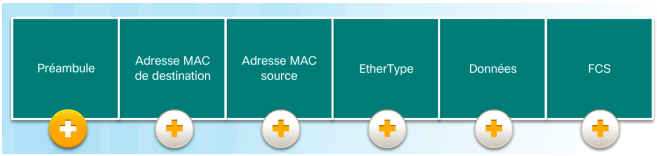
SOMMAIRE

1. Protocole Ethernet:

1.1 Champs de trame Ethernet :



Préambule :
Le champ Préambule (à 7 octets) et le champ Délimiteur de début de trame (SFD), également appelé Début de trame (à 1 octet) sont utilisés à des fins de synchronisation entre les périphériques d'envoi et de réception. Les huit premiers octets de la trame préparent les noeuds de réception à recevoir. Les quelques premiers octets indiquent essentiellement aux récepteurs de se préparer à recevoir une nouvelle trame.

Adresse MAC de destination :
Ce champ de 6 octets est l'identifiant du destinataire. Comme nous l'avons vu précédemment, cette adresse est utilisée par la couche 2 pour aider les périphériques à déterminer si une trame leur est adressée. L'adresse de la trame est comparée à l'adresse MAC du périphérique. Si les deux correspondent, le périphérique accepte la trame. Il peut s'agir d'une adresse de monodiffusion, de multidiffusion ou de diffusion.

Adresse MAC source :
Ce champ de 6 octets identifie la carte réseau ou l'interface d'origine de la trame. Il doit s'agir d'une adresse de monodiffusion.

Ethertype :
Ce champ de 2 octets identifie le protocole de la couche supérieure encapsulé dans la trame Ethernet. Les valeurs hexadécimales les plus fréquentes sont 0x800 pour IPv4, 0x86DD pour IPv6 et 0x806 pour ARP.

Données :
Ce champ de 46 à 1 500 octets contient les données encapsulées d'une couche supérieure, ce qui correspond à une unité de données de protocole de la couche 3, c'est-à-dire un paquet IPv4. La longueur minimale de la trame est fixée à 64 octets. Si un paquet de petite taille est encapsulé, d'autres bits appelés remplissage sont utilisés pour augmenter la trame et la ramener à cette taille minimale.

Séquence de contrôle de trame :
Ce champ de 4 octets permet de détecter les erreurs d'une trame. Il utilise le contrôle de redondance cyclique (CRC, Cyclic Redundancy Check). Le périphérique d'envoi inclut les résultats d'un CRC dans le champ FCS de la trame. Le périphérique de réception reçoit la trame et génère un CRC pour détecter les erreurs. Si les calculs correspondent, aucune erreur ne se produit. Les calculs non rapprochés indiquent que les données ont changé et que la trame est abandonnée. Si les données sont modifiées, cela provient sans doute d'une perturbation des signaux électriques qui représentent les bits.

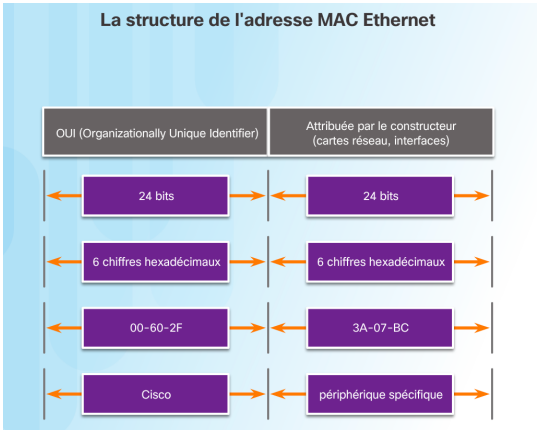
La taille minimale des trames Ethernet est de 64 octets et la taille maximale de 1 518 octets. Cela comprenait tous les octets du champ Adresse MAC de destination jusqu'au champ Séquence de contrôle de trame. Le champ Préambule n'est pas inclus dans la description de la taille d'une trame.

Toute trame inférieure à 64 octets est interprétée comme un « fragment de collision » ou une « trame incomplète » et est automatiquement rejetée par les périphériques récepteurs. Les trames de plus de 1 500 octets de données sont considérées comme des trames « jumbo » (géantes) ou « baby giant frames » (légèrement géantes).

Si la taille d'une trame transmise est inférieure à la taille minimale ou supérieure à la taille maximale, le périphérique récepteur abandonne la trame. Les trames abandonnées sont souvent le résultat de collisions ou d'autres signaux rejetés et donc traités comme étant non valides.

1.2 Adresse MAC :

Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal).



Dans la norme Ethernet, chaque périphérique réseau se connecte au même support partagé. À une époque, Ethernet était principalement une topologie en mode semi-duplex utilisant un bus à accès multiple, et plus tard, des concentrateurs Ethernet. Ainsi, tous les nœuds recevaient toutes les trames transmises. Pour éviter la surcharge excessive liée au traitement de chaque trame, des adresses MAC qui identifient la source et la destination réelles ont été créées. L'adressage MAC fournit une méthode d'identification des périphériques au niveau inférieur du modèle OSI. Bien qu'Ethernet utilise désormais des cartes réseau et des commutateurs en mode duplex intégral, il reste possible qu'un périphérique reçoive une trame Ethernet alors qu'elle ne lui est pas destinée.

Structure de l'adresse MAC :

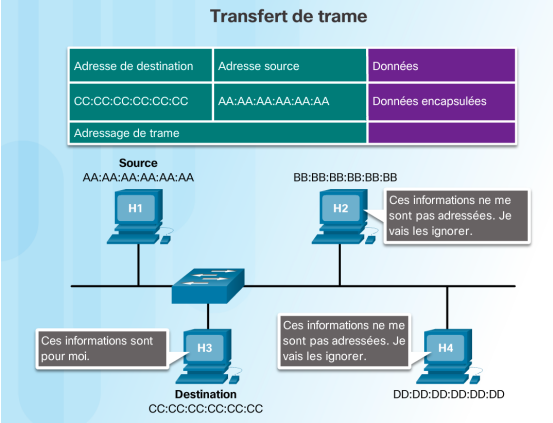
La valeur de l'adresse MAC est un résultat direct des règles mises en application par l'IEEE auprès des revendeurs pour garantir l'attribution d'adresses uniques à chaque périphérique Ethernet, et ce, à l'échelle mondiale. Les règles établies par l'IEEE exigent de chaque revendeur de périphérique Ethernet qu'il s'enregistre auprès de l'IEEE. L'IEEE attribue au constructeur un code de 3 octets (24 bits) appelé OUI (Organizationally Unique Identifier).

L'IEEE demande aux constructeurs de respecter deux règles simples représentées sur la figure :

- Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.
- Toutes les adresses MAC ayant le même identifiant OUI doivent utiliser une valeur unique dans les 3 derniers octets.

Remarque : il peut exister des doublons d'adresses MAC en raison d'erreurs liées à la fabrication ou à certaines méthodes de mise en œuvre de machines virtuelles. Dans tous les cas, l'adresse MAC devra être modifiée à l'aide d'une nouvelle carte réseau ou dans le logiciel.

1.3 Traitement des trames :



L'adresse MAC est souvent dite rémanente (BIA), car, à l'origine, elle était gravée dans la mémoire morte (ROM) de la carte réseau. Cela signifie que l'adresse est codée de manière permanente dans la puce de mémoire morte.

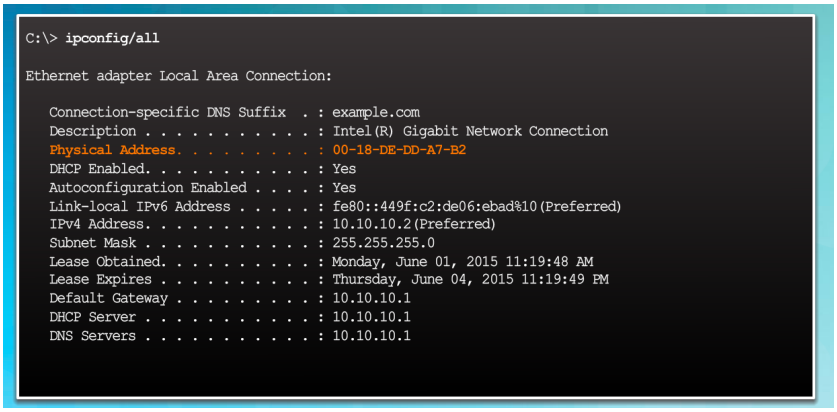
Remarque : sur les systèmes d'exploitation et les cartes réseau des ordinateurs actuels, il est possible de modifier l'adresse MAC dans le logiciel. Cela peut être utile si vous essayez d'obtenir l'accès à un réseau qui filtre les adresses rémanentes. De ce fait, le filtrage ou le contrôle du trafic sur la base de l'adresse MAC n'est plus aussi sécurisé.

Lorsque l'ordinateur démarre, la carte réseau commence par copier l'adresse MAC de la mémoire morte à la mémoire vive. Lorsqu'un périphérique transmet un message à un réseau Ethernet, il intègre des informations d'en-tête au paquet. Les informations d'en-tête contiennent l'adresse MAC source et de destination.

Lorsqu'une carte réseau reçoit une trame Ethernet, elle observe l'adresse MAC de destination pour voir si elle correspond à l'adresse MAC physique du périphérique stockée dans la mémoire vive (RAM). En l'absence de correspondance, la carte réseau ignore la trame. Si elle correspond, la carte réseau transmet la trame aux couches OSI, et la désencapsulation a lieu.

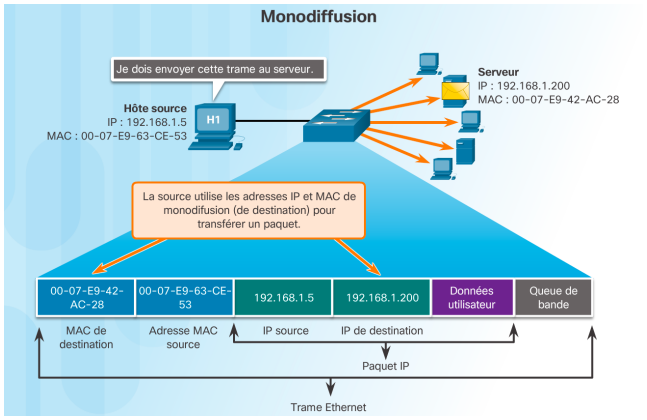
Remarque : les cartes réseau Ethernet acceptent également les trames si l'adresse MAC de destination est un groupe de diffusion ou de multidiffusion auquel l'hôte appartient.
Une adresse MAC doit être attribuée à tout périphérique qui peut être la source ou la destination d'une trame Ethernet. Cela inclut les postes de travail, les serveurs, les imprimantes, les appareils mobiles et les routeurs.

1.4 Représentations des adresses MAC :



Sur un hôte Windows, la commande **ipconfig /all** permet d'identifier l'adresse MAC d'un adaptateur Ethernet. Sur la figure précédente, notez que l'écran indique que l'adresse physique (MAC) de l'ordinateur est 00-18-DE-DD-A7-B2. Si vous avez accès à la ligne de commande, vous pouvez déterminer celle de votre propre ordinateur. Sur les hôtes MAC ou Linux, c'est la commande **ifconfig** qui est utilisée.

1.8 Adresse MAC de monodiffusion :



Avec Ethernet, des adresses MAC différentes sont utilisées pour la monodiffusion (unicast), la multidiffusion (multicast) et la diffusion (broadcast) sur la couche 2.

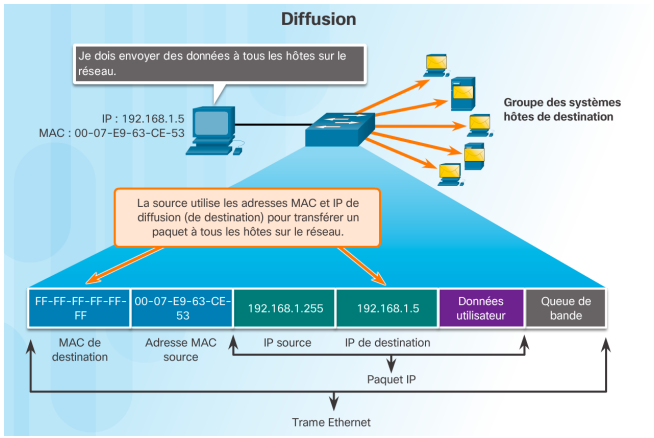
L'adresse MAC de monodiffusion est l'adresse unique utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique émetteur, à un seul périphérique destinataire.

Sur le schéma précédent, un hôte avec l'adresse IPv4 192.168.1.5 (source) demande une page web au serveur dont l'adresse IPv4 de monodiffusion est 192.168.1.200. Pour qu'un paquet monodiffusion soit envoyé et reçu, une adresse IP de destination doit figurer dans l'en-tête du paquet IP. Une adresse MAC de destination correspondante doit également être présente dans l'en-tête de la trame Ethernet. Les adresses IP et MAC se combinent pour transmettre les données à un hôte de destination spécifique.

Le processus qu'un hôte source utilise pour déterminer l'adresse MAC de destination est appelé protocole ARP (Address Resolution Protocol). Il est traité ultérieurement dans ce chapitre.

L'adresse MAC de destination peut donc être une adresse de monodiffusion, de diffusion ou de multidiffusion, mais l'adresse MAC source doit toujours être une adresse de monodiffusion.

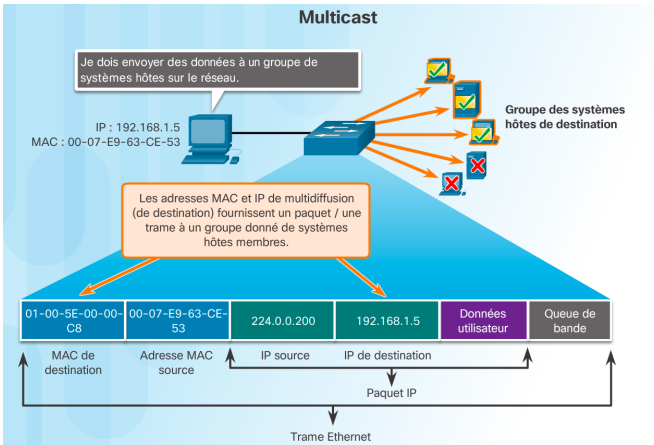
1.5 Adresse MAC de diffusion :



Un paquet de diffusion contient une adresse IPv4 de destination qui ne contient que des uns (1) dans la partie hôte. Cette numérotation implique que tous les hôtes sur le réseau local (domaine de diffusion) recevront le paquet et le traiteront. De nombreux protocoles réseau, tels que DHCP et ARP, utilisent les diffusions.

Sur le schéma précédent, l'hôte source envoie un paquet de diffusion IPv4 à tous les périphériques sur son réseau. L'adresse de destination IPv4 est une adresse de diffusion, 192.168.1.255. Lorsque le paquet de diffusion IPv4 est encapsulé dans la trame Ethernet, l'adresse MAC de destination est l'adresse de diffusion MAC FF-FF-FF-FF-FF-FF au format hexadécimal (48 uns en binaire).

1.6 Adresse MAC de multidiffusion :



Les adresses de multidiffusion permettent à un périphérique source d'envoyer un paquet à un groupe de périphériques. 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. La plage d'adresses de multidiffusion IPv6 commence par FF00::/8. Dans la mesure où les adresses multidiffusion représentent un groupe d'adresses (parfois appelé groupe d'hôtes), elles ne peuvent s'utiliser que dans la destination d'un paquet. La source doit toujours être une adresse de monodiffusion.

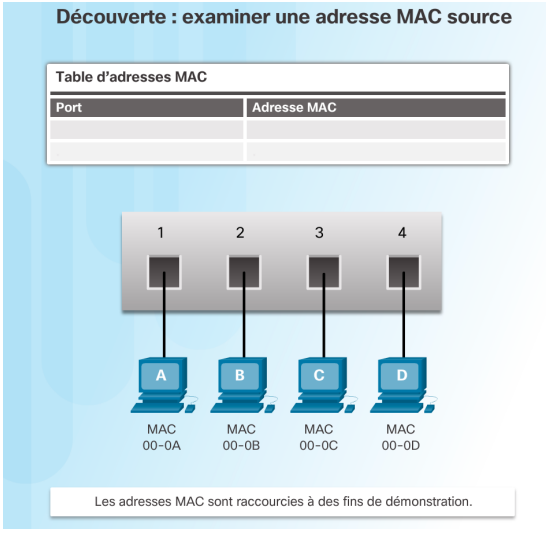
Les adresses de multidiffusion sont notamment utilisées dans les jeux en ligne, où plusieurs joueurs sont connectés à distance au même jeu. L'enseignement à distance par visioconférence fait également appel aux adresses de multidiffusion. Plusieurs étudiants sont ainsi connectés au même cours.

Comme avec les adresses monodiffusion et de diffusion, l'adresse IP multidiffusion nécessite une adresse MAC multidiffusion correspondante pour remettre les trames sur un réseau local. L'adresse MAC de multidiffusion associée à une adresse de multidiffusion IPv4 est une valeur spéciale commençant par 01-00-5E dans un format hexadécimal. L'autre partie de l'adresse MAC de multidiffusion provient de la conversion des 23 bits inférieurs de l'adresse IP du groupe de multidiffusion en 6 caractères hexadécimaux. Pour une adresse IPv6, l'adresse MAC de multidiffusion commence par 33-33.

L'adresse de multidiffusion en hexadécimal 01-00-5E-00-00-C8 représentée dans l'animation en est un exemple. Le dernier octet (ou les huit derniers bits) de l'adresse IP 224.0.0.200 est la valeur décimale 200. Le moyen le plus simple d'obtenir l'équivalent hexadécimal est de convertir d'abord l'adresse en binaire en mettant un espace entre chaque groupe de quatre bits : 200 (décimal) = 1100 1000 (binaire), puis d'utiliser le tableau de conversion binaire/hexadécimal présenté précédemment : 1100 1000 (binaire) = 0xC8.

2. Commutateur LAN:

2.1 Commutateurs : notions essentielles :

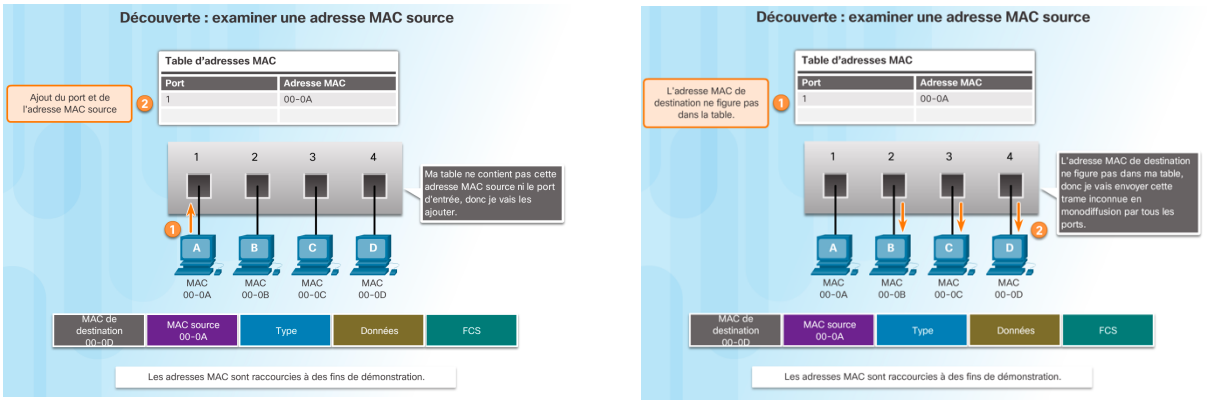


Un commutateur Ethernet de couche 2 utilise des adresses MAC pour prendre des décisions de transmission. Il ignore totalement le protocole transporté dans la partie données de la trame, tel qu'un paquet IPv4. Les décisions du commutateur concernant la transmission de données reposent uniquement sur les adresses MAC Ethernet de couche 2.

Contrairement à un concentrateur Ethernet qui répète les bits sur tous les ports sauf le port entrant, un commutateur Ethernet consulte une table d'adresses MAC pour décider de la transmission de chaque trame. Sur la figure, le commutateur à quatre ports vient d'être mis sous tension. Il n'a pas encore acquis les adresses MAC des quatre PC connectés.

Remarque : la table d'adresses MAC est parfois appelée table de mémoire associative (CAM). Même si le terme de table CAM est également utilisé, nous préfèrerons parler de la table d'adresses MAC dans le cadre de ce cours.

2.2 Acquérir les adresses MAC :



Le commutateur crée la table d'adresses MAC de manière dynamique en examinant l'adresse MAC source des trames reçues sur un port. Pour transmettre les trames, le commutateur recherche une correspondance entre l'adresse MAC de destination qui figure dans la trame et une entrée de la table d'adresses MAC.

Le processus suivant se déroule sur chaque trame Ethernet entrant dans un commutateur.

Découverte - Examen de l'adresse MAC source

Le commutateur vérifie si de nouvelles informations sont disponibles sur chacune des trames entrantes. Pour cela, il examine l'adresse MAC source de la trame et le numéro du port par lequel la trame est entrée dans le commutateur.

- Si l'adresse MAC source n'existe pas, elle est ajoutée à la table , tout comme le numéro du port d'entrée. Sur la figure de gauche, PC-A envoie une trame Ethernet à PC-D. Le commutateur ajoute l'adresse MAC de PC-A à la table.
- Si l'adresse MAC source existe, le commutateur réinitialise le compteur d'obsolescence de cette entrée. Par défaut, la plupart des commutateurs Ethernet conservent les entrées dans la table pendant 5 minutes.

Remarque : si l'adresse MAC source existe dans la table, mais sur un autre port, le commutateur la traite comme une nouvelle entrée. L'ancienne entrée est alors remplacée par la même adresse MAC associée au numéro de port actuel.

Transfert - Examen de l'adresse MAC de destination

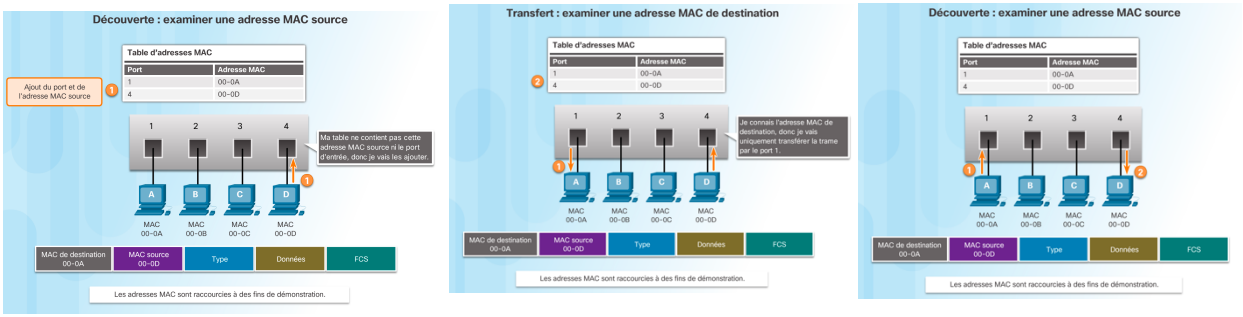
Ensuite, si l'adresse MAC de destination est une adresse de monodiffusion, le commutateur recherche une correspondance entre l'adresse MAC de destination qui figure dans la trame et une entrée de sa table d'adresses MAC.

- Si l'adresse MAC de destination se trouve dans la table, le commutateur transfère la trame par le port spécifié.
- Si l'adresse MAC de destination ne se trouve pas dans la table, le commutateur transfère la trame sur tous les ports sauf celui d'entrée. C'est ce qu'on appelle la monodiffusion inconnue. Comme le montre la figure de droite, la table d'adresses du

commutateur ne contient pas l'adresse MAC de destination de PC-D, donc il envoie la trame sur tous les ports sauf le port 1.

Remarque : si l'adresse MAC de destination est une adresse de diffusion ou de multidiffusion, la trame est également envoyée par tous les ports sauf celui d'entrée.

2.3 Filtrage des trames :

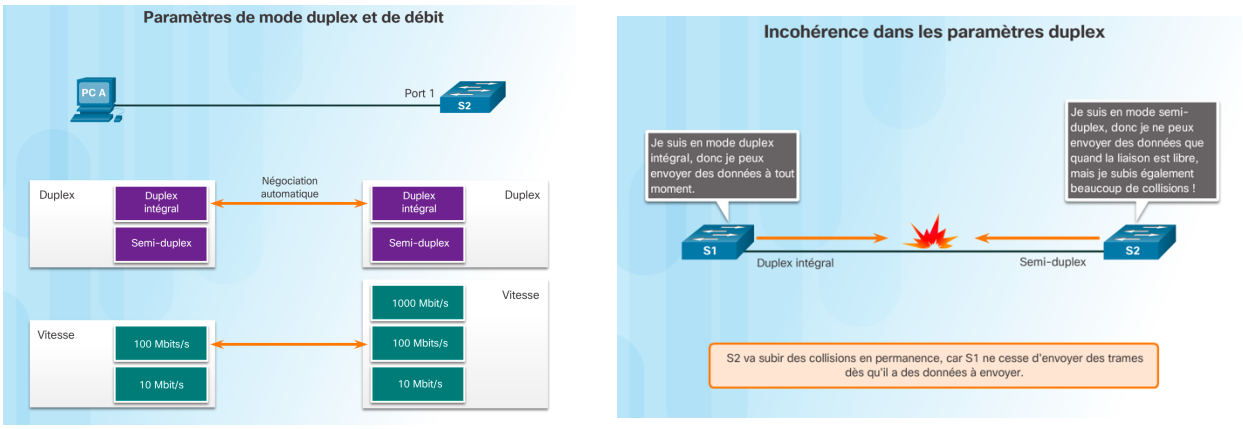


À mesure qu'un commutateur reçoit des trames de différents périphériques, il remplit sa table d'adresses MAC en examinant l'adresse MAC source de chaque trame. Si la table d'adresses MAC du commutateur contient l'adresse MAC de destination, il peut filtrer la trame et la diffuser sur un sol port.

Les figures de gauche et du centre représentent PC-D qui renvoie une trame à PC-A. D'abord, le commutateur acquiert l'adresse MAC de PC-D. Ensuite, comme l'adresse MAC de PC-A figure dans la table du commutateur, il envoie la trame par le port 1 uniquement.

La figure de droite représente PC-A qui envoie une autre trame à PC-D. La table d'adresses MAC contient déjà l'adresse MAC de PC-A, donc le compteur d'obsolescence de cinq minutes pour cette entrée est réinitialisé. Ensuite, comme la table du commutateur contient l'adresse MAC de PC-D, il envoie la trame uniquement par le port 4.

2.4 Paramètres de mode duplex et de débit :



Les paramètres de bande passante et de mode duplex de chaque port de commutateur sont des paramètres fondamentaux. Il est essentiel que ceux du port de commutateur et des périphériques connectés (ordinateur ou autre commutateur) soient en adéquation.

Deux types de paramètres duplex sont employés pour les communications sur les réseaux Ethernet : le mode half-duplex et le mode full-duplex.

- **Mode full-duplex** : les deux extrémités de la connexion peuvent envoyer et recevoir des données simultanément.
- **Mode half-duplex** : une seule extrémité de la connexion peut envoyer des données à la fois.

La négociation automatique est une option proposée sur la plupart des commutateurs Ethernet et des cartes réseau. Elle permet l'échange automatique d'informations sur le débit et le mode duplex entre deux périphériques. Le commutateur et le périphérique connecté choisissent le mode le plus performant. Le mode full-duplex est choisi si les deux périphériques sont compatibles et que la bande passante commune la plus importante est sélectionnée.

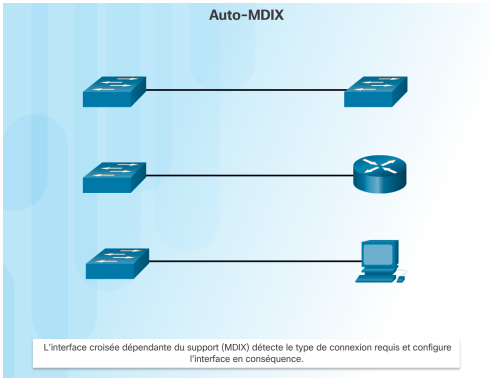
Par exemple, sur la figure de gauche, la carte réseau Ethernet de PC-A peut fonctionner en mode full-duplex ou en mode half-duplex, et à un débit de 10 ou 100 Mbit/s. PC-A est connecté au commutateur S1 sur le port 1 qui peut fonctionner en mode full-duplex ou half-duplex, et à un débit de 10, 100 ou 1 000 Mbit/s (1 Gbit/s). Si les deux périphériques utilisent la négociation automatique, le mode de fonctionnement est full-duplex, avec un débit de 100 Mbit/s.

Remarque : sur la plupart des commutateurs et des cartes réseau Ethernet Cisco, la négociation automatique est définie par défaut pour le débit et le mode duplex. Les ports Gigabit Ethernet fonctionnent uniquement en mode full-duplex.

Incohérence dans les paramètres duplex

L'un des principaux problèmes de performances sur les liaisons Ethernet à 10/100 Mbit/s survient lorsque l'un des ports de la liaison fonctionne en mode semi-duplex alors que l'autre fonctionne en mode duplex intégral, comme illustré sur la figure de droite. Cela se produit lorsque l'un des ports ou les deux ports d'une liaison sont réinitialisés et qu'après le processus de négociation automatique, les deux partenaires de la liaison ne possèdent plus la même configuration. Le problème peut également survenir lorsque des utilisateurs reconfigurent un côté d'une liaison et oublient d'en faire autant de l'autre côté. La négociation automatique doit être soit activée soit désactivée des deux côtés.

2.5 Auto-MDIX :



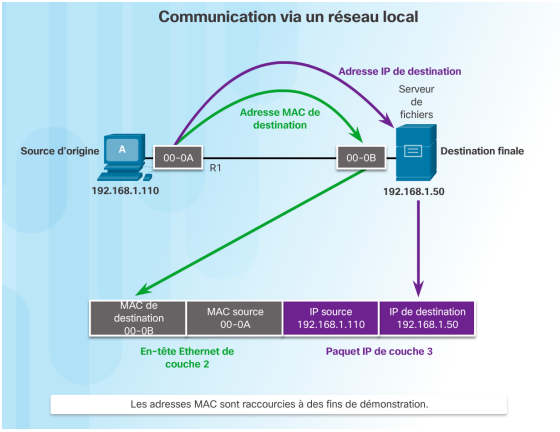
Outre le paramètre duplex approprié, il est également nécessaire que le type de câble adéquat soit défini pour chaque port. Les connexions entre des périphériques spécifiques, notamment entre deux commutateurs, un commutateur et un routeur, un commutateur et un hôte, et un routeur et des périphériques hôtes nécessitaient au départ l'utilisation de types de câble spécifiques (croisés ou droits). Désormais, la plupart des commutateurs prennent en charge la commande de configuration d'interface mdix auto dans l'interface en ligne de commande (CLI), qui active la fonction auto-MDIX.

Lorsque vous activez cette fonction, le commutateur détecte le type de câble connecté au port et configure les interfaces en conséquence. Vous devez donc opter pour un câble croisé ou un câble droit pour les connexions sur un port 10/100/1000 cuivre sur le commutateur, quel que soit le type de périphérique à l'autre extrémité de la connexion.

Remarque : par défaut, la fonction auto-MDIX est activée sur les commutateurs qui exécutent la version 12.2(18)SE (ou ultérieure) du logiciel Cisco IOS.

3. Protocole ARP :

3.1 Destination sur le même réseau :



Chaque périphérique d'un réseau LAN Ethernet possède deux adresses principales :

- **l'adresse physique (adresse MAC)**, qui est utilisée pour les communications entre des cartes réseau d'un même réseau.
- **l'adresse logique (adresse IP)**, qui sert à envoyer le paquet de la source d'origine à la destination finale.

Les adresses IP permettent d'identifier l'adresse de la source initiale et de la destination finale. L'adresse IP de destination peut se trouver sur le même réseau IP que la source ou sur un réseau distant.

Comme les adresses MAC Ethernet, les adresses physiques ou de couche 2 ont une autre finalité. Elles servent à acheminer la trame liaison de données contenant le paquet IP encapsulé d'une carte réseau à une autre sur le même réseau. Si l'adresse IP de destination appartient au même réseau, l'adresse MAC de destination est celle du périphérique de destination.

La figure montre les adresses MAC Ethernet et l'adresse IP permettant à PC-A d'envoyer un paquet IP au serveur de fichiers sur le même réseau.

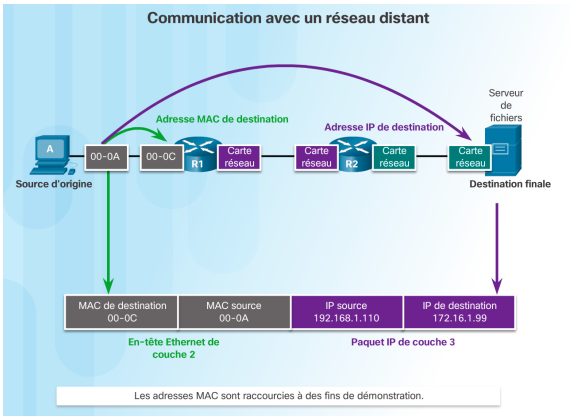
La trame Ethernet de couche 2 contient :

- **l'adresse MAC de destination**, c'est-à-dire l'adresse MAC de la carte réseau Ethernet du serveur de fichiers.
- **l'adresse MAC source**, c'est-à-dire l'adresse MAC de la carte réseau Ethernet de PC-A.

Le paquet IP de couche 3 contient :

- **l'adresse IP source**, c'est-à-dire l'adresse IP de la source d'origine, PC-A.
- **l'adresse IP de destination**, c'est-à-dire l'adresse IP de la destination finale : le serveur de fichiers.

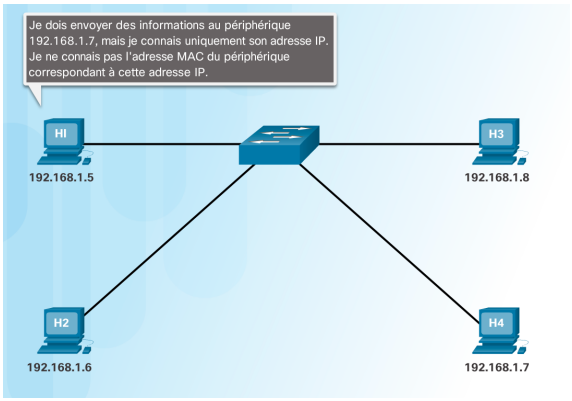
3.2 Destination sur un réseau distant :



Lorsque l'adresse IP de destination appartient à un réseau distant, l'adresse MAC de destination est celle de la passerelle par défaut de l'hôte, c'est-à-dire la carte réseau du routeur, comme le montre la figure. Si l'on fait l'analogie avec la poste, ce processus reviendrait à déposer une lettre au bureau de poste le plus proche. Il suffit d'apporter la lettre au bureau de poste, qui prend alors la responsabilité de l'acheminer jusqu'à sa destination finale.

La figure présente les adresses MAC Ethernet et les adresses IP permettant à PC-A d'envoyer un paquet IP à un serveur Web sur un réseau distant. Les routeurs examinent l'adresse IPv4 de destination afin de déterminer le meilleur chemin pour acheminer le paquet IPv4. Cela équivaut à l'acheminement de la lettre par le service postal en fonction de l'adresse du destinataire.

3.3 Présentation du protocole ARP :



Souvenez-vous que tout périphérique possédant une adresse IP sur un réseau Ethernet possède également une adresse MAC Ethernet. Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient deux adresses :

- **l'adresse MAC de destination**, c'est-à-dire l'adresse MAC de la carte réseau Ethernet qui correspond soit à l'adresse MAC du périphérique de destination finale soit à celle du routeur.
- **l'adresse MAC source**, c'est-à-dire l'adresse MAC de la carte réseau de l'expéditeur.

Pour déterminer l'adresse MAC de destination, le périphérique utilise le protocole ARP. Le protocole ARP assure deux fonctions principales :

- la résolution des adresses IPv4 en adresses MAC ;
- la tenue d'une table des mappages.

3.4 Fonctions du protocole ARP :

Résolution des adresses IPv4 en adresses MAC

Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame Ethernet, le périphérique consulte une table stockée dans sa mémoire pour connaître l'adresse MAC qui est mappée à l'adresse IPv4. Cette table est appelée table ARP ou cache ARP. Le tableau ARP est stocké dans la mémoire vive (RAM) du périphérique.

Le périphérique expéditeur recherche dans sa table ARP une adresse IPv4 de destination et une adresse MAC correspondante.

- Si l'adresse IPv4 de destination du paquet appartient au même réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de destination dans sa table ARP.
- Si l'adresse IPv4 de destination du paquet appartient à un autre réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de la passerelle par défaut dans sa table ARP.

Dans les deux cas, il recherche une adresse IPv4 et l'adresse MAC correspondante du périphérique.

Chaque entrée, ou ligne, de la table ARP relie une adresse IPv4 à une adresse MAC. La relation entre les deux valeurs s'appelle un mappage. Autrement dit, si vous choisissez une adresse IPv4 dans la table, vous trouverez l'adresse MAC correspondante. La table ARP stocke temporairement (dans la mémoire cache) le mappage des périphériques du réseau local.

Si le périphérique localise l'adresse IPv4, l'adresse MAC correspondante est utilisée comme adresse MAC de destination dans la trame. Si l'entrée n'existe pas, le périphérique envoie une requête ARP.

3.5 Requête ARP :

Une requête ARP est envoyée lorsqu'un périphérique a besoin d'une adresse MAC associée à une adresse IPv4 qui ne figure pas dans sa table ARP.

Les messages ARP sont encapsulés directement dans une trame Ethernet. Il n'existe pas d'en-tête IPv4. Le message de la requête ARP contient les éléments suivants :

- **l'adresse IPv4 cible**, c'est-à-dire l'adresse IPv4 dont l'adresse MAC correspondante est requise.
- **l'adresse MAC cible**, qui n'est pas connue et n'est donc pas renseignée dans le message de la requête ARP.

La requête ARP est encapsulée dans une trame Ethernet à l'aide des informations d'en-tête suivantes :

- **l'adresse MAC de destination** - il s'agit d'une adresse de diffusion qui nécessite que toutes les cartes réseau Ethernet sur le LAN acceptent et traitent la requête ARP.
- **l'adresse MAC source**, qui correspond à l'adresse MAC de l'expéditeur de la requête ARP.
- **le type** - les messages ARP ont un champ type de 0x806. Ce type informe la carte réseau réceptrice que la partie données de la trame doit être transmise au processus ARP.

Comme les requêtes ARP sont des diffusions, elles sont envoyées par tous les ports du commutateur sauf le port récepteur. Toutes les cartes réseau Ethernet du LAN traitent les diffusions. Chaque périphérique doit traiter la requête ARP pour voir si l'adresse IPv4 cible correspond à la sienne. Les routeurs ne transmettent pas les diffusions par d'autres interfaces.

Seul un périphérique du réseau local possède l'adresse IPv4 correspondant à l'adresse IPv4 cible de la requête ARP. Aucun des autres périphériques ne répond.

3.6 Réponse ARP :

Seul le périphérique dont l'adresse IPv4 correspond à l'adresse IPv4 cible de la requête ARP envoie une réponse ARP. Le message de réponse ARP contient les éléments suivants :

- **l'adresse IPv4 de l'expéditeur**, c'est-à-dire celle du périphérique dont l'adresse MAC est requise.
- **l'adresse MAC de l'expéditeur**, c'est-à-dire celle requise par l'expéditeur de la requête ARP.

La réponse ARP est encapsulée dans une trame Ethernet à l'aide des informations d'en-tête suivantes :

- **l'adresse MAC de destination**, c'est-à-dire l'adresse MAC de l'expéditeur de la requête ARP.
- **l'adresse MAC source**, c'est-à-dire l'adresse MAC de l'expéditeur de la réponse ARP.
- **le type** - les messages ARP ont un champ type de 0x806. Ce type informe la carte réseau réceptrice que la partie données de la trame doit être transmise au processus ARP.

Seul le périphérique à l'origine de la requête ARP reçoit la réponse ARP en monodiffusion. Il ajoute ensuite l'adresse IPv4 et l'adresse MAC associée à sa table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames à l'aide de l'adresse MAC correspondante.

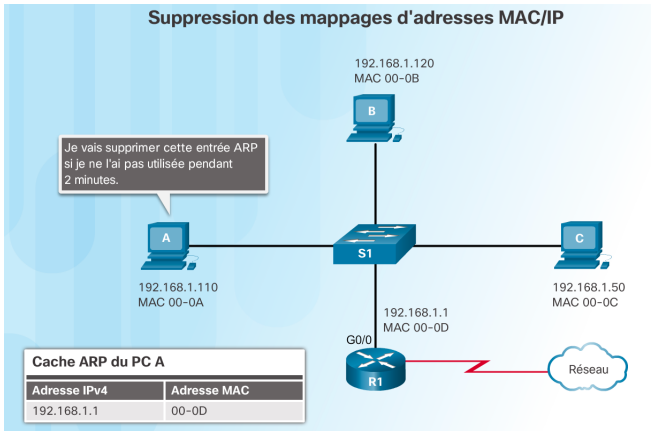
Si aucun périphérique ne répond à la requête ARP, le paquet est abandonné car il est impossible de créer une trame.

Les entrées de la table ARP sont horodatées. Si le périphérique ne reçoit pas de trame d'un périphérique précis avant expiration de l'horodatage, l'entrée correspondant à ce périphérique précis est supprimée du tableau ARP.

Des entrées statiques de mappage peuvent également être ajoutées dans un tableau ARP, mais ceci ne se produit que rarement. Les entrées statiques du tableau ARP n'expirent pas avec le temps et elles doivent être supprimées manuellement.

Remarque : IPv6 utilise un processus similaire au protocole ARP appelé la détection des voisins ICMPv6. De la même manière qu'IPv4 avec les requêtes et les réponses ARP, le protocole IPv6 utilise des messages de sollicitation et d'annonce

3.7 Suppression des entées d'une table ARP :



Pour chaque périphérique, un compteur de cache ARP supprime les entrées ARP qui n'ont pas été utilisées pendant une période donnée. Cette période varie en fonction du système d'exploitation du périphérique. Par exemple, certains systèmes d'exploitation Windows stockent les entrées de cache ARP pendant 2 minutes, comme illustré sur la figure précédente.

Des commandes permettent aussi de supprimer manuellement les entrées du tableau ARP totalement ou partiellement. Lorsqu'une entrée est supprimée, le processus d'envoi d'une requête ARP et de réception d'une réponse ARP doit être répété pour entrer le mappage dans le tableau ARP.

3.8 Tables ARP :

```
Router# show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229     -    0000.0c59.f892  ARPA   Ethernet0/0
Internet  172.16.233.218     -    0000.0c07.ac00  ARPA   Ethernet0/0
Internet  172.16.168.11      -    0000.0c63.1300  ARPA   Ethernet0/0
Internet  172.16.168.254     9    0000.0c36.6965  ARPA   Ethernet0/0
```

Sur un routeur Cisco, la commande **show ip arp** permet d'afficher la table ARP, comme illustré à la figure précédente.

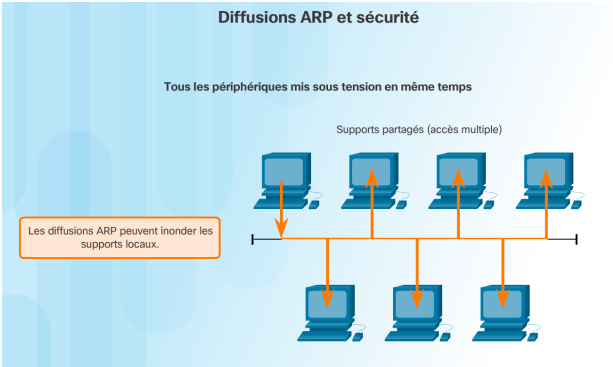
```
C:\> arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254         64-0f-29-0d-36-91     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.82.253.91 --- 0x10
  Internet Address      Physical Address      Type
  10.82.253.92          64-0f-29-0d-36-91     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

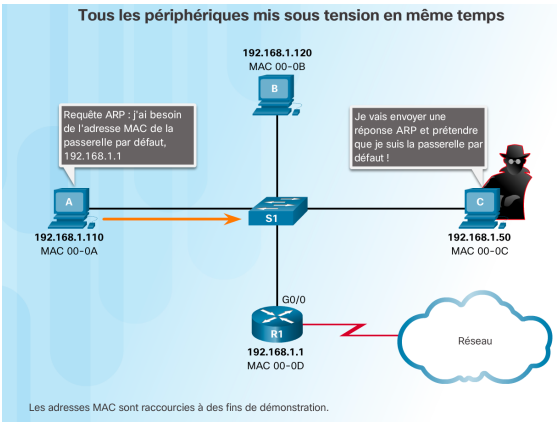
Sur les ordinateurs exécutant Windows 7, c'est la commande **arp –a** qui affiche la table ARP, comme illustré à la figure précédente.

3.9 Diffusion ARP :



Comme les trames de diffusion, les requêtes ARP sont reçues et traitées par chaque périphérique du réseau local. Sur un réseau d'entreprise type, ces diffusions auraient probablement une incidence minime sur les performances du réseau. Toutefois, si un grand nombre de périphériques sont mis sous tension et accèdent aux services du réseau au même moment, les performances du réseau peuvent s'en trouver réduites sur un court laps de temps, comme l'illustre la figure précédente. Si les périphériques envoient les messages de diffusion ARP initiaux et disposent des adresses MAC nécessaires, l'impact sur le réseau sera minime.

3.10 Usurpation ARP :



Dans certains cas, l'utilisation du protocole ARP peut créer un risque de sécurité potentiel appelé usurpation ARP ou empoisonnement ARP. Il s'agit d'une technique utilisée par un pirate pour répondre à une requête ARP concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut, comme l'illustre la figure précédente. Le pirate envoie une réponse ARP avec sa propre adresse MAC. Ainsi, le récepteur de la réponse ARP ajoute la mauvaise adresse MAC à sa table ARP et envoie les paquets au pirate.