

# Protocole ARP (Address Resolution Protocol)

## ARP (Address Resolution Protocol)

Le protocole ARP (Address Resolution Protocol) est un standard TCP/IP obligatoire défini dans la RFC 826, « Address Resolution Protocol (ARP) ». Le protocole ARP résout les adresses IP utilisées par le logiciel exploitant TCP/IP pour les adresses de contrôle d'accès au support utilisées par le matériel du réseau local. Le protocole ARP propose les services de protocole suivants pour des hôtes situés sur le même réseau physique :

- Les adresses de contrôle d'accès au support sont obtenues en utilisant une requête de diffusion de réseau sous forme de question « Quelle est l'adresse MAC du périphérique associé à cette adresse IP ? ».
- Lorsque vous obtenez des résultats pour une requête ARP, l'émetteur de la réponse ARP et le demandeur initial ARP enregistrent leurs adresses IP mutuelles ainsi que l'adresse de contrôle d'accès au support sous forme d'entrée dans une table locale appelée cache ARP pour une future référence.

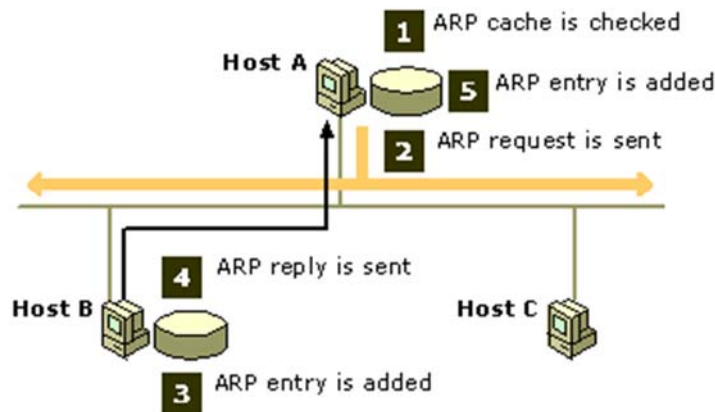
## Adressage de matériel

La création de matériel pour une utilisation sur des réseaux locaux doit contenir une adresse unique programmée dans le périphérique par le fabricant. Pour le matériel de réseau local Ethernet et Token Ring, cette adresse porte le nom d'adresse de contrôle d'accès au support.

Chaque adresse de contrôle d'accès au support identifie le périphérique dans son propre réseau physique avec un nombre à 6 octets programmé dans la mémoire morte (ROM) de chaque périphérique matériel physique, comme une carte réseau. Les adresses de contrôle d'accès au support sont généralement affichées en format hexadécimal (par exemple, 00-AA-00-3F-89-4A). L'autorité et l'inscription des adresses de contrôle d'accès au support sont réglementées par l'IEEE (Institute of Electrical and Electronics Engineers). Généralement, l'IEEE enregistre et affecte des nombres uniques pour les trois premiers octets de l'adresse de contrôle d'accès au support à chaque fabricant. Chaque fabricant peut ensuite affecter les trois derniers octets de l'adresse de contrôle d'accès au support à chaque carte réseau.

# Comment ARP résout les adresses de contrôle d'accès au support pour un trafic local

L'illustration suivante explique comment ARP résout les adresses IP en adresses matérielles pour des hôtes de même réseau local.



Dans cet exemple, deux hôtes TCP/IP, les Hôtes A et B, sont tous les deux situés sur le même réseau physique. L'Hôte A est affecté de l'adresse IP 10.0.0.99 et l'Hôte B est affecté de l'adresse IP 10.0.0.100.

Lorsque l'Hôte A tente de communiquer avec l'Hôte B, les étapes suivantes permettent de résoudre l'adresse affectée au logiciel de l'Hôte B (10.0.0.100) en adresse de contrôle d'accès au support affectée au matériel de l'Hôte B :

1. Suivant le contenu de la table de routage de l'Hôte A, IP détermine que l'adresse IP de transmission à utiliser pour atteindre l'Hôte B est 10.0.0.100. L'Hôte A contrôle ensuite son propre cache ARP local pour une adresse matérielle correspondante pour l'Hôte B.
2. Si l'Hôte A ne trouve aucun mappage dans le cache, il diffuse une trame de requête ARP vers tous les hôtes du réseau local avec la question « Quelle est l'adresse matérielle de 10.0.0.100 ? ». Les adresses matérielle et logicielle de la source, Hôte A, sont intégrées dans la requête ARP.

Chaque hôte du réseau local reçoit la requête ARP et recherche une correspondance avec sa propre adresse IP. Si un hôte ne trouve pas de correspondance, il ignore la requête ARP.

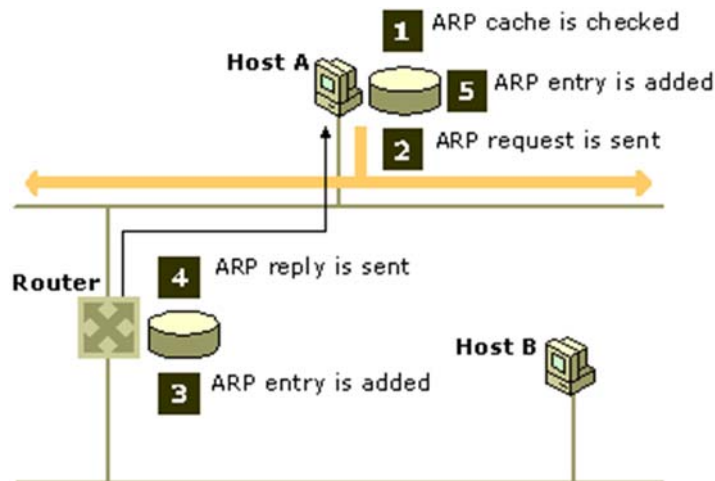
3. L'Hôte B indique que l'adresse IP de la requête ARP correspond à sa propre adresse IP et ajoute un mappage d'adresse matérielle/logicielle pour l'Hôte A à son propre cache local ARP.
4. L'Hôte B renvoie directement à l'Hôte A un message de réponse ARP contenant son adresse matérielle.
5. Lorsque l'Hôte A reçoit le message de réponse ARP de l'Hôte B, il met à jour son cache ARP à l'aide d'un mappage d'adresse matérielle/logicielle pour l'Hôte B.

Une fois que l'adresse de contrôle d'accès au support pour l'Hôte B a été déterminée, l'Hôte A peut envoyer un trafic IP à l'Hôte B en l'adressant à l'adresse de contrôle d'accès au support de l'Hôte B.

## Comment ARP résout les adresses de contrôle d'accès au support pour un trafic distant

ARP est également utilisé pour transmettre des datagrammes IP aux routeurs locaux pour des destinations qui ne se trouvent pas sur le réseau local. Dans ce cas, ARP résout l'adresse de contrôle d'accès au support d'une interface de routeur sur le réseau local.

L'illustration suivante explique comment ARP résout les adresses IP en adresses matérielles pour deux hôtes de réseaux physiques différents connectés par un routeur commun.



Dans cet exemple, l'Hôte A est affecté d'une adresse IP 10.0.0.99 et l'Hôte B utilise une adresse IP 192.168.0.99. L'interface de routeur 1 se trouve sur le même réseau physique que l'Hôte A et utilise l'adresse IP 10.0.0.1. L'Interface de routeur 2 se trouve sur le même réseau physique que l'Hôte B et utilise l'adresse IP 192.168.0.1.

Lorsque l'Hôte A tente de communiquer avec l'Hôte B, les étapes suivantes permettent de résoudre l'adresse affectée au logiciel de l'Interface de routeur 1 (10.0.0.1) en son adresse de contrôle d'accès au support affectée au matériel :

1. Suivant le contenu de la table de routage de l'Hôte A, IP détermine que l'adresse IP de transmission à utiliser pour atteindre l'Hôte B est 10.0.0.1, adresse de sa passerelle par défaut. L'Hôte A contrôle ensuite son propre cache ARP local pour une adresse matérielle correspondante pour 10.0.0.1.
2. Si l'Hôte A ne trouve aucun mappage dans le cache, il diffuse une trame de requête ARP vers tous les hôtes du réseau local avec la question « Quelle est l'adresse matérielle de 10.0.0.1 ? ». Les adresses matérielle et logicielle de la source, Hôte A, sont intégrées dans la requête ARP.

Chaque hôte du réseau local reçoit la requête ARP et recherche une correspondance avec sa propre adresse IP. Si un hôte ne trouve pas de correspondance, il ignore la requête ARP.

3. Le routeur indique que l'adresse IP de la requête ARP correspond à sa propre adresse IP et ajoute un mappage d'adresse matérielle/logicielle pour l'Hôte A à son propre cache local ARP.
4. Le routeur renvoie directement à l'Hôte A un message de réponse ARP contenant son adresse matérielle.
5. Lorsque l'Hôte A reçoit le message de réponse ARP du routeur, il met à jour son cache ARP à l'aide d'un mappage d'adresse matérielle/logicielle pour 10.0.0.1.

Une fois que l'adresse de contrôle d'accès au support pour l'Interface de réseau 1 a été déterminée, l'Hôte A peut envoyer un trafic IP à l'Interface de réseau 1 en l'adressant à l'adresse de contrôle d'accès au support de l'Interface de réseau 1. Le routeur transfère ensuite le trafic vers l'Hôte B à l'aide du même processus ARP, tel que décrit dans cette section.

## Cache ARP

Pour réduire le nombre de diffusions, ARP conserve un cache de mappages d'adresses de contrôle d'accès adresse IP-support pour pouvoir l'utiliser ultérieurement. Le cache ARP peut contenir des entrées dynamiques et statiques. Les entrées dynamiques sont ajoutées et supprimées automatiquement dans le temps. Elles sont conservées dans le cache jusqu'au redémarrage de l'ordinateur.

Chaque entrée de cache dynamique ARP possède une durée de vie potentielle de 10 minutes. Les nouvelles entrées ajoutées au cache sont horodatées. Si une entrée n'est pas réutilisée dans les 2 minutes qui suivent leur ajout, elle expire et est supprimée du cache ARP. Si une entrée est utilisée, il lui est accordé au moins deux minutes de durée de vie. Si une entrée est toujours en cours d'utilisation, il lui est accordé une durée de vie supplémentaire allant de deux minutes jusqu'à un maximum de 10 minutes. Vous pouvez consulter le cache ARP à l'aide de la commande **arp**. Pour afficher le cache ARP, tapez **arp -a** à l'invite de commandes. Pour afficher les options de la ligne de commande **arp**, tapez **arp /?** à l'invite de commandes.

## Remarque

Il existe un cache ARP individuel pour chaque carte réseau.

(Source : <http://msdn.microsoft.com> – Mise à jour octobre 2017)