Proxy ARP

Document ID: 13718

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 the need to configure routing or a default gateway. Proxy ARP is defined in RFC 1027 .

Prerequisites

Requirements

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

Components Used

The information in this document is based on these software and hardware versions:

- 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.

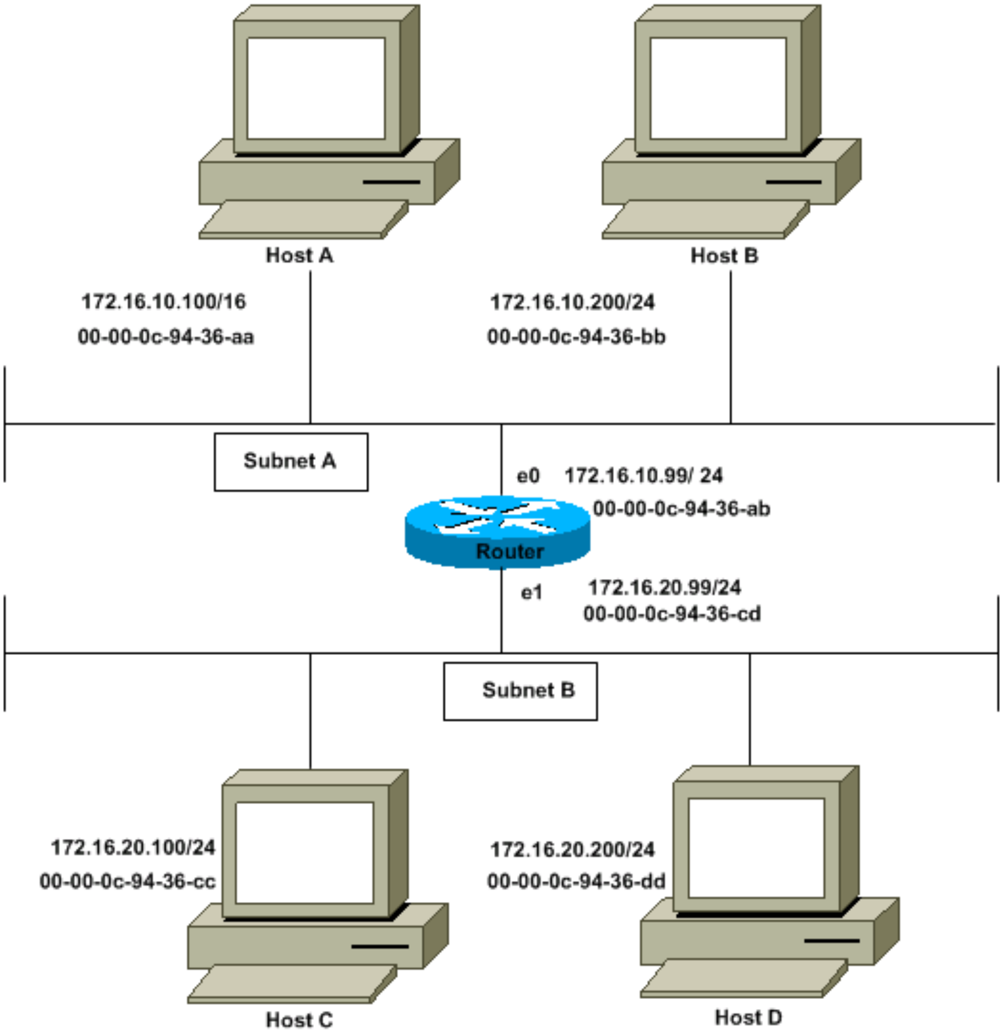
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

How Does Proxy ARP Work?

This 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, 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 sends 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.

In order 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 shown:

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 this ARP request, Host A (172.16.10.100) requests that Host D (172.16.20.200) send its MAC address. The ARP request packet is then encapsulated in an Ethernet frame with the MAC address of Host A 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, which includes the e0 interface of the router, but does not reach Host D. The broadcast does 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 replies 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

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

Upon receipt of this ARP reply, Host A updates its ARP table, as shown:

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

From now on, Host A forwards 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 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 shown in this table:

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 MAC address of this router, which indicates that proxy ARP is in use.

The interface of the Cisco must be configured to accept and respond to proxy ARP. This is enabled by default. The **no ip proxy−arp** command must be configured on the interface of the router connected to the ISP router. Proxy ARP can be disabled on each interface individually with the interface configuration command **no ip proxy−arp**, as shown:

```
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#
```

In order to enable proxy ARP on an interface, issue the **ip proxy−arp** interface configuration command.

Note: When Host B (172.16.10.200/24) on Subnet A tries to send packets to destination Host D (172.16.20.200) on Subnet B, it looks into its IP routing table and routes the packet accordingly. Host B (172.16.10.200/24) does not ARP for Host D IP address 172.16.20.200 because it belongs to a different subnet than what is configured on Host B ethernet interface 172.16.20.200/24.

Advantages of Proxy ARP

The main advantage of proxy ARP is that it can be added to a single router on a network and does not disturb the routing tables of the other routers on the network.

Proxy ARP must be used on the network where IP hosts are not configured with a default gateway or do 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. These are some of the disadvantages:

- It increases the amount of ARP traffic on your segment.
- Hosts need larger ARP tables in order to handle IP−to−MAC address mappings.
- Security can 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 that connects two physical networks.

Refer to the Enabling Proxy ARP section of Configuring IP Addressing for more information about configuring proxy ARP.

Related Information

- **IP Support Resources**
- **NAT Support Page**
- **Tools & Resources**
- **Technical Support − Cisco Systems**

Updated: Jan 28, 2008 Document ID: 13718