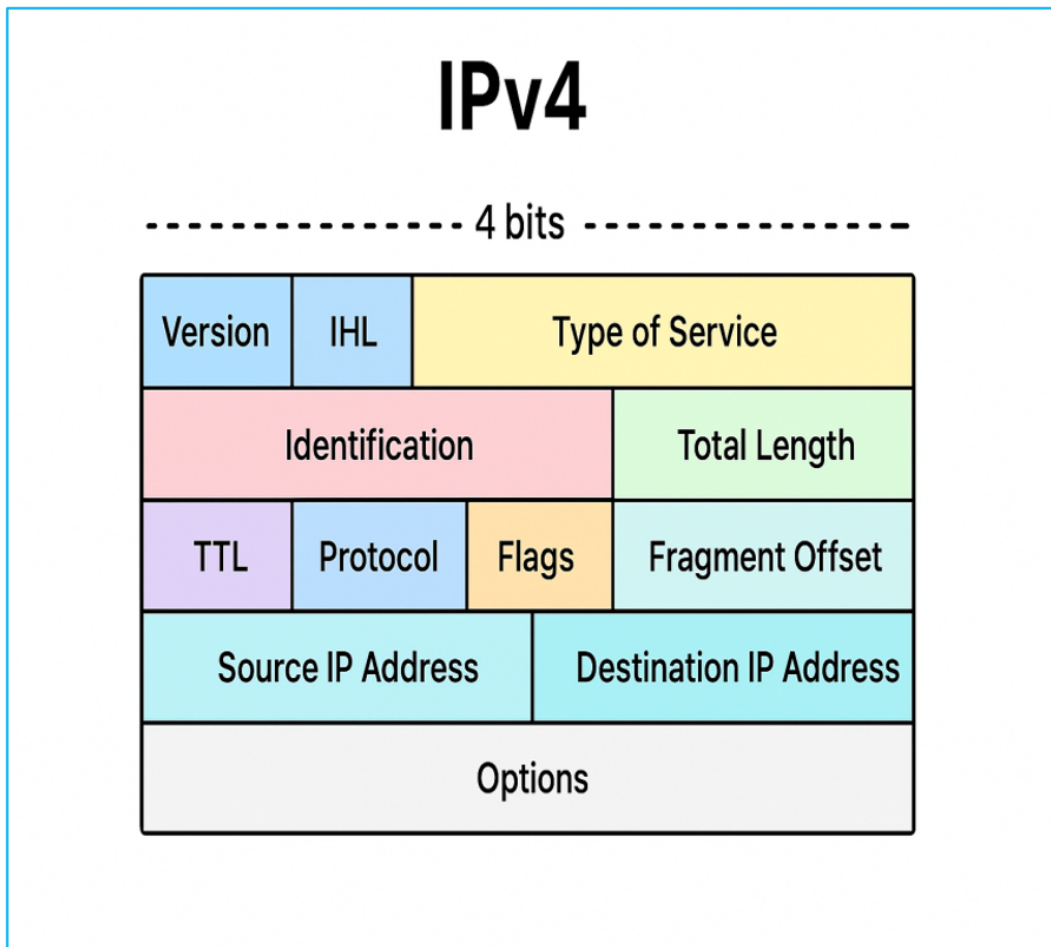


L'entête IP est une partie essentielle des paquets réseau. Il contient toutes les informations nécessaires pour l'acheminement. Deux versions principales : IPv4 et IPv6.¹

¹. RFC 791 – Internet Protocol (IPv4)

Champs principaux:

- Version : Indique IPv4 ou IPv6.
- IHL : Taille de l'entête.
- Type of Service (ToS) : Priorité / QoS.
- Taille totale : Taille du paquet en octets.
- Identification, Flags, Offset : Fragmentation.
- TTL : Durée de vie du paquet.
- Protocole : TCP=6, UDP=17, etc.
- Checksum : Contrôle d'erreur.
- Adresse IP Source et Destination.

*Entête IPv4***Fragmentation et Flags (IPv4)****Fondamental**

Identification: regroupe les fragments d'un paquet.

Flags :

- 0 = Réserve.
- 1 = Ne pas fragmenter.
- 2 = Plus de fragments.

Offset : position du fragment dans le paquet.

La fragmentation dans IPv4 consiste à découper un paquet IP trop grand en plusieurs fragments plus petits, afin qu'ils puissent traverser un réseau dont La taille maximale des paquets (MTU) est plus petite.

MTU (Maximum Transmission Unit) = taille maximale (en octets) d'un paquet que peut transporter un lien réseau sans être fragmenté.

Ethernet → MTU = 1500 octets

Chaque fragment devient un nouveau paquet IP indépendant, avec son propre en-tête.

La réassemblage se fait uniquement au niveau du destinataire final, jamais par les routeurs intermédiaires.

Les champs de l'en-tête IPv4 utilisés:

Champ Rôle Identification (16 bits): Même valeur pour tous les fragments d'un même paquet. Sert à les regrouper.

Flags (3 bits):

- Bit 0 : réservé (0) ;
- Bit 1 : DF (Don't Fragment) ;
- Bit 2 : MF (More Fragments)
- Fragment Offset (13 bits): Indique la position du fragment dans le paquet d'origine (en multiples de 8 octets).

? Exemple

Supposons :

Paquet initial = 4000 octets

En-tête IP = 20 octets

MTU=1500octets

Données utiles par paquet = 1500 – 20 = 1480 octets.

::Entête IPv4::

? Exemple

```
4 5 00 0050 2061 0000 80 01 C564 C7F5B40A C7F5B409 08 00 00 1C 01 02 03 04 05
06 07 0809 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 1819 1A 1B 1C 1D 1E 1F 20 21
22 23 24 25 26 27 28292A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38
```

4 = protocole IP version 4 ;

5 = longueur de l'en-tête du paquet = $5 \times 4 = 20$ octets = longueur par défaut d'un en-tête sans option.

00 Type of Service = 0 pas de service particulier (en fait, avec IPv4, il n'y a pas de service particulier. Ce champ est donc toujours nul, et s'il n'était pas nul, il serait ignoré !).

00 50 Longueur totale = $0 \times 4096 + 0 \times 256 + 5 \times 16 + 0 \times 1 = 80$ octets, donc la longueur du contenu du champ de données est de 80

20 = 60 octets.(80-20=60octet) la taille sans en tête de données.

20 61 Identifiant du paquet (ne sera utile que s'il est fragmenté).

00 00 Drapeaux et déplacement = tout à zéro = paquet non fragmenté, a priori normal puisqu'il n'y a que 60 octets de données.

80 Durée de vie = $80 = 8 \times 16 + 0 \times 1 = 128$ routeurs que le paquet pourrait encore traverser.

01 Protocole transporté dans le paquet: 1 = code du protocole ICMP.

C5 64 Bloc de contrôle d'erreur de l'en-tête.

C7 F5 B4 0A Adresse IP émetteur = 199.245.180.10.

C7 F5 B4 09 Adresse IP destinataire = 199.245.180.9. Les deux machines sont dans le même réseau de classe C, le réseau 199.245.180.0.

5.3. Adresse IP



Une adresse IP :⁶est une adresse numérique. Ça permet d'identifier un ordinateur ou bien n'importe quel équipement du réseau. Dans le monde de l'informatique, on utilise souvent le terme IP pour désigner l'adresse IP. Chaque appareil doit avoir une IP unique, pour pouvoir communiquer sur le réseau. L'IP se compose de deux parties : L'adresse réseau Et l'adresse hôte, aussi se compose en deux versions principales : **IPv4 et IPv6**.

- Voici un exemple d'une IP en version 4 :

Adresse IPv4 : **192.168.0.1**
 Octet 32 bits → 4 294 467 295 IP

- L'IPv4 est la version qui est la plus utilisée aujourd'hui, mais plus pour très longtemps... Car elle sera, à terme, remplacée par l'IPv6.
- L'IPv4 est une adresse numérique de 32 bits, qui s'écrit en quatre chiffres, séparés par des points.
- Et chaque groupe de chiffres se fait appeler « Octet ».
- Il s'agit d'un chiffre qui peut être compris entre 0 et 255.
- La version 4 de l'IP peut produire+ de 4 milliards d'adresses...
- Les personnes qui ont inventé « Internet » pensaient que ce nombre d'adresses serait largement suffisant... Mais aujourd'hui, on est en manque d'adresse IPv4, et c'est pour cette raison que l'IPv6 est en train d'être déployé. La principale différence entre l'IPv4 et l'IPv6, c'est la longueur de l'adresse.

L'IPv4 est une adresse numérique en 32 bits, tandis que IPv6 est une adresse hexadécimale en 128 bits.

Voici maintenant un exemple d'une adresse IPv6 :

Adresse IPv6 : **21AE: 4F74: AB47: 27FE: 00DA: 05FC: BA54: 8814**
 128 bits → 340 282 366 920 938 463 463 374 607 431 768 211 456 IP

- L'hexadécimal utilise à la fois des chiffres et des alphabets dans l'adresse. Avec ça, il est possible d'avoir un nombre illimité d'adresses IPv6^{2...3}
- Car pour saturer le système, il faudrait placer plus de 667 milliards d'appareils connectés à internet sur chaque millimètre carré de la surface terrestre ! L'hexadécimal utilise à la fois des chiffres et des alphabets dans l'adresse. Avec ça, il est possible d'avoir un nombre illimité d'adresses IPv6... Car pour saturer le système, il faudrait placer plus de 667 milliards d'appareils connectés à internet sur chaque millimètre carré de la surface terrestre !

Comme on a vu, l'IP se compose de deux parties :

Une partie est pour *le réseau*

Et l'autre, pour *l'hôte*.

•MASQUE DE SOUS-RÉSEAU

Maintenant, pour savoir quelle partie appartient au réseau ou à l'hôte, eh bien c'est là que rentre en jeu : Le masque de sous-réseau!

². RFC 8200 – Internet Protocol Version 6 (IPv6)

³. RFC 2460 –Internet Protocol Version 6 (IPv6)

Un masque de sous-réseau est un nombre qui ressemble à une IP.

Il permet de savoir combien de bits de l'IP sont utilisés pour le réseau, en masquant la partie réseau de l'adresse.

•CALCUL IP

Par exemple, ici, nous avons l'adresse réseau **192.168.0.1** comme masque de sous-réseau, le **255.255.255.0**.

Les **3** premiers octets du masque sont alors **255**.

À présent, si nous passons le masque de sous-réseau en binaire, eh bien les **3** premiers octets ne seront que des «**1**», car l'ensemble des nombres d'un octet est égal à **255**.

Adresse IP			
Réseau	192	168	0
128	64	32	16
8	4	2	1
0	0	0	0
128 + 64 + 32	128 + 32 + 16 + 8 + 4 + 2 + 1	0 + 0	0 + 0
192	255	255	0

Masque de sous-réseau			
Réseau	255	255	255
128	64	32	16
8	4	2	1
0	0	0	0
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1
255	255	255	255

•CALCUL IP

Pour savoir **quelle partie de l'adresse IPv4 fait partie** du réseau, eh bien, **il faut se baser sur son masque de sous-réseau**.

La partie réseau de l'IPv4 correspond à tous les chiffres «**1**» du masque de sous-réseau.

Le chiffre «**1**» indique la position de l'adresse IP qui définit le réseau.

Nous allons donc barrer tous les chiffres de l'IP qui s'alignent avec les «**1**» du masque de sous-réseau.

Adresse IP			
Réseau	192	168	0
128	64	32	16
8	4	2	1
0	0	0	0
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1	128 + 64 + 32 + 16 + 8 + 4 + 2 + 1
255	255	255	255

5.4. Classe IP

Classe IP



On va maintenant parler des différentes classes qui existent. Voici une représentation des masques de sous-réseau par défaut pour les IP de **classe A, B et C, D, E**.

Vous pouvez voir les différentes parties du réseau et des hôtes en fonction des classes.

En tout, il y a en fait 5 classes, mais seules les **3** premières sont à connaître pour la certification **CompTIA**.

On peut différencier ces différentes classes, très simplement, en regardant le **1^{er} octet**.

Par exemple, le **1^{er} octet de** :

- Classe A: de 1.0.0.0 à 126.255.255.255
- Classe B: de 128.0.0.0 à 191.255.255.255
- Classe C: de 192.0.0.0 à 223.255.255.255
- Classe D: de 224.0.0.0 à 239.255.255.255
- Classe E: de 240.0.0.0 à 255.255.255.255

Vous remarquerez qu'il **manque le 127**. Eh bien, c'est parce qu'il s'agit d'un réseau réservé pour des tests qui se font appeler «**Loopback**».

❌ De 127.0.0.0 à 127.255.255.255 ❌ Loopback

@Loopback

- **Adresse Loopback (boucle locale):** L'adresse **loopback** est une adresse IP spéciale utilisée pour tester la pile réseau d'un ordinateur sans passer par le réseau physique (câble, carte réseau, etc.). En d'autres termes, le message envoyé reste dans la machine.
- Aucune communication réelle n'a lieu avec d'autres ordinateurs.
- En IPv4 :

L'adresse loopback est : 127.0.0.1

Le réseau réservé est : 127.0.0.0/8 (toutes les adresses de 127.0.0.0 à 127.255.255.255)

Toutes ces adresses pointent vers la machine locale.

? **Exemple**

Si vous tapez dans votre terminal :

ping 127.0.0.1

On obtiens une réponse du style :

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Cela prouve que ta pile TCP/IP fonctionne correctement.

Aucune donnée n'a quitté ton ordinateur.

Comparaison IPv4 vs IPv6

- IPv4 : 32 bits, ~4 milliards d'adresses.
- IPv6 : 128 bits, quasi illimité.
- IPv4 : fragmentation par routeurs.
- IPv6 : fragmentation par la source.
- IPv6 : entête simplifié + QoS + sécurité (IPSec).

5.5. ARP (Address Resolution Protocol)

ARP (Address Resolution Protocol)

🔑 **Définition**

Pour établir la correspondance entre l'adresse IP et l'adresse MAC, le protocole ARP (Address Resolution Protocol) est utilisé au niveau de la couche Liaison.

: ARP Il permet **de trouver l'adresse MAC** (adresse physique d'une carte réseau) correspondant **à une adresse IP donnée**. Il est utilisé uniquement dans un réseau local (LAN) pour assurer la communication entre machines⁴.

Concrètement : Une machine connaît l'adresse IP du destinataire, mais pas son adresse MAC. Elle envoie une requête ARP (**ARP Request**) diffusée à toutes les machines du réseau. La machine possédant cette IP répond avec son adresse MAC (**ARP Reply**). L'émetteur peut alors encapsuler ses données dans une trame Ethernet contenant l'adresse MAC du destinataire.³

⁴. RFC 826 – Address Resolution Protocol (ARP)

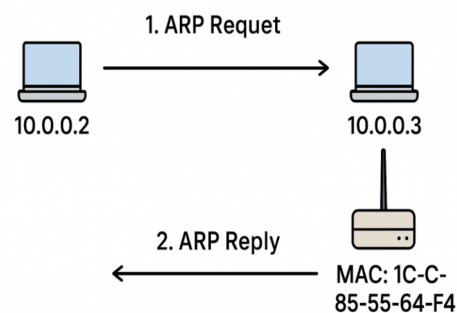
Processus ARP

1. ARP Request (Requête ARP)

- Quand un PC (ex. : 10.0.0.2) veut communiquer avec une machine du réseau local (10.0.0.3), il connaît son adresse IP, mais pas son adresse MAC.
- Il envoie donc une requête ARP en broadcast à toutes les machines du LAN : « Qui a l'adresse IP 10.0.0.3 ? Donnez-moi votre adresse MAC ».

2. ARP Reply (Réponse ARP)

- Seule la machine concernée (10.0.0.3) répond à l'émetteur avec sa MAC address unique (ex. 1C-C-85-55-64-F4).
- Cette réponse est envoyée en unicast directement au demandeur (10.0.0.2).



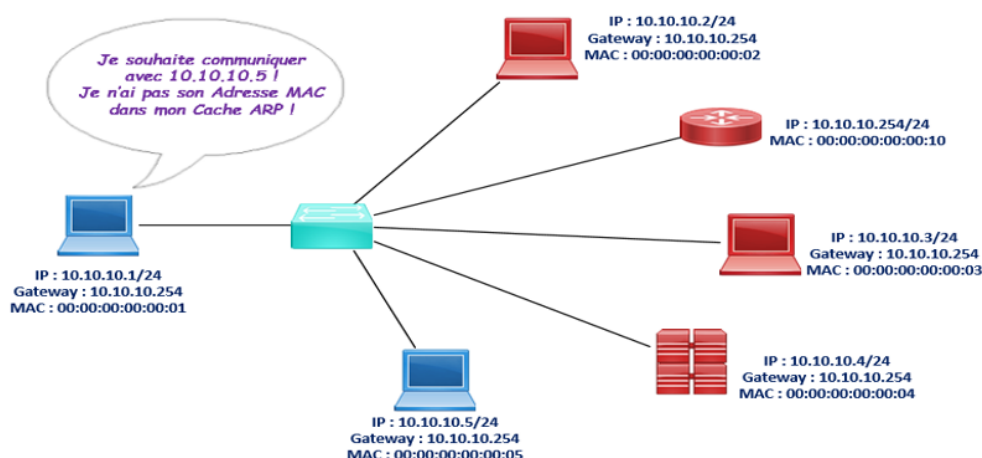
ARP Procédure

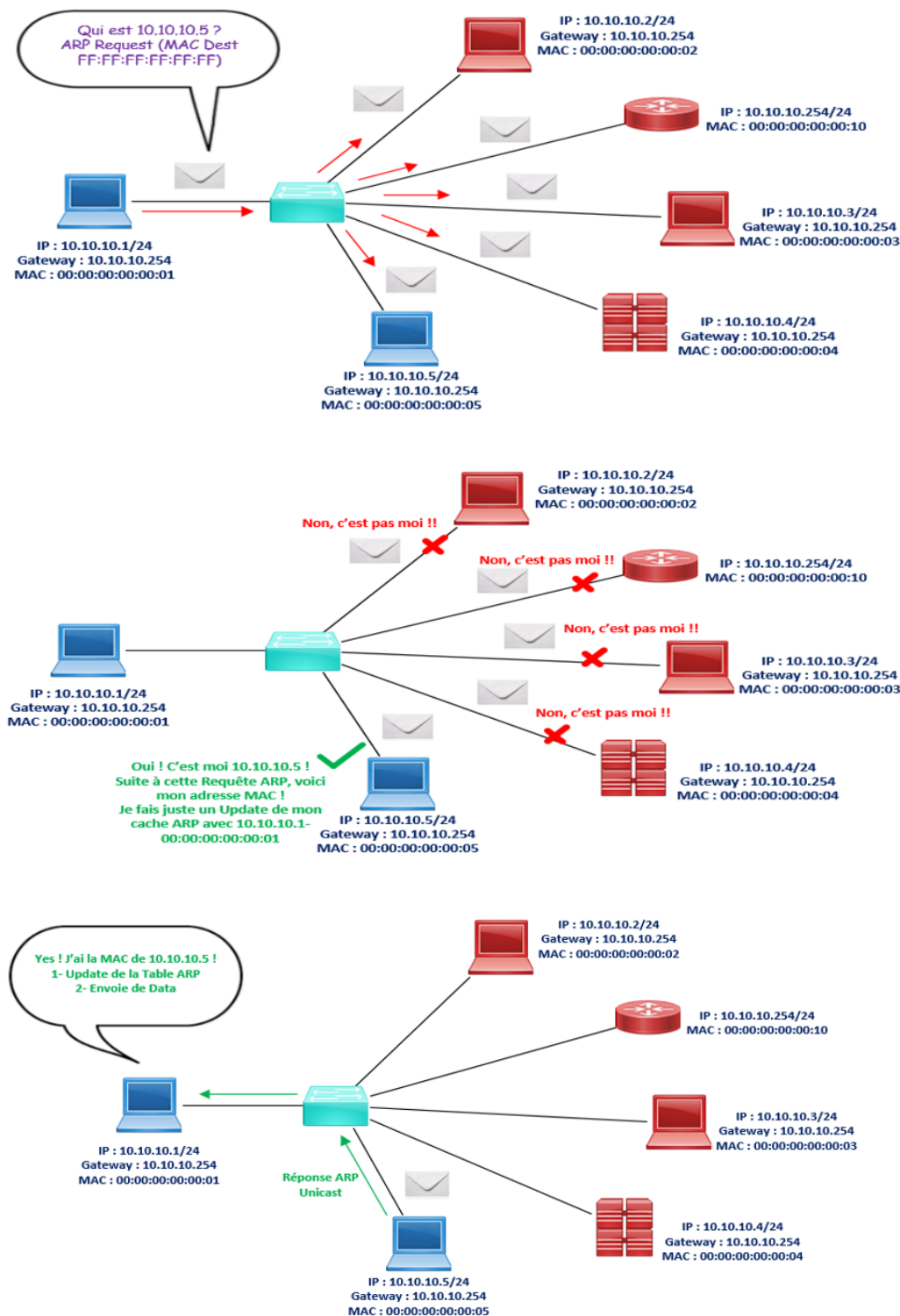
3. Mise à jour de la table ARP

- Le PC 10.0.0.2 enregistre désormais l'association IP ↔ MAC dans sa table ARP pour accélérer les futures communications.
- Ainsi, la prochaine fois, il n'aura pas besoin d'envoyer une requête ARP (gain de temps et de bande passante).

Les étapes (ARP)

? Exemple





Config et Visualisation:

Sur un PC, la commande "**arp -a**" permet de visualiser le cache ARP :

Sur un Routeur ou un Switch Layer 3 Cisco, la commande est "**show arp**"; \$il ne faut pas oublier\$

```
C:\Windows\system32>arp -a
Interface: 10.58.240.216 --- 0xe
Adresse Internet    Adresse physique    Type
10.58.240.42        de-49-bb-00-e5-50   dynamique
10.58.240.255       ff-ff-ff-ff-ff-ff   statique
224.0.0.22          01-00-5e-00-00-16   statique
224.0.0.251         01-00-5e-00-00-fb   statique
224.0.0.252         01-00-5e-00-00-fc   statique
239.255.255.250     01-00-5e-7f-ff-fa   statique
255.255.255.255     ff-ff-ff-ff-ff-ff   statique
```

CMD Windows

5.6. Exercice

Fonctionnement du protocole ARP

Énoncé: On considère un petit réseau local constitué de trois machines et d'un routeur :

Les quatre machines sont dans le même réseau local : **192.168.1.0/24**.

Aucune table ARP n'est encore renseignée.

Question :

1. Que se passe-t-il lorsque PC1 veut envoyer un paquet IP à PC2 (192.168.1.3) ?
2. Quelle trame ARP est émise ?
3. Quelle réponse ARP est reçue ?
4. Que contient la table ARP de PC1 après cet échange ?
5. Que se passe-t-il lorsque PC1 veut envoyer un message à Internet (ex. 8.8.8.8)?

Appareil	Adresse IP	Adresse MAC
PC1	192.168.1.2	AA-AA-AA-AA-AA-AA
PC2	192.168.1.3	BB-BB-BB-BB-BB-BB
PC3	192.168.1.4	CC-CC-CC-CC-CC-CC
Routeur (interface LAN)	192.168.1.1	DD-DD-DD-DD-DD-DD

5.7. Attribution des adresses IP

a) Attribution des adresses IP



Définition

Avant de terminer avec couche Internet, on va parler des différentes méthodes pour se faire attribuer une adresse IP.

Chaque ordinateur du réseau doit avoir une adresse IPv4, pour pouvoir communiquer.

Il existe deux façons d'attribuer une adresse IP à un ordinateur:

- Soit en utilisant une IP dynamique
- Soit avec une IP statique.

L'IP dynamique s'obtient automatiquement à l'aide d'un serveur DHCP (dynamic host configuration protocol).

1. Sous-adressage (Subnetting):

Technique qui consiste à diviser un réseau en sous-réseaux plus petits.

Objectifs :

Réduire les domaines de broadcast

Optimiser l'utilisation des adresses IP

Séparer les départements d'une entreprise

Améliorer la sécurité et la gestion.

b) Sous Adressage(S/D): Sta



Définition

Une adresse **IPv4 = 32 bits**, divisée en **4 octets (ex : 192.168.1.10)**.

Composée de :

- -Partie réseau (Network ID)
- -Partie hôte (Host ID)

Le masque de sous-réseau (subnet mask) détermine cette séparation.

? Exemple

Adresse : **192.168.1.10/24**

Masque : **255.255.255.0**

Réseau : **192.168.1.0**

Diffusion : **192.168.1.255**

Plage d'hôtes : **192.168.1.1 → 192.168.1.254**

Sous-adressage statique(Réseaux égaux)



Fondamental

L'administrateur configure manuellement les sous-réseaux et attribue les IP.

Par exemple

Réseau de base : **192.168.1.0/24 (254 hôtes).**

Besoin : **4 sous-réseaux égaux. (FLSM)**

Nouveau masque : /26 → 255.255.255.192.

Résultat :

- 192.168.1.0/26 → 62 hôtes utilisables
- 192.168.1.64/26 → 62 hôtes
- 192.168.1.128/26 → 62 hôtes
- 192.168.1.192/26 → 62 hôtes

Sous-adressage Statique (VLSM): Permet de créer des sous-réseaux de tailles variables (VLSM : Variable Length Subnet Mask). à partir d'un même réseau. Contrairement au sous-réseautage classique (où tous les sous-réseaux ont la même taille), le VLSM permet d'attribuer des tailles adaptées aux besoins réels (nombre d'hôtes par réseau).⁵

Pourquoi utiliser le VLSM ?

• Sans VLSM :

Tous les sous-réseaux ont la même taille, donc gaspillage d'adresses IP. Exemple : on crée 4 sous-réseaux de 62 hôtes même si un d'eux n'a besoin que de 10 machines.

• Avec VLSM :

On optimise l'espace d'adressage IP en allouant à chaque sous-réseau juste ce qu'il lui faut.

VLSM

? Exemple

VLSM

Réseau : 192.168.10.0/24

Besoins :

A : 100 hôtes

C : 25 hôtes

B : 50 hôtes

D : 10 hôtes

Solution :

A : 192.168.10.0/25 → 126 hôtes

B : 192.168.10.128/26 → 62 hôtes

C : 192.168.10.192/27 → 30 hôtes

D : 192.168.10.224/28 → 14 hôtes

- **Avantages:**

1. Contrôle total par l'administrateur.
2. Adapté aux petits réseaux fixes.

- **Inconvénients:**

1. Configuration lourde et sujette à erreurs.
2. Difficulté de maintenance dans un grand réseau.

c) Exercice : VLSM

Réseau : 192.168.50.0/24

Tu dois connecter 3 sous-réseaux :

- Site A : 58 hôtes
- Site B : 12 hôtes
- Site C : 6 hôtes
- Réserve pour future expansion : 30 hôtes

► Questions :

1. Donne les sous-réseaux selon VLSM?
2. Indique le masque et les plages d'hôtes?

d) Sous Adressage (S/D): Dyn



Le **DHCP** est un protocole qui permet de configurer des hôtes dynamiquement. Le serveur DHCP permet donc d'attribuer automatiquement une adresse IP à un ordinateur.

Par exemple, si j'ouvre les propriétés TCP/IP de la carte réseau de mon PC portable qui tourne sous Windows, on peut voir qu'il est configuré de manière à recevoir une adresse IPv4 automatiquement.

- Le serveur DHCP attribue automatiquement :
 - **une adresse IP,**
 - **un masque de sous-réseau,**
 - **la passerelle (gateway),**
 - **et le DNS.**
- Fonctionnement DHCP :
 - **DHCP Discover** : le client cherche un serveur DHCP.
 - **DHCP Offer** : le serveur propose une adresse IP.
 - **DHCP Request** : le client accepte la proposition.
 - **DHCP ACK** : le serveur confirme et attribue l'adresse IP.

L'adresse IP est louée pour une durée déterminée (lease time).

Pour visualiser ces paramètres en **CMD**, il suffit de taper la commande: «**ipconfig /all**». Il est toujours possible de libérer et/ou renouveler une configuration **IP DHCP** en tapant les deux commandes suivantes: «**ipconfig /release**» et «**ipconfig /renew**».

```

Adresse physique . . . . . : 26-6D-57-7B-05-50
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui

Carte réseau sans fil Connexion réseau sans fil :
Suffixe DNS propre à la connexion . . . :
Description . . . . . : Qualcomm Atheros AR9285 Wireless Net
work Adapter
Adresse physique . . . . . : 44-6D-57-7B-05-50
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui
Adresse IPv6 de liaison locale . . . . . : fe80::e4e5:ab7:bd59:466a%14<préféré>

Adresse IPv4 . . . . . : 10.58.240.216<préféré>
Masque de sous-réseau . . . . . : 255.255.255.0
Bail obtenu . . . . . : vendredi 3 octobre 2025 21:59:03
Bail expirant . . . . . : vendredi 3 octobre 2025 22:59:02
Passerelle par défaut . . . . . : 10.58.240.42
Serveur DHCP . . . . . : 10.58.240.42
ID ID DHCPv6 . . . . . : 272919895
DUID de client DHCPv6 . . . . . : 00-01-00-01-1B-AA-1C-E6-DC-0E-A1-E5-57-A9

Serveurs DNS . . . . . : 10.58.240.42
NetBIOS sur Tcpip . . . . . : Activé

Carte Ethernet Connexion au réseau local :
Statut du média . . . . . : Média déconnecté
Suffixe DNS propre à la connexion . . . :
Description . . . . . : Realtek PCIe FE Family Controller
Adresse physique . . . . . : DC-0E-A1-E5-57-A9
DHCP activé . . . . . : Oui
Configuration automatique activée . . . : Oui

```

Avantages

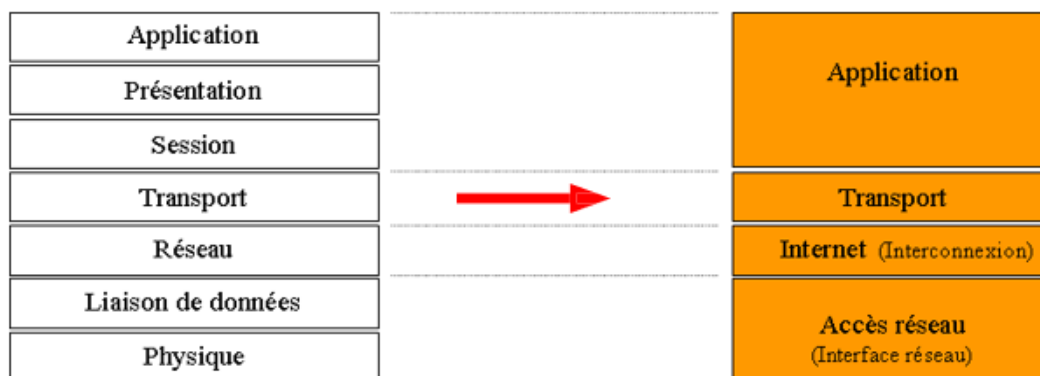
1. Optimisation maximale des adresses.
2. Facilité d'administration.

Inconvénients

1. Dépendance au serveur DHCP.
2. Plus complexe à mettre en place.

6. Couche-Transport

6.1. Couche-Transport



L'architecture O.S.I.

L'architecture TCP/IP
d'Internet

*Correspondance entre l'architecture O.S.I et l'architecture TCP/IP
d'Internet.*

La couche transport comporte 2 protocoles :

- **UDP** (User Datagramme Protocol)
- **TCP** (Transmission Control Protocol)

6.2. TCP



TCP est un protocole de communication de la couche Transport du modèle TCP/IP.²

- Il est orienté connexion (connection-oriented), ce qui signifie qu'avant d'envoyer des données, une connexion fiable doit être établie entre l'émetteur et le récepteur.
- Il est utilisé par beaucoup d'applications Internet : Web (HTTP/HTTPS), email (SMTP, IMAP, POP3), transfert de fichiers (FTP), etc.

Fonctionnement TCP

1. Établissement de la connexion (3-way handshake)

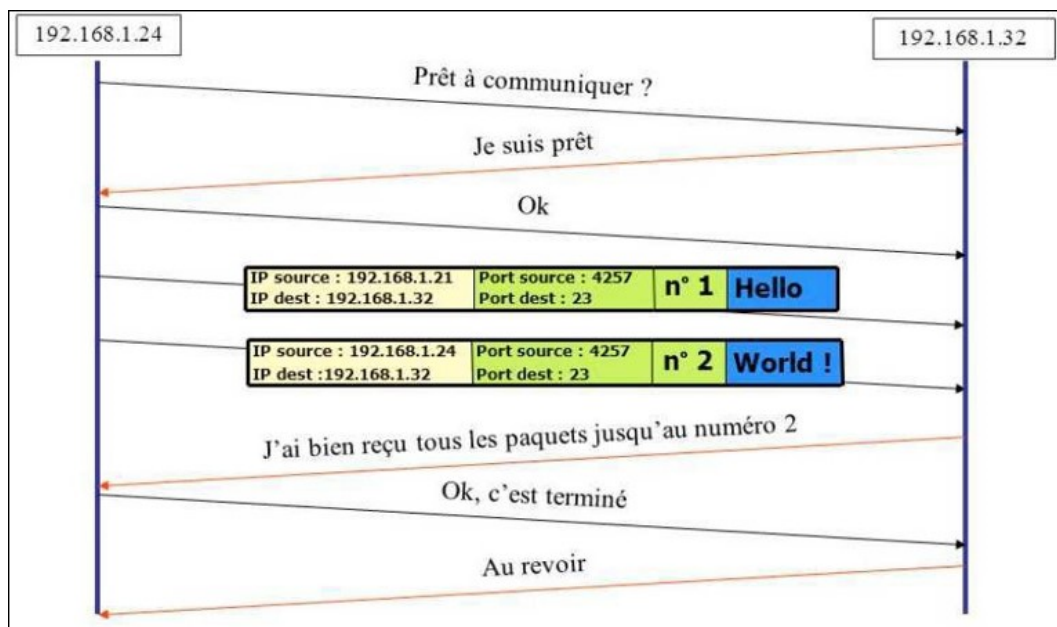
- Client → Serveur : SYN (je veux me connecter).
- Serveur → Client : SYN + ACK (d'accord, je t'entends).
- Client → Serveur : ACK (confirmation). àààConnexion établie.

2. Transmission des données

- Données découpées en segments.
- Chaque segment reçoit un numéro de séquence.
- Le récepteur envoie des accusés de réception (ACK) pour confirmer ce qu'il a bien reçu.
- En cas de perte → retransmission.

3. Fermeture de la connexion

- Se fait en 4 étapes (FIN, ACK, FIN, ACK).
- Permet de libérer proprement les ressources.



Quand vous ouvrez un site web (**ex. www.google.com**) :

Votre PC établit une connexion **TCP** avec le serveur **Google** (**port 443 en HTTPS**).

Les segments **TCP** transportent les requêtes HTTP (GET, POST...).

TCP garantit que les données arrivent bien, sans perte ni désordre. Une fois la page reçue, la connexion est fermée.

6.3. UDP



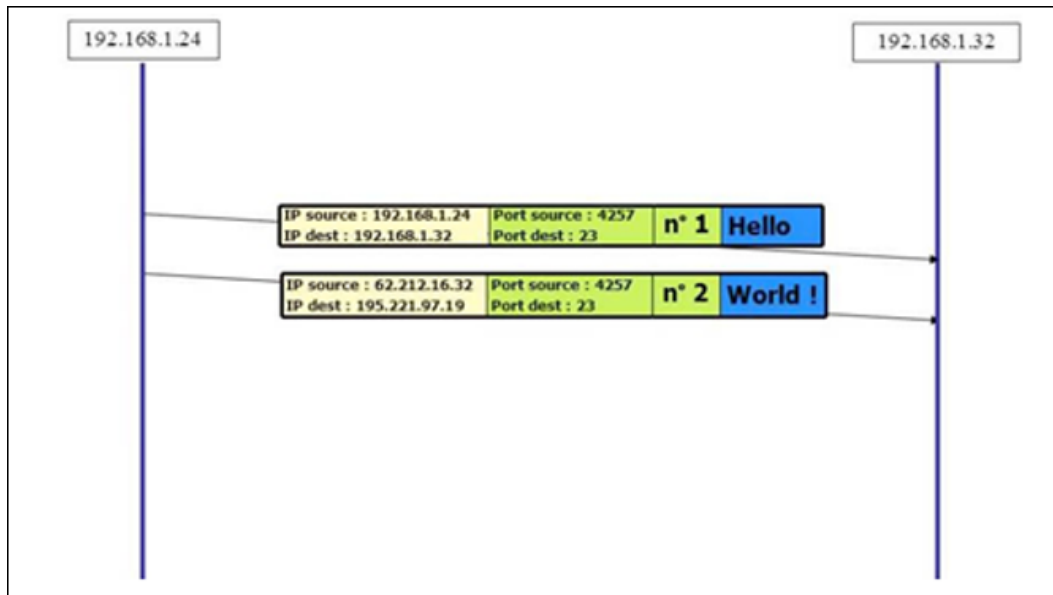
UDP (User Datagramme Protocol): protocole particulièrement simple.²

Avantage:

- Un temps d'exécution court qui permet de tenir compte des contraintes de «temps réel» ou de limitation de place sur un processeur.

Inconvénients:

- Non fiable (du point de vue sécurité). •Fournit un service sans reprise sur erreur, n'utilise aucun acquittement, •Ne re-séquence pas les messages et ne met en place aucun contrôle de flux.
- Les messages UDP peuvent être perdus, dupliqués, remis hors séquence ou arrivés trop tôt pour être traités lors de leur réception

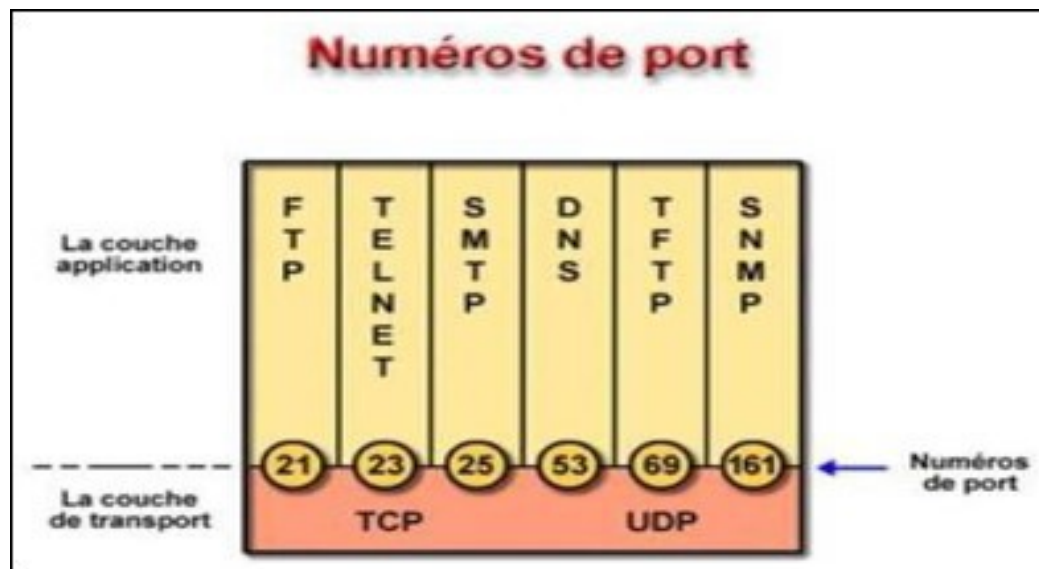


6.4. Notion de Port



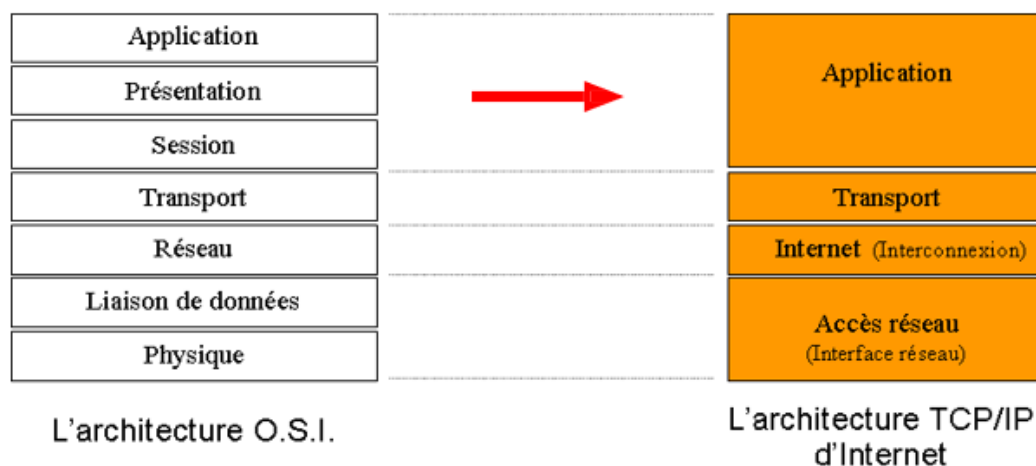
•**TCP et UDP** utilisent des numéros de port (ou de prise) pour transmettre de l'information aux couches supérieures. Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau •Les numéros inférieurs à 255 sont réservés aux applications publiques.

•**Les numéros de 255 à 1023** sont attribués aux entreprises pour les applications à commercialiser.



7. Couche-Application

7.1. Couche-Application



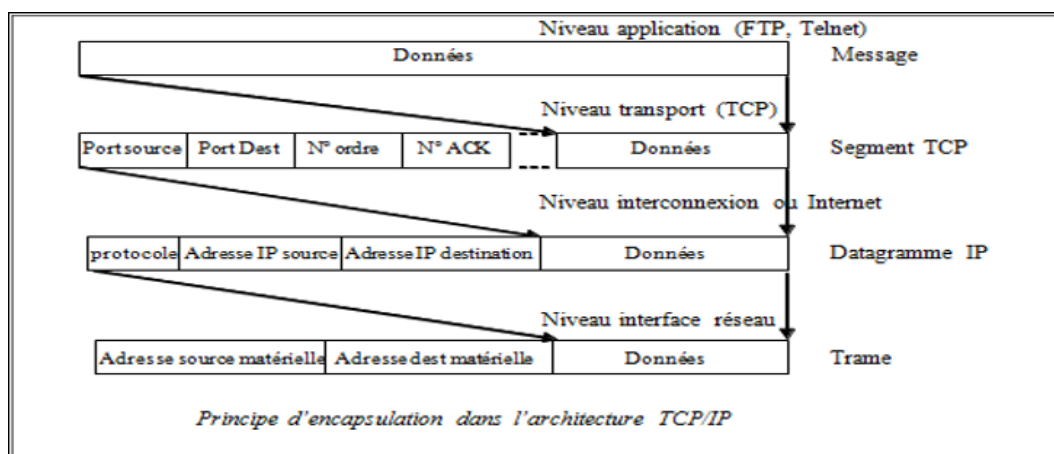
Correspondance entre l'architecture O.S.I et l'architecture TCP/IP d'Internet.

- **Héberge** la plupart des programmes et protocoles réseaux. Ces programmes fonctionnent généralement juste au- dessus des protocoles TCP et UDP et sont souvent associés à des ports bien définis (par défaut!).
- C'est l'application la **plus riche du point** de vue nombre d'applications réseaux et services associés.
- Elle englobe l'ensemble des couches **{session + présentation + application}** du modèle OSI.

N°	Nom de la couche	protocoles							Terminologie
		utilitaires							
4	Application	Telnet	HTTP	FTP	PING	FINGER	SMTP	SNMP...	Messages
3	Transport	TCP					UDP		Paquets
2	Internet (Interconnexion)	IP , ARP							Datagrammes
1	Interface du réseau	Ethernet, Token Ring, X25, ...							Trames

Protocoles de l'architecture TCP/IP

Protocoles (TCP/IP)



Principe d'encapsulation {TCP/IP}

8. Exercice : TEST

Le modèle TCP/IP comporte :

- ☐ 2 couches
- ☐ 4 ou 5 couches selon la présentation
- ☐ 7 couches obligatoires
- ☐ 10 couches

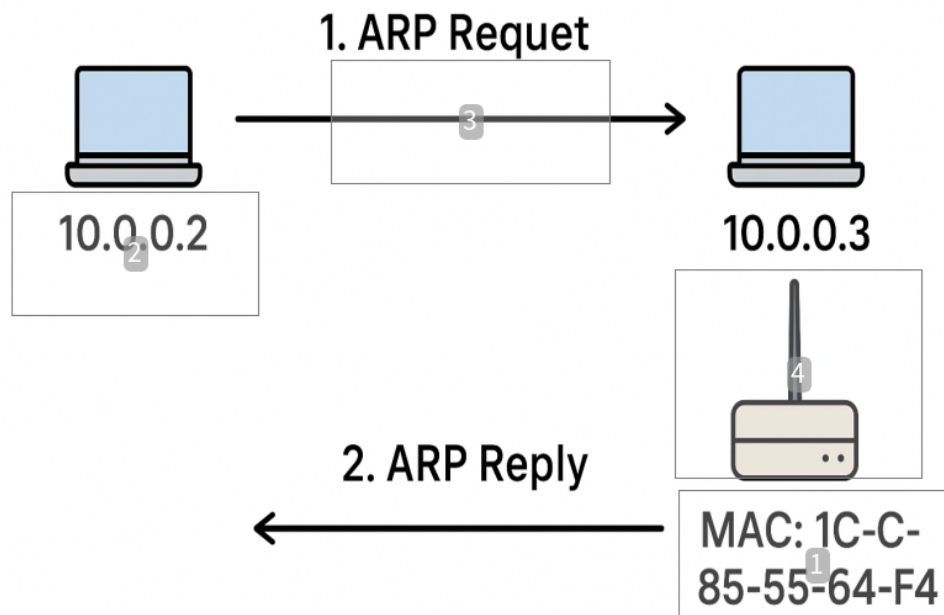
9. Exercice : TEST

L'adresse loopback en IPv4 est :

127.0.0.1

10. Exercice

Le protocole ARP permet de :



ARP Procédure

- ☐ **Zone 1**
Trouver une adresse MAC à partir d'une adresse IP
- ☐ **Zone 2**
Trouver une adresse IP à partir d'une adresse MAC sur Internet
- ☐ **Zone 3**
envoyer un paquet
- ☐ **Zone 4**
Assurer le routage dynamique