RESEAUX INFORMATIQUES : ADRESSAGE D'UN EQUIPEMENT

1 – PRINCIPES DE BASE DE LA COMMUNICATION

1.1 – Protocoles réseaux

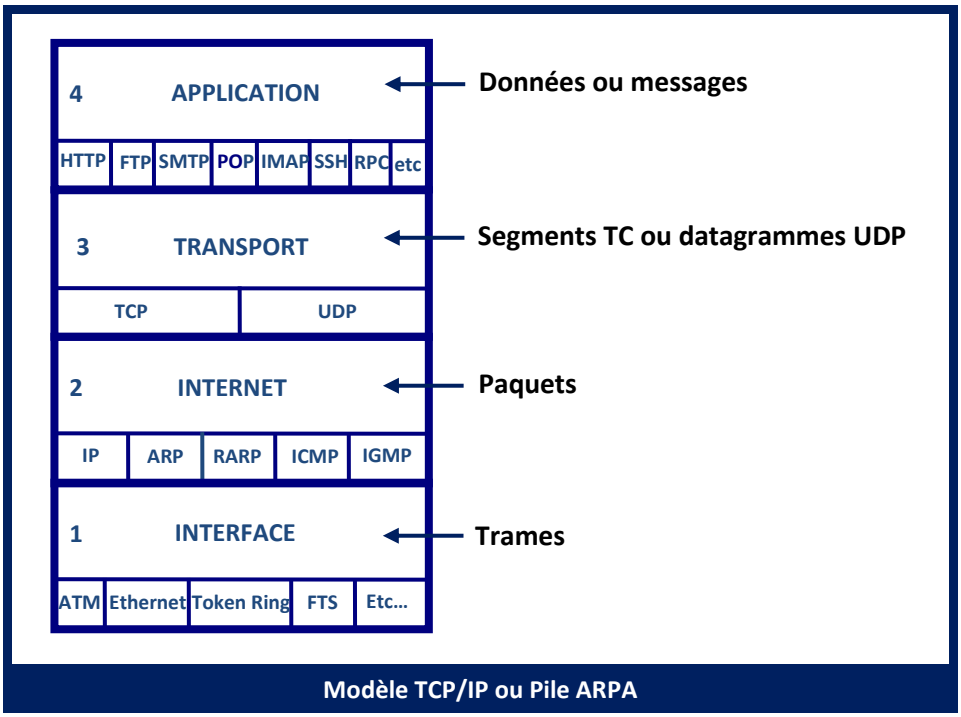
Un réseau peut être très complexe et consister en des périphériques connectés à Internet, ou alors très simple, comme deux ordinateurs connectés directement entre eux par un seul câble. La taille, la forme et la fonction des réseaux peuvent varier. Cependant, il ne suffit pas de connecter physiquement, via une connexion filaire ou sans fil, des périphériques finaux pour permettre la communication. **Les périphériques doivent également savoir comment communiquer**. Une communication doit être régie par des **règles appelées protocoles**. Les protocoles réseaux permettent de :

- Identifier l'expéditeur et le destinataire.
- Coder les messages.
- Formater et encapsuler les messages.
- Définir la taille des messages.
- Synchroniser les messages.
- S'assurer de la bonne transmission des messages.

1.2 – Protocoles TCP/IP

La **suite de protocoles TCP/IP** (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) a été développée à la fin des années 1970 à l'issue d'un projet de recherche sur les interconnexions de réseaux mené par le Département de la Défense Américain. La suite TCP/IP est actuellement la famille de protocoles réseau **la plus répandue**. Il s'agit notamment des **protocoles de l'Internet**. Il s'agit de **protocoles ouverts**, **indépendants du support physique** et avec **un mode d'adressage commun** à tous les utilisateurs.

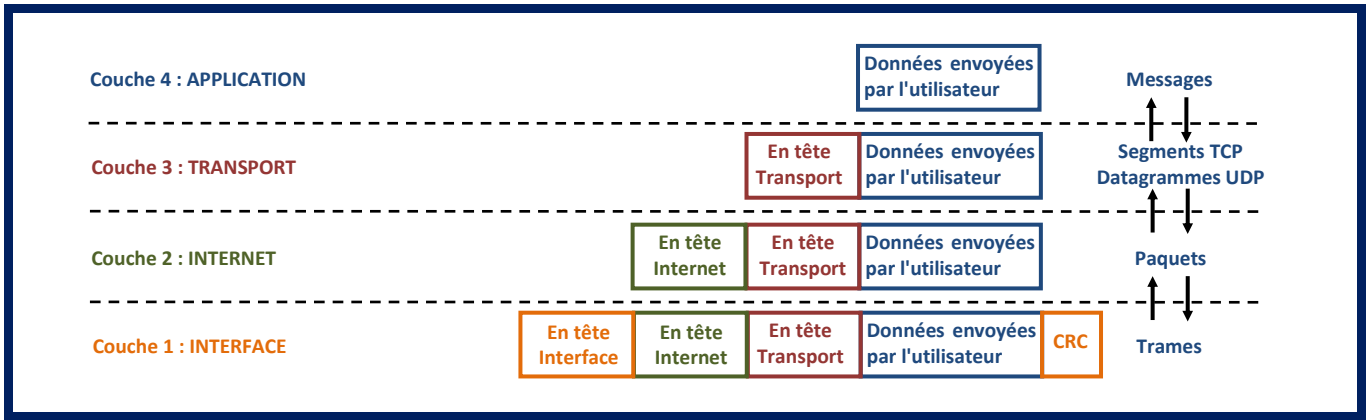
La **suite de protocoles TCP/IP** peut être modélisée par le modèle à 4 couches suivant nommé **modèle TCP/IP ou pile ARPA**.



Modèle TCP/IP ou Pile ARPA

1.3 - Encapsulation des protocoles

Lorsqu'une information passe d'une couche à une autre, le protocole qui **y ajoute** (**ou enlève**) **un En-tête** (**header**) qui lui est spécifique. On parle **d'encapsulation** (**ou décapsulation**) des protocoles.



Encapsulation-Décapsulation

1.4 – Segmentation

Le **MTU** (Maximum Transmission Unit) est la **taille maximale d'une trame** pouvant être **transmis en une seule fois** (sans fragmentation) par le réseau physique. Un paquet IP est destiné à être **encapsulé dans une trame qui ne peut excéder 1500 octets** pour une trame Ethernet.

Le découpage : Avant d'être envoyées sur le réseau, le **paquet est découpé en «morceaux multiples de 8 octets» appelés segments.** Ces segments peuvent circuler indépendamment les uns des autres sur le réseau. Chaque segment comprend **une étiquette avec son numéro d'ordre, son adresse de destination ainsi que l'identification de l'émetteur**.

L'aiguillage : Au cours du voyage, **il peut arriver que les segments n'empruntent pas tous la même route pour arriver à destination**, notamment parce qu'un routeur s'est rendu compte qu'un chemin est brusquement devenu saturé et qu'il valait mieux aiguiller quelques paquets sur une autre route.

Le regroupement : A la réception, les segments **n'arrivent pas forcément dans le bon ordre**. La **couche INTERNET du récepteur réassemble les segments** dans le bon ordre **à mesure leur arrivée grâce à leur numéro d'ordre** pour délivrer le **paquet initial** à la couche supérieure.

2 – ADRESSAGE

2.1 – Adresses réseau

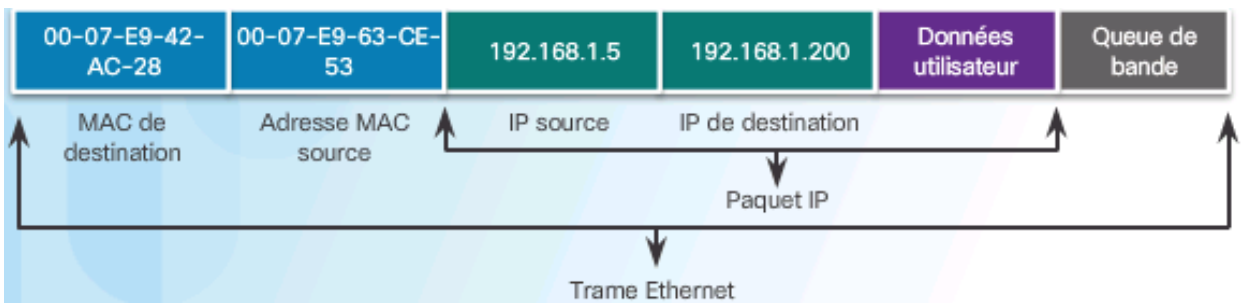
La grande majorité des réseaux actuels utilisent le **protocole Ethernet** et la **suite de protocoles TCP/IP**.

Le **protocole Ethernet et le protocole IP sont chargées de transmettre les données du périphérique source au périphérique de destination**. Ces protocoles gèrent des adresses source et de destination, mais ils ne les utilisent pas aux mêmes fins.

Le protocole Ethernet utilise les **adresses MAC (adresses physiques)** source et de destination pour **transmettre les trames** d'une carte réseau à une autre, **sur un même réseau**.

Le protocole IP utilise les **adresses IP** (**adresses logiques**) source et de destination pour **remettre les paquet IP** sur le **même réseau ou sur un réseau distant**.

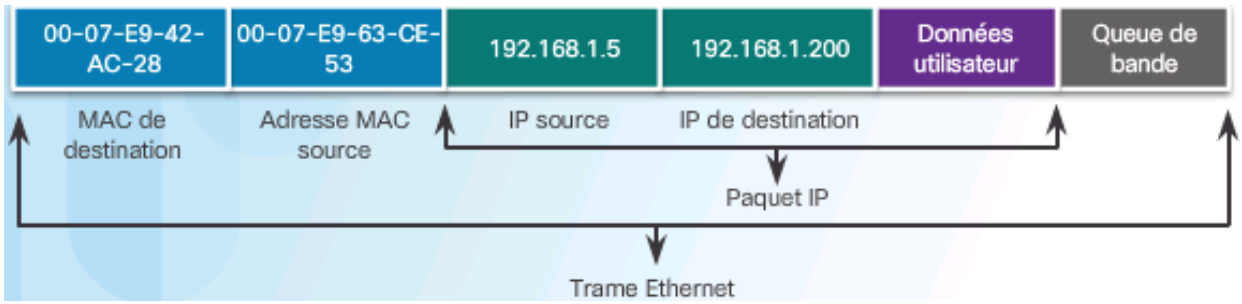
Une trame transmise sur un réseau TCP/IP va contenir les adresses MAC et les adresses IP de la source et de la destination.



Trame Ethernet

2.2 – Adresse IP

L'adresse IP ou adresse logique utilisée pour acheminer un paquet IP de la source d'origine à la destination. Il existe deux versions d'adresses IP : **les adresse IPV4 et les adresses IPV6**. Les réseaux actuels utilisent essentiellement les adresse IPV4 mais le déploiement de l'adressage IPV6 est en cours. Des mécanismes permettent la cohabitation des 2 modes d'adressage.



Adressage IP

Les adresses IPV4 sont codées sur **32 bits**, elles sont représentées sous la forme **de 4 octets compris entre 0 et 255** (valeur d'un octet). Cette adresse IPV4 se compose de 2 parties :

- **La partie réseau** ou **Net-Id** : qui permet d'identifier le réseau auquel appartient l'hôte.
- **La partie hôte** ou **Host-Id** : qui permet d'identifier l'hôte dans le réseau.

	Partie réseau			Partie hôte
Adresse IPV4	**192**	**168**	**10**	**10**
	11000000	**10101000**	**00001010**	**00001010**

Adressage IPV4

2.3 – Masque de sous réseau et adresse réseau

La partie réseau et la partie hôte d'une adresse IPV4 sont de **longueurs vari**ables.

Les **bits de la partie réseau doivent être identiques** pour tous les périphériques installés sur le même réseau. Les **bits de la partie hôte doivent être uniques**, pour identifier un hôte spécifique dans un réseau.

Le **masque de sous-réseau** permet d'**identifier la partie réseau et la partie hôte** dans une adresse IPV4. Il est donc utilisé **pour déterminer l'adresse du réseau** auquel le périphérique appartient. L'adresse réseau étant identique pour tous les périphériques du même réseau.

	Partie réseau			Partie hôte
Masque de sous-réseau	**255**	**255**	**255**	**0**
	11111111	**11111111**	**11111111**	**00000000**

Masque de sous-réseau

Les bits à 1 dans le masque de sous-réseau représentent la partie réseau, et les bits à 0 représentent la partie hôte. Pour **trouver l'adresse du réseau** auquel appartient un hôte, il faut réaliser un **ET logique entre son adresse IP et le masque de sous-réseau**.

Adresse IPV4	**192**	**168**	**10**	**10**
	11000000	**10101000**	**00001010**	**00001010**
Masque de sous-réseau	**255**	**255**	**255**	**0**
	11111111	**11111111**	**11111111**	**00000000**
Résultat ET logique	**11000000**	**10101000**	**00001010**	**00000000**
Adresse réseau	**192**	**168**	**10**	**0**

Masque de sous-réseau et Adresse réseau

Il est nécessaire quand on indique une adresse IPV4, de donner l'adresse IP et son masque de sous réseau : **Adresse IP = 192.168.1.1 - 255.255.255.0**

Cela peut être fastidieux mais il existe une méthode plus rapide **d'identification du masque de sous-réseau**, appelée la **longueur de préfixe**.

Cette longueur de préfixe correspond **au nombre de bits définis à 1 dans le masque de sous-réseau** : **192.168.1.1 - 255.255.255.0 = 192.168.1.1/24**

63.0.0.0 - 255.0.0.0 = **63.0.0.0/8**

172.16.0.0 - 255.255.0.0 = **172.16.0.0/16**

194.160.10.0 - 255.255.255.0 = **194.160.10/24**

168.38.64.0 - 255.255.192.0 = **168.38.64.0/18**

Exemples d'adresses IP et longueur de préfixe

2.4 – Adressage par classe

En 1981, les adresses IPV4 publiques étaient attribuées à l'aide de **l'adressage par classe**. Les clients recevaient une adresse réseau basée sur l'une **des trois classes, A, B ou C**.

Classe	Nb de Bits Net-ID	Nb de Bits Host-ID	Masque de sous-reseau	Premier octet	Plage d'adresses
A	8	24	255.0.0.0	0XXXX XXXX	0.0.0.0 à 127.255.255.255
B	16	16	255.255.0.0	10XX XXXX	128.0.0.0 à 192.255.255.255
C	24	8	255.255.255.0	110X XXXX	192.0.0.0 à 223.255.255.255

Classe A :
AD_IP : 12.15.5.45
Masque de sous - réseau : **255.0.0.0**
Adresse réseau : **12.0.0.0**

Classe B :
AD_IP : 143.25.67.89
Masque de sous - réseau : **255.255.0.0**
Adresse réseau : **143.25.0.0**

Classe C :
AD_IP : 192.23.67.123
Masque de sous - réseau : **255.0.0.0**
Adresse réseau : **192.23.67.0**

Exemples d'adressage par classe

Ce **type d'adressage a gaspillé de nombreuses adresses** et épuisé les adresses IPv4 disponibles. Cet adressage a été abandonné à la fin des années 1990 au profit **du système d'adressage sans classe** toujours d'actualité. L'adressage par classe est tout de même toujours utilisé dans les réseaux actuels dans la configuration de certaines fonctionnalités des routeurs ou par les systèmes d'exploitation des ordinateurs qui attribuent un masque de sous-réseau par défaut à partir des adresses IPV4.

2.5 – Adressage sans classe

Le système utilisé aujourd'hui porte le nom **d'adressage sans classe**. Son nom formel est le **routage CIDR** (**C**lassless **I**nter-**D**omain **R**outing, routage interdomaine sans classe). Ce système permet aux fournisseurs de services **d'attribuer des adresses IPV4 avec n'importe quelle longueur de préfixe** au lieu d'utiliser uniquement les classes A, B ou C. L'objectif était de retarder la pénurie voire l'épuisement des adresses IPV4.

2.6 – Adresse réseau, adresse hôte et adresse de broadcast

Lorsque **tous les bits de la partie hôte sont à 0**, nous obtenons **l'adresse réseau** auquel appartient cette adresse IPV4. Cette adresse ne peut pas être affectée à un hôte.

Lorsque **tous les bits de la partie hôte sont à 1**, nous obtenons **l'adresse de broadcast** du réseau auquel appartient cette adresse IPV4. Cette adresse ne peut pas être affectée à un hôte.

Le **nombre d'hôtes adressables** dans un réseau est donc : $\mathbf{2^{nbh}} - \mathbf{2}$ avec **nbh** correspondant au nombre de bits de la partie hôte.

AD_IP1: 172.16.35.2 – 255.255.0.0
Nb d'hôtes : $\mathbf{2^{16} - 2 = 64534}$ **hôtes**
Adresse réseau : 172.16.**00000000.00000000 = 172.16.0.0**
Adresse 1er hôte : 172.16.**00000000.00000000 = 172.16.0.1**
Adresse dernier hôte : 172.16.**11111111.11111110 = 172.16.0.254**
Adresse broadcast : 172.16.**11111111.11111111 = 172.16.0.255**

AD_IP2: 194.104.2.28/28
Nb d'hôtes : $\mathbf{2^{4} - 2 = 14}$ **hôtes**
Adresse réseau : 194.104.2.0001**0000 = 194.104.2.16**
Adresse 1er hôte : 194.104.2.0001**0001 = 194.104.2.17**
Adresse dernier hôte : 194.104.2.0001**1110 = 194.104.2.30**
Adresse broadcast : 194.104.2.0001**1111 = 194.104.2.31**

Exemples

2.7 – Adresses IPV4 publiques et privées

Les **adresses IPV4 publiques peuvent acheminées sur internet**. Certains blocs d'adresses appelés **adresses privées** sont utilisés dans les réseaux locaux pour attribuer des adresses IPv4 aux hôtes internes. Ces adresses **ne sont pas routables sur internet**.

Les blocs d'adresses privées sont les suivants :

- **10.0.0.0 /8** : **10.0.0.0 à 10.255.255.255**
- **172.16.0.0 /12** : **172.16.0.0 à 172.31.255.255**
- **192.168.0.0 /16** : **192.168.0.0 à 192.168.255.255**

2.8 – Adresses IPV4 d'utilisateurs spéciaux

Certaines adresses, telles que l'adresse réseau et l'adresse de diffusion ne peuvent pas être attribuées à des hôtes. **Il existe également des adresses spéciales qui peuvent être attribuées aux hôtes**, mais des restrictions s'appliquent sur les interactions de ces hôtes sur le réseau.

Adresses de bouclage (**127.0.0.0 /8** ou **127.0.0.1** à **127.255.255.254**) : Ces adresses spéciales sont utilisées par des hôtes pour **diriger le trafic vers eux-mêmes**. Par exemple, elles peuvent être utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle.

Adresses locales-liens (**169.254.0.0 /16** ou **169.254.0.1** à **169.254.255.254**) : Ces adresses sont utilisées par un client DHCP Windows pour se **configurer automatiquement si aucun serveur DHCP n'est disponible**.

Adresses TEST-NET (**192.0.2.0/24** ou **192.0.2.0** à **192.0.2.255**) : ces adresses sont réservées à des fins pédagogiques et utilisées dans la documentation et dans des exemples de réseau.

2.9 – Adresses IPV6

Le manque d'espace d'adressage IPV4 a conduit à la transition vers l'IPV6. Le **protocole IPV6 possède un plus grand espace d'adressage** (**adresse IPV6 sur 128 bits**). Il apporte également quelques **améliorations** par rapport protocole IPV4. Ces deux protocoles vont coexister pendant un certain temps. Des mécanismes ont été mis en place pour assurer la coexistence des protocoles.

Une adresse IPV6 a une longueur de **128 bits** et sont notées sous forme de **symboles hexadécimaux organisés par groupes de 4 séparés par « : »** :

2001	**:**	**0DB8**	**:**	**0000**	**:**	**1111**	**:**	**0000**	**:**	**0000**	**:**	**0000**	**:**	**0200**

Deux règles permettent de simplifier l'écriture d'une adresse IPV6 :

Règle n °1 - Omettre les zéros en début de segment

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200

2001	**:**	**DB8**	**:**	**0**	**:**	**1111**	**:**	**0**	**:**	**0**	**:**	**0**	**:**	**200**

Règle n°2 - Omettre les séquences composées uniquement de zéros
Une suite de deux fois deux points « **::** » peut remplacer toute suite d'un ou plusieurs groupes composés uniquement de zéros. Cette suite ne peut être utilisée qu'une seule fois par adresse

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200

2001	:	DB8	:	0	:	1111	:	**0**	:	**0**	:	**0**	:	200

2001 : DB8 : 0 : 1111 :: 200

3 – ADRESSES PHYSIQUES ET PROTOCOLE ARP

3.1 – Notion d'adresse physique

Chaque machine connectée au réseau possède **un numéro d'identification de 48 bits**. Ce numéro est un numéro unique qui est fixé dès la fabrication de la carte en usine. **On la retrouve sous la dénomination adresse MAC ou adresse physique.** Le protocole Ethernet utilise ces adresses physiques **pour identifier les périphériques connectés sur le réseau**.

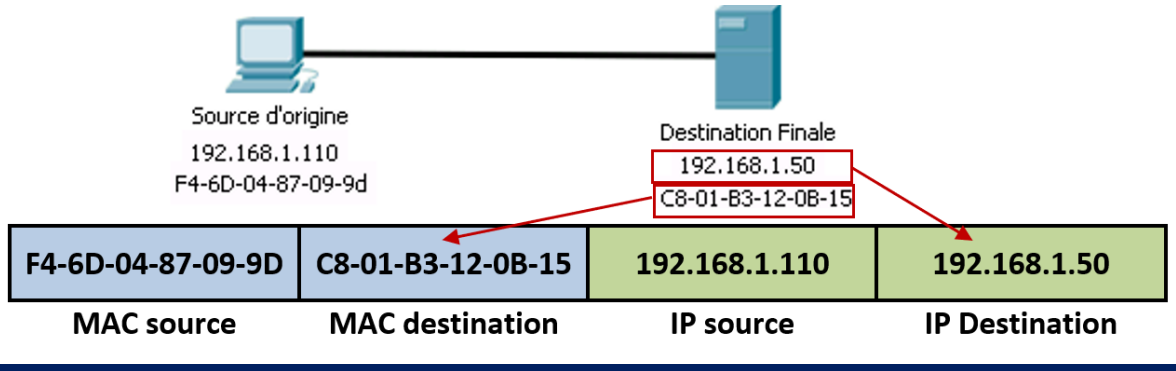
Une adresse MAC est constituée de **48 bits** organisés sous la forme **de 12 symboles hexadécimaux**. Les 24 bits de poids forts (3 octets) permettent **d'identifier le fabricant** de la carte réseau (identifiant OUI : Organizationally Unique Identifier). Les 24 bits suivants permettent **d'identifier la carte réseau avec une valeur unique**.

OUI						**Identifiant carte**				
F4	**–**	**6d**	**–**	**04**	**–**	**87**	**–**	**09**	**–**	**9D**

ASUSTek COMPUTER INC

3.2 – Transfert des trames sur le même réseau

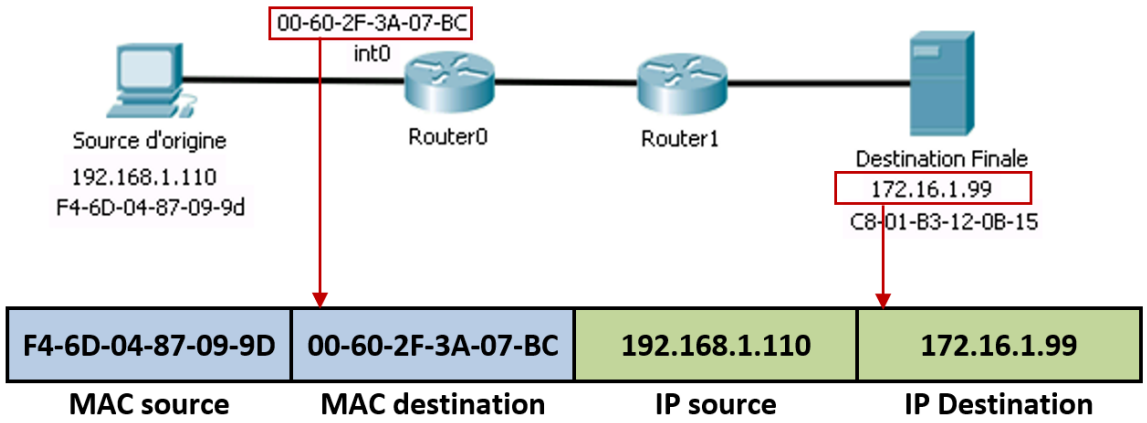
Si un hôte envoie une trame à un autre hôte sur le même réseau, la **trame transmise est constituée des adresses IP et MAC de l'hôte destinataire**.



Transfert de trames sur le même réseau

3.3 – Transfert des trames sur réseau distant

Si un hôte envoie une trame à un hôte sur un réseau distant, la **trame est constituée de l'adresses IP de l'hôte destinataire et de l'adresse MAC de la passerelle par défaut (interface routeur)**.



Transfert de trames sur réseau distant

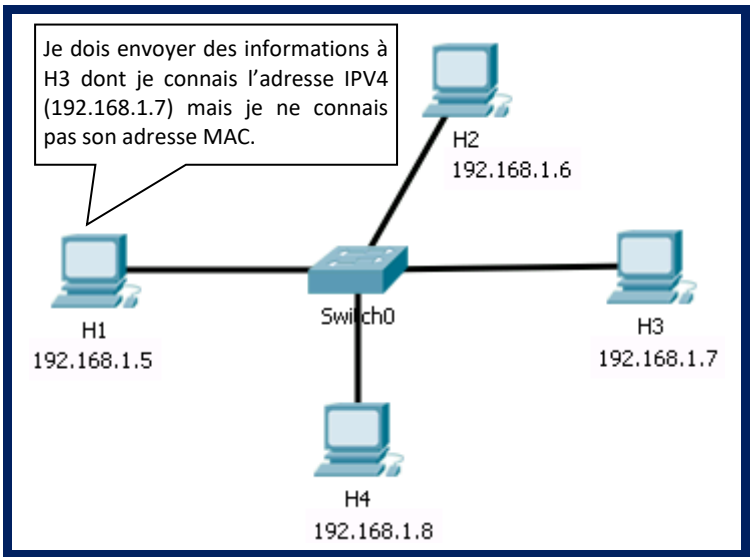
3.3 – Traitement des trames

Lorsqu'une carte réseau reçoit une trame Ethernet, elle observe **l'adresse MAC de destination** pour voir **si elle correspond son adresse MAC**. En l'absence de correspondance, la **carte réseau ignore la trame**. Si elle correspond, la **carte réseau transmet la trame à l'ordinateur** au système d'exploitation.

3.4 – Correspondance adresse IP - adresse MAC (Protocole ARP)

Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient les adresses IP de la source et de la destination. **Elle contient également les adresses MAC de la source et de la destination**.

Si un périphérique ne connait pas l'adresse MAC d'un destinataire, il va utiliser le **protocole ARP** (Protocole de Résolution d'Adresse) qui permet de faire **correspondre les adresses physiques aux adresses IP**. Ce protocole interroge les machines du réseau pour connaître leur adresse physique, puis créer une table ARP qui fait correspondre les adresses IP et physiques.

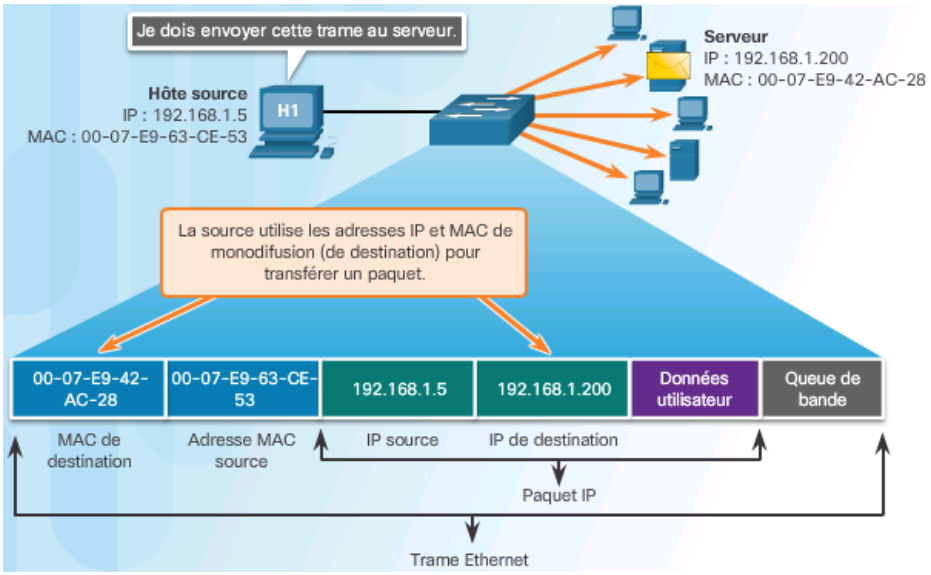


Protocole ARP

4 – DIFFERENTS TYPES DE DIFFUSION DE MESSAGES

4.1 – Monodiffusion ou « unicast »

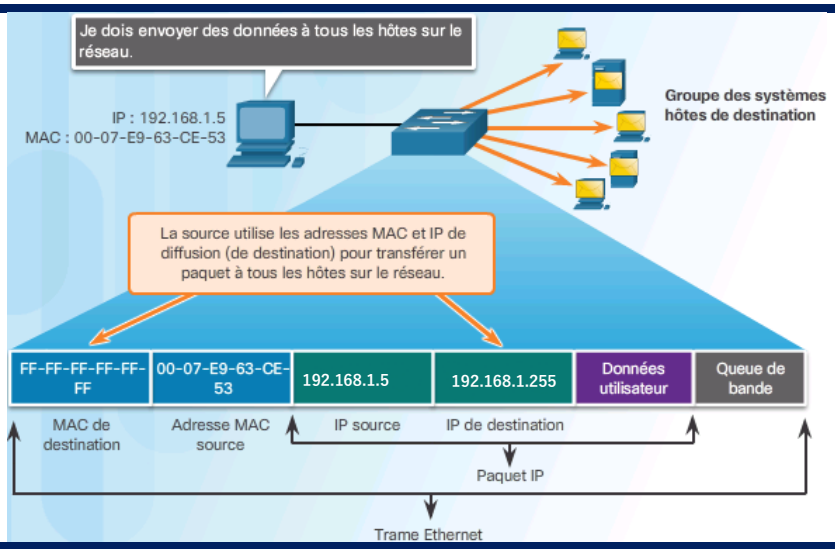
C'est le principe le plus utilisé et le plus simple. On peut envoyer les trames en **spécifiant l'adresse IP de l'hôte à qui on veut envoyer les informations**. Seule la machine ayant l'adresse contenue dans la trame regarde et traite l'information.



Monodiffusion

4.2 – Diffusion ou « broadcast »

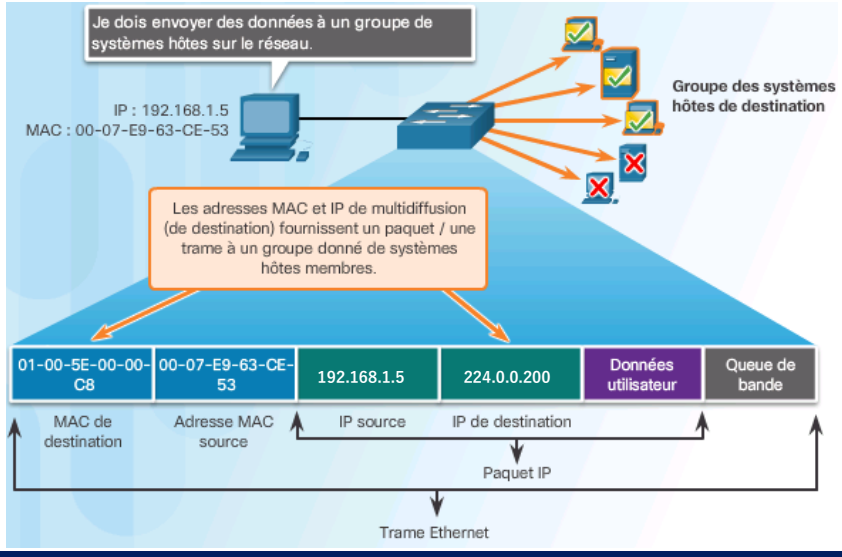
Le principe du **broadcast** est **d'envoyer une information à tous les hôtes du réseau en utilisant une adresse spécialisée dite de broadcast**. L'adresse IPV4 de broadcast **s'obtient en tous les bits de la partie hôte à 1**. L'adresse MAC de broadcast est **FF-FF-FF-FF-FF-FF**.



Diffusion

4.2 – Multidiffusion ou « multicast »

Le principe du **multicast** est **d'envoyer une information à un groupe de périphériques du réseau.** Les périphériques qui font partie d'un groupe multidiffusion se voient affecter une **adresse IP de groupe multidiffusion**. La plage d'adresses de multidiffusion IPV4 s'étend de **224.0.0.0 à 239.255.255.255**.
L'adresse **MAC de multidiffusion** commence toujours par **01-00-5E**. L'autre partie de l'adresse MAC de multidiffusion correspond à la **conversion des 23 bits de poids faible de l'adresse IPV4** du groupe de multidiffusion en 6 symboles hexadécimaux.



Multidiffusion