Comprendre le proxy ARP

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés
- Conventions

Informations générales

Fonctionnement du proxy ARP

- Diagramme du réseau

Avantages du proxy ARP

Inconvénients du proxy ARP

Informations connexes

Introduction

Ce document décrit comment le protocole ARP (Proxy Address Resolution Protocol) aide les hôtes à atteindre des sous-réseaux distants sans routes d'hôte ou passerelle par défaut.

Conditions préalables

Exigences

Ce document nécessite une connaissance des environnements ARP et Ethernet.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS® version 12.2(10b)
- Routeurs Cisco, série 2600

Remarque : Le comportement décrit dans ce document ne se limite pas à ces composants. Le proxy ARP est disponible sur plusieurs plates-formes Cisco IOS et Cisco IOS XE. La disponibilité des fonctionnalités, le comportement par défaut et la prise en charge des commandes peuvent varier selon la plate-forme et la version du logiciel.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le proxy ARP est la technique par laquelle un hôte, généralement un routeur, répond aux requêtes ARP destinées à une autre machine. Le routeur répond avec sa propre adresse MAC et achemine les paquets vers la destination réelle. Le proxy ARP peut aider les ordinateurs d'un sous-réseau à atteindre des sous-réseaux distants sans avoir à configurer le routage ou une passerelle par défaut. Le proxy ARP est défini dans la RFC 1027.

Fonctionnement du proxy ARP

Voici un exemple du fonctionnement du protocole Proxy ARP :

Diagramme du réseau

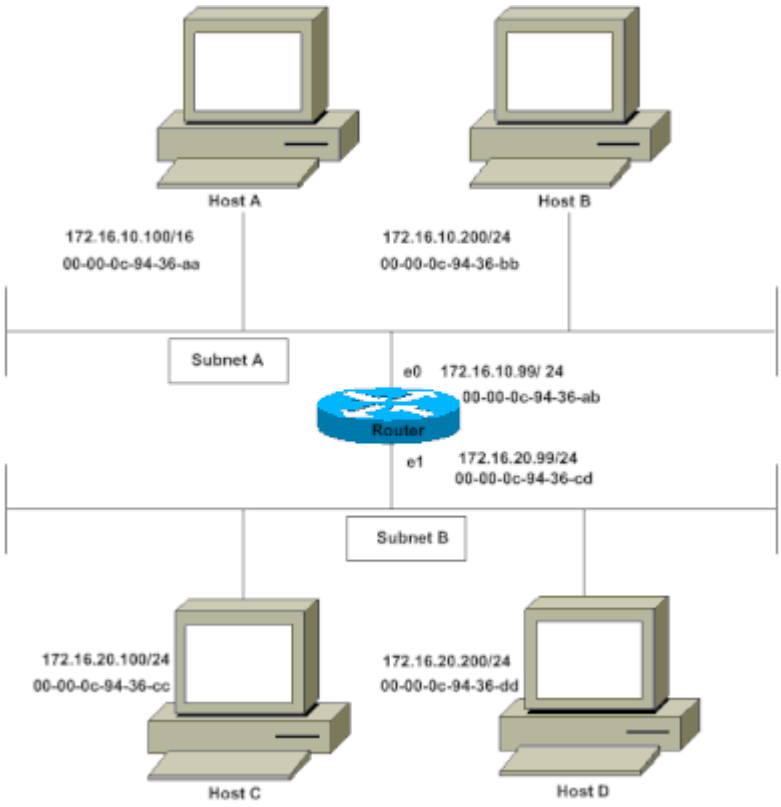


Diagramme du réseau

L'hôte A (172.16.10.100) sur le sous-réseau A doit envoyer des paquets à l'hôte D (172.16.20.200) sur le sous-réseau B. Comme l'illustre le schéma du réseau, l'hôte A possède un masque de sous-réseau /16. Cela signifie que l'hôte A croit être directement connecté à l'ensemble du réseau 172.16.0.0. Lorsque l'hôte A doit communiquer avec un périphérique qu'il croit être directement connecté, il envoie une requête ARP à la destination. Par conséquent, lorsque l'hôte A doit envoyer un paquet à l'hôte D, l'hôte A croit que l'hôte D est directement connecté et envoie donc une requête ARP à l'hôte D.

Pour atteindre l'hôte D (172.16.20.200), l'hôte A demande l'adresse MAC associée à l'adresse IP de destination.

Par conséquent, l'hôte A diffuse une requête ARP sur le sous-réseau A, comme indiqué :

Adresse MAC de l'expéditeur	Adresse IP de l'expéditeur	Adresse MAC cible	Adresse IP cible
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

Dans cette requête ARP, l'hôte A (172.16.10.100) demande à l'hôte D (172.16.20.200) d'envoyer son adresse MAC. Le paquet de requête ARP est ensuite encapsulé dans une trame Ethernet avec l'adresse MAC de l'hôte A comme adresse source et une adresse de diffusion (FFFF.FFFF.FFFF) comme adresse de destination. Comme la requête ARP est une diffusion, elle atteint tous les noeuds du sous-réseau A, qui inclut l'interface Ethernet 0 (e0) du routeur, mais n'atteint pas l'hôte D. La diffusion n'atteint pas l'hôte D parce que les routeurs, par défaut, ne transfèrent pas les trames de diffusion de couche 2 entre les interfaces.

Comme le proxy ARP est activé sur l’interface de réception et que le routeur dispose d’une route vers l’hôte D (172.16.20.200) via une autre interface, le routeur répond à l’hôte A avec sa propre adresse MAC.

Adresse MAC de l'expéditeur	Adresse IP de l'expéditeur	Adresse MAC cible	Adresse IP cible
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Il s’agit de la réponse ARP proxy que le routeur envoie à l’hôte A. Le paquet de réponse ARP proxy est encapsulé dans une trame Ethernet avec l’adresse MAC du routeur comme adresse source et l’adresse MAC de l’hôte A comme adresse de destination. La réponse ARP proxy dans cet échange est monodiffusion vers le demandeur d'origine. À la réception de cette réponse ARP, l’hôte A met à jour sa table ARP, comme indiqué :

Adresse IP	Adresse MAC :
172.16.20.200	00-00-0c-94-36-ab

Jusqu’à ce que l’entrée ARP expire ou soit modifiée, l’hôte A envoie des paquets pour 172.16.20.200 (hôte D) à l’adresse MAC 00-00-0c-94-36-ab, qui appartient au routeur. Comme le routeur sait comment atteindre l’hôte D, il transfère le paquet à l’hôte D. Le cache ARP d’un hôte sur le sous-réseau A contient l’adresse MAC du routeur pour chaque destination distante pour laquelle le routeur fournit une réponse ARP proxy. Par conséquent, tous les paquets destinés au sous-réseau B sont envoyés au routeur. Le routeur transfère ces paquets aux hôtes du sous-réseau B.

Le cache ARP de l’hôte A est indiqué dans ce tableau :

Adresse IP	Adresse MAC :
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb



Remarque : Plusieurs adresses IP sont mappées à une seule adresse MAC, qui est l'adresse MAC de ce routeur. Dans cette topologie, ce modèle peut indiquer que le proxy ARP est utilisé.

Le proxy ARP doit être activé sur une interface de routeur Cisco pour que le routeur puisse répondre au nom des destinations distantes. Sur Cisco IOS, Proxy ARP est activé par défaut sur les interfaces compatibles ARP. Avant de désactiver le protocole ARP proxy, assurez-vous que les hôtes concernés disposent d'une route valide ou d'une passerelle par défaut. Sur une interface où Proxy ARP n'est pas requis, désactivez-le avec no ip proxy-arp :

<#root>

```
Router#
```

```
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#

interface ethernet 0

Router(config-if)#

no ip proxy-arp

Router(config-if)#

^Z

Router#
```

Afin d'activer le proxy ARP sur une interface, exécutez la commande de configuration d'interface ip proxy-arp. Exécutez show ip interface <interface> afin de vérifier que le résultat indique que le proxy ARP a été activé.



Remarque : Lorsque l'hôte B (172.16.10.200/24) sur le sous-réseau A tente d'envoyer des paquets à l'hôte D (172.16.20.200) sur le sous-réseau B, il vérifie sa table de routage IP. L'hôte B n'envoie pas de requête ARP pour l'hôte D, car la destination se trouve en dehors du sous-réseau configuré sur l'interface Ethernet de l'hôte B. L'hôte B envoie le paquet à un tronçon suivant configuré. Sans route ou passerelle par défaut correspondante, la communication échoue.

Avantages du proxy ARP

Le principal avantage du protocole ARP proxy est qu'il peut être activé sur un seul routeur sur un réseau et ne modifie pas les tables de routage des autres routeurs du réseau.

Le proxy ARP peut être utilisé sur un réseau où les hôtes IP n'ont pas de passerelle par défaut ou de route vers la destination distante.

Inconvénients du proxy ARP

Les hôtes n’ont pas de visibilité sur la topologie physique du réseau et traitent le réseau comme un segment plat où une requête ARP peut résoudre n’importe quelle adresse de destination.

Le comportement du proxy ARP présente plusieurs inconvénients :

- Elle augmente le volume du trafic ARP sur votre segment.
- Les hôtes ont besoin de tables ARP plus volumineuses pour gérer les mappages d’adresses IP vers MAC.
- La sécurité peut être compromise. Une machine peut prétendre en être une autre afin d'intercepter des paquets, un acte appelé mystification.
- Elle ne fonctionne pas pour les réseaux qui n’utilisent pas le protocole ARP pour la résolution d’adresses.
- Il peut produire une sélection de tronçon suivant imprévisible lorsque plusieurs routeurs fournissent des réponses ARP proxy pour la même destination.

Informations connexes

- Ressources de support IP
- Page de support NAT
- Outils et ressources
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.