Cisco – Proxy ARP

Table of Contents

Proxy ARP

Introduction

This document explains the concept of proxy Address Resolution Protocol (ARP). Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP can help machines on a subnet reach remote subnets without configuring routing or a default gateway.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

This document requires an understanding of the ARP and Ethernet environment.

Components Used

The information in this document is based on the software and hardware versions below.

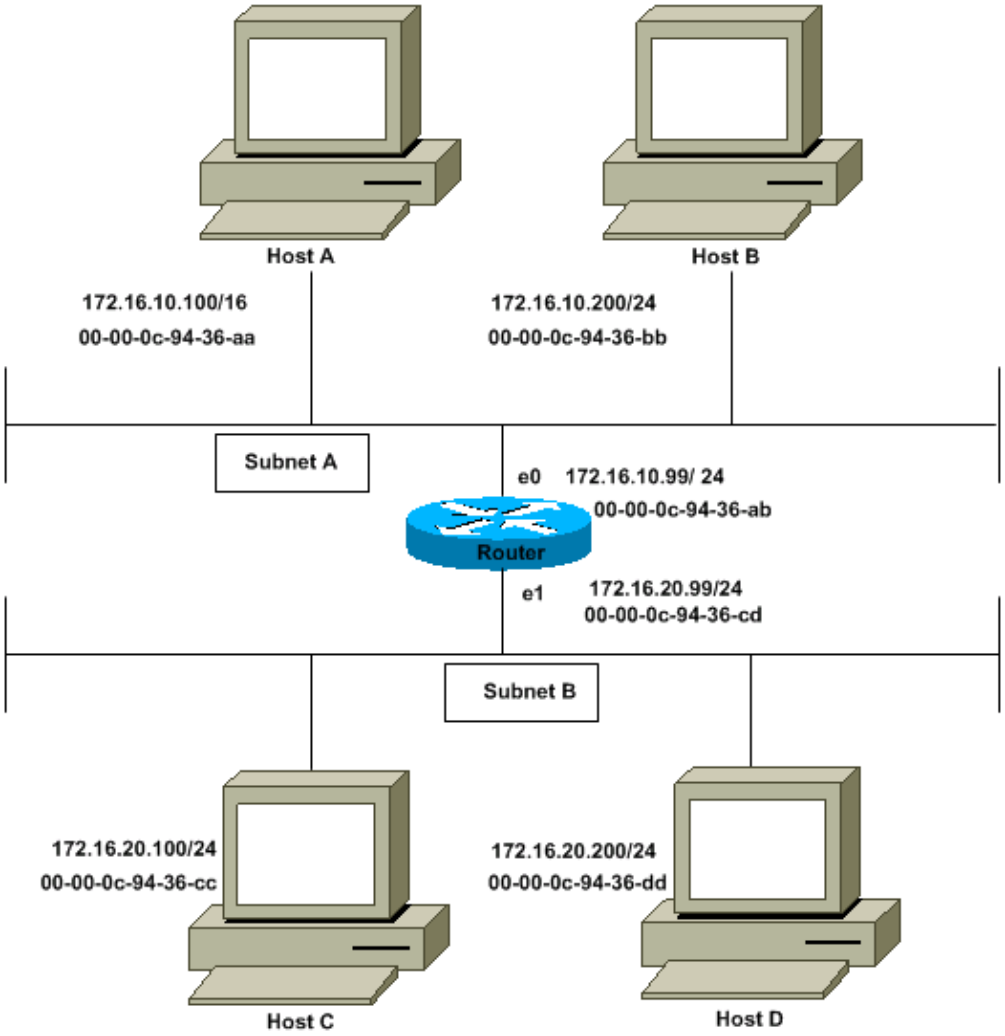
- Cisco IOS® Software Release 12.2(10b)
- Cisco 2500 Series Routers

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

How Does Proxy ARP Work?

Below is an example of how proxy ARP works:

Network Diagram



The Host A (172.16.10.100) on Subnet A needs to send packets to Host D (172.16.20.200) on Subnet B. As shown in the diagram above, Host A has a /16 subnet mask. What this means is that Host A believes that it is directly connected to all of network 172.16.0.0. When Host A needs to communicate with any devices it believes are directly connected, it will send an ARP request to the destination. Therefore, when Host A needs to send a packet to Host D, Host A believes that Host D is directly connected, so it sends an ARP request to Host D.

To reach Host D (172.16.20.200), Host A needs the MAC address of Host D.

Therefore, Host A broadcasts an ARP request on Subnet A, as below:

Sender's MAC Address	Sender's IP Address	Target MAC Address	Target IP Address
00−00−0c−94−36−aa	172.16.10.100	00−00−00−00−00−00	172.16.20.200

In above ARP request, Host A (172.16.10.100) is requesting that Host D (172.16.20.200) send its MAC address. The above ARP request packet is then encapsulated in an Ethernet frame with Host A's MAC address as the source address and a broadcast (FFFF.FFFF.FFFF) as the destination address. Since the ARP request is a broadcast, it reaches all the nodes in the Subnet A, including the router's e0 interface, but does not reach Host D. The broadcast will not reach Host D because routers, by default, do not forward broadcasts.

Since the router knows that the target address (172.16.20.200) is on another subnet and can reach Host D, it will reply with its own MAC address to Host A.

Sender's MAC Address	Sender's IP Address	Target MAC Address	Target IP Address
00−00−0c−94−36−ab	172.16.20.200	00−00−0c−94−36−aa	172.16.10.100

Above is the Proxy ARP reply that the router sends to Host A. The proxy ARP reply packet is encapsulated in an Ethernet frame with router's MAC address as the source address and Host A's MAC address as the destination address. The ARP replies are always unicast to the original requester.

On receiving this ARP reply, Host A updates its ARP table as below:

IP Address	MAC Address
172.16.20.200	00−00−0c−94−36−ab

From now on Host A will forward all the packets that it wants to reach 172.16.20.200 (Host D) to the MAC address 00−00−0c−94−36−ab (router). Since the router knows how to reach Host D, the router forwards the packet to Host D. The ARP cache on the hosts in Subnet A is populated with the MAC address of the router for all the hosts on the Subnet B. Hence all packets destined to Subnet B are sent to the router. The router forwards those packets to the hosts in Subnet B.

The ARP cache of Host A is given below:

IP Address	MAC Address
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

Note: Multiple IP addresses are mapped to a single MAC address (the router's MAC address), indicating that proxy ARP is in use.

The Cisco router's interface should be configured to accept and respond to proxy ARP. This is enabled by default. Proxy ARP can be disabled on a per interface basis with the interface configuration command **no ip proxy−arp**, as shown below:

```
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#
```

To enable proxy ARP on an interface, use the **ip proxy−arp** interface configuration command.

Advantages of Proxy ARP

The main advantage of using proxy ARP is that it can be added to a single router on a network without disturbing the routing tables of the other routers on the network.

Proxy ARP should be used on the network where IP hosts are not configured with default gateway or does not have any routing intelligence.

Disadvantages of Proxy ARP

Hosts have no idea of the physical details of their network and assume it to be a flat network in which they can reach any destination simply by sending an ARP request. But using ARP for everything has disadvantages, some of which are listed below:

- It increases the amount of ARP traffic on your segment.
- Hosts need larger ARP tables to handle IP−to−MAC address mappings.
- Security may be undermined. A machine can claim to be another in order to intercept packets, an act called "spoofing."
- It does not work for networks that do not use ARP for address resolution.
- It does not generalize to all network topologies (for example, more than one router connecting two physical networks).

For more information about configuring proxy ARP, refer to Configuring IP Addressing.

Related Information

- **TCP/IP Routing and Routed Protocols Support Page**
- **Tools and Utilities**
- **Technical Support−Cisco Systems**