ARP Proxy

Contenu

Introduction

Ce document explique le concept du Protocole de résolution d'adresse (ARP) de proxy. Le proxy ARP est la technique par laquelle un hôte, habituellement un routeur, répond à des requêtes ARP destinées à une autre machine. En « truquant » son identité, le routeur accepte la responsabilité du routage de paquets vers la destination « réelle ». Le proxy ARP peut aider des machines sur un sous-réseau à atteindre des sous-réseaux sans devoir configurer un routage ou une passerelle par défaut. Le proxy ARP est défini dans RFC 1027 .

Conditions préalables

Conditions requises

Ce document implique de comprendre l'ARP et l'environnement Ethernet.

Composants utilisés

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

- Cisco IOS® Version du logiciel 12.2(10b)
- Routeurs de la gamme Cisco 2500

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

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

Comment le proxy ARP fonctionne-t-il ?

Ceci est un exemple de la façon dont le proxy ARP fonctionne :

Diagramme du réseau

L'hôte A (172.16.10.100) sur le sous-réseau A doit envoyer des paquets pour héberger D (172.16.20.200) sur le sous-réseau B. suivant les indications du diagramme, hébergent A a un masque de sous-réseau de /16. Cela signifie que l'hôte A croit qu'il est directement connecté à tout le réseau 172 16 0 0. Quand un hôte A a besoin de communiquer avec tout périphérique qu'il croit directement connecté, il envoie une requête ARP à la destination. Par conséquent, quand l'hôte A a besoin d'envoyer un paquet à l'hôte D, l'hôte A croit que l'hôte D est directement connecté, ainsi il envoie une requête ARP à l'hôte D.

Afin d'atteindre l'hôte D (172.16.20.200), l'hôte A a besoin de l'adresse MAC de l'hôte D.

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+F10534
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 que l'hôte D envoie (de 172.16.20.200) son adresse MAC. Le paquet de requête ARP est alors encapsulé dans une trame Ethernet avec l'adresse MAC de l'hôte A en tant qu'adresse source et diffusion (FFFF.FFFF.FFFF) comme adresse de destination. Puisque la requête ARP est une diffusion, elle atteint tous les noeuds dans le sous-réseau A, qui inclut l'interface e0 du routeur, mais n'atteint pas l'hôte D. La diffusion n'atteint pas l'hôte D parce que les routeurs, par défaut, Button, ne transfèrent pas des diffusions.

Puisque le routeur sait que l'adresse de destination (172.16.20.200) est sur un autre sous-réseau et peut atteindre l'hôte D, il répond avec sa propre adresse MAC à l'hôte A.

Adresse MAC de l'expéditeur	Adresse IP de l'expéditeur	Adresse MAC cible	Adresse IP cible+F10534
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

C'est la réponse du proxy ARP que le routeur envoie à l'hôte A. Le paquet de réponse ARP du proxy est encapsulé dans une trame Ethernet avec l'adresse MAC du routeur en tant qu'adresse source et l'adresse MAC de l'hôte A en tant qu'adresse de destination. Les réponses ARP sont toujours monodiffusées au demandeur initial.

Dès 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

Dorénavant, l'hôte A renvoie tous les paquets qu'il veut pour accéder à 172.16.20.200 (hôte D) à l'adresse MAC 00-00-0c-94-36-ab (routeur). Puisque le routeur sait comment atteindre l'hôte D, le routeur transfère le paquet à l'hôte D. Le cache d'ARP sur les hôtes dans le sous-réseau A est rempli avec l'adresse MAC du routeur pour tous les hôtes sur le sous-réseau B. Hence, tous les paquets destinés au sous-réseau B sont envoyés au routeur. Le routeur transfère ces paquets aux hôtes dans le sous-réseau B.

Le cache ARP de l'hôte A est indiqué dans cette table :

Adresse IP	Adresse MAC
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.99	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb

Remarque: Des adresses IP multiples sont tracées vers une adresse MAC simple, l'adresse MAC de ce routeur, qui indique que le proxy ARP est en service.

L'interface de Cisco doit être configurée pour accepter et répondre au proxy ARP. Ceci est activé par défaut. La commande **no ip proxy-arp** doit être configurée sur l'interface du routeur connectée au routeur de l'ISP. Le proxy ARP peut être désactivé sur chaque interface individuellement avec la commande de configuration d'interface **no ip proxy-arp**, comme indiqué :

```
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, lancez la commande **ip proxy-arp interface configuration**.

Remarque: Quand l'hôte B (172.16.10.200/24) sur le sous-réseau A essaie d'envoyer des paquets à l'hôte D destinataire (172.16.20.200) sur le sous-réseau B, il regarde dans la table de routage IP et conduit le paquet en conséquence. L'hôte B (172.16.10.200/24) ne fait pas ARP pour l'adresse IP de l'hôte D 172.16.20.200 parce qu'il appartient à un sous-réseau différent de ce qui est configuré sur l'interface Ethernet 172.16.20.200/24 de l'hôte B.

Avantages du proxy ARP

L'avantage principal du proxy ARP est qu'il peut être ajouté à un seul routeur sur un réseau et n'affecte pas les tables de routage des autres routeurs sur le réseau.

Le proxy ARP doit être utilisé sur le réseau où les hôtes IP ne sont pas configurés avec une passerelle par défaut ou n'ont pas d'intelligence de routage.

Inconvénients de proxy ARP

Les serveurs n'ont aucune idée des détails physiques de leur réseau et l'assument en tant que réseau non hiérarchique dans lequel ils peuvent atteindre n'importe quelle destination simplement en envoyant une requête ARP. Mais utiliser ARP pour tout a des inconvénients. Voici certains des inconvénients :

- Cela augmente la quantité du trafic ARP sur votre segment.
- Les hôtes ont besoin de plus grandes tables ARP afin de traiter des tracés d'adresse IP-vers-MAC.
- Cela peut nuire à la sécurité. Une machine peut prétendre être une autre afin d'intercepter des paquets, acte appelé « spoofing ».
- Cela ne fonctionne pas pour les réseaux qui n'utilisent pas ARP pour la résolution d'adresse.
- Il ne se généralise pas à toutes les topologies du réseau. Par exemple, plus qu'un routeur qui se connecte à deux réseaux physiques.

Reportez-vous à la section Activation d'un Proxy ARP de Configuration d'un adressage IP pour plus d'informations sur la configuration d'un proxy ARP.

Informations connexes

- Ressources de support IP
- Page de support NAT
- Outils et ressources
- Support technique - Cisco Systems