Understand Proxy ARP

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Background Information

How Proxy ARP Works

- Network Diagram

Advantages of Proxy ARP

Disadvantages of Proxy ARP

Related Information

Introduction

This document describes how Proxy Address Resolution Protocol (ARP) helps hosts reach remote subnets without host routes or a default gateway.

Prerequisites

Requirements

This document requires knowledge of ARP and Ethernet environments.

Components Used

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

- Cisco IOS® Software Release 12.2(10b)
- Cisco 2600 Series Routers

Note: The behavior described in this document is not limited to these components. Proxy ARP is

---

available on multiple Cisco IOS and Cisco IOS XE platforms. Feature availability, default behavior, and command support can vary by platform and software release.

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. If your network is live, ensure that you understand the potential impact of any command.

Conventions

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

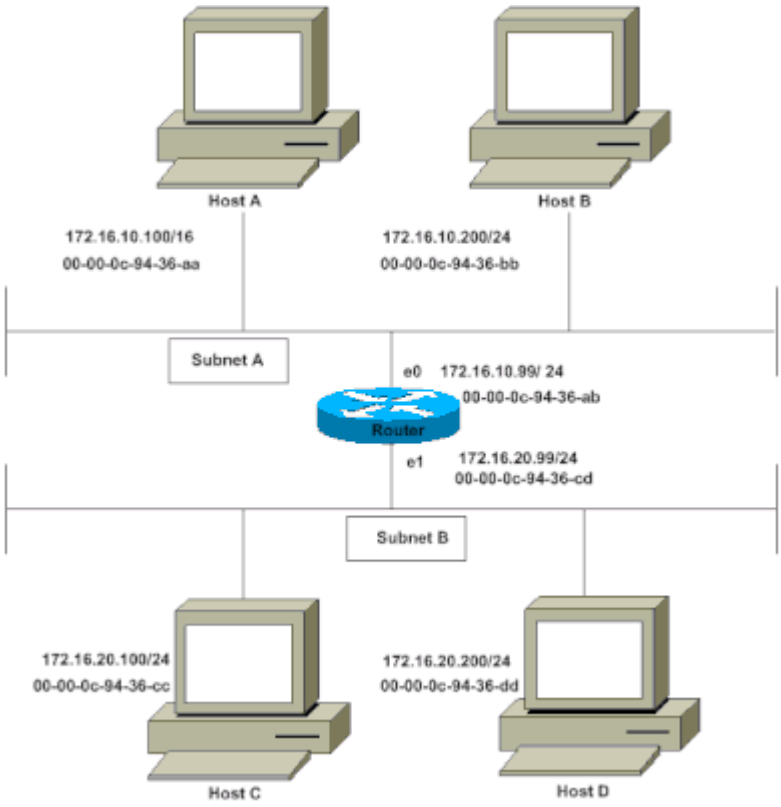
Background Information

Proxy ARP is the technique in which one host, usually a router, answers ARP requests intended for another machine. The router replies with its own MAC address and routes packets to the actual 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.

How Proxy ARP Works

This is an example of how Proxy ARP works:

Network Diagram



Network Diagram

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 Network 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 device it believes is 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 requests the MAC address associated with the destination IP address.

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

Sender MAC Address	Sender 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 nodes on Subnet A, which includes the Ethernet 0 (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 Layer 2 broadcast frames between interfaces.

Because Proxy ARP is enabled on the receiving interface and the router has a route to Host D (172.16.20.200) through another interface, the router replies to Host A with its own MAC address.

Sender MAC Address	Sender 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 Proxy ARP reply in this exchange is 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

Until the ARP entry expires or changes, Host A sends packets for 172.16.20.200 (Host D) to MAC address 00-00-0c-94-36-ab, which belongs to the router. Since the router knows how to reach Host D, the router forwards the packet to Host D. The ARP cache of a host on Subnet A contains the router MAC address for each remote destination for which the router provides a Proxy ARP reply. 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
172.16.10.200	00-00-0c-94-36-bb



Note: Multiple IP addresses are mapped to a single MAC address, which is the MAC address of this router. In this topology, this pattern can indicate that Proxy ARP is in use.

Proxy ARP must be enabled on a Cisco router interface in order for the router to respond on behalf of remote destinations. On Cisco IOS, Proxy ARP is enabled by default on ARP-capable interfaces. Before you disable Proxy ARP, ensure that affected hosts have a valid route or default gateway. On an interface where Proxy ARP is not required, disable it with **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#
```

In order to enable Proxy ARP on an interface, run the **ip proxy-arp** interface configuration command. Run **show ip interface <interface>** in order to verify that the output reports Proxy ARP as enabled.



Note: When Host B (172.16.10.200/24) on Subnet A tries to send packets to Host D (172.16.20.200) on Subnet B, it checks its IP routing table. Host B does not send an ARP request for Host D because the destination is outside the subnet configured on the Host B Ethernet interface. Host B sends the packet to a configured next hop. Without a matching route or default gateway, communication fails.

Advantages of Proxy ARP

The main advantage of Proxy ARP is that it can be enabled on a single router on a network and does not change the routing tables of the other routers on the network.

Proxy ARP can be used on a network where IP hosts do not have a default gateway or another route to the remote destination.

Disadvantages of Proxy ARP

Hosts do not have visibility into the physical network topology and treat the network as a flat segment where an ARP request can resolve any destination address.

The Proxy ARP behavior has several 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 can produce unpredictable next-hop selection when multiple routers provide Proxy ARP replies for the same destination.

Related Information

- IP Support Resources
- NAT Support Page
- Tools and Resources
- Cisco Technical Support and Downloads