

# 프록시 ARP(Address Resolution Protocol) 이해

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[프록시 ARP 작동 방식](#)

[네트워크 다이어그램](#)

[프록시 ARP의 장점](#)

[프록시 ARP의 단점](#)

[관련 정보](#)

---

## 소개

이 문서에서는 프록시 ARP를 사용하여 라우팅 또는 기본 게이트웨이를 구성할 필요 없이 서버넷의 머신이 원격 서버넷에 도달하는 방법을 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에서는 ARP(Proxy Address Resolution Protocol) 및 이더넷 환경에 대한 이해가 필요합니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software 릴리스 12.2(10b)
- Cisco 2500 Series 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

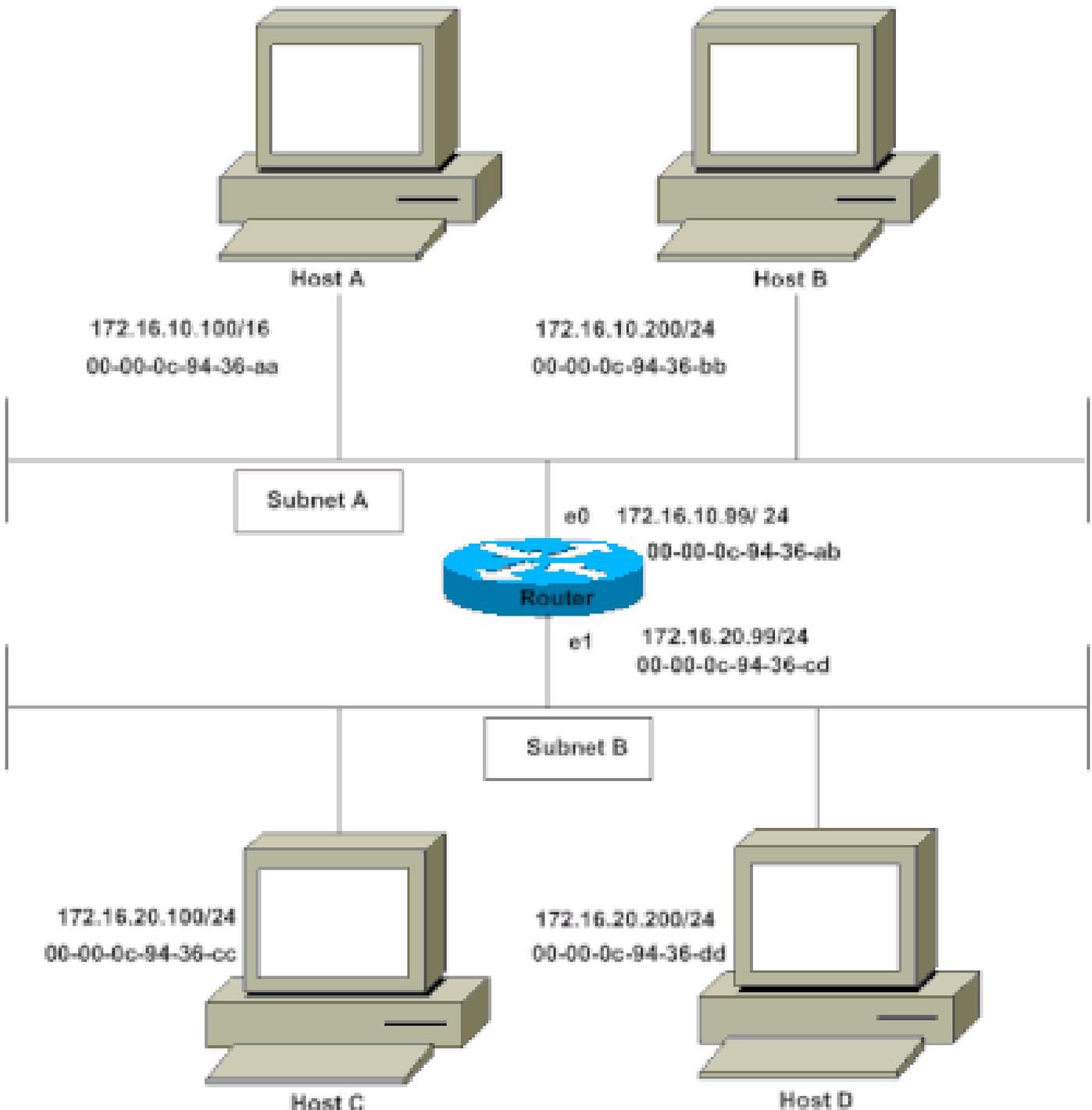
## 배경 정보

이 문서에서는 프록시 ARP(Address Resolution Protocol)의 개념을 설명합니다. 프록시 ARP은 일반적으로 라우터인 한 호스트에서 다른 시스템을 위한 ARP 요청에 응답하는 기술입니다. ID를 위조한 경우, 라우터는 패킷을 "실제" 목적지로 라우팅하는 데 대한 책임을 수락합니다. 프록시 ARP는 라우팅 또는 기본 게이트웨이를 설정할 필요 없이 서브넷의 시스템이 원격 서브넷에 연결되도록 지원할 수 있습니다. 프록시 ARP는 RFC 1027에 정의되어 있습니다.

## 프록시 ARP 작동 방식

다음은 프록시 ARP 작동 방식의 예입니다.

### 네트워크 다이어그램



네트워크 다이어그램

서브넷 A의 호스트 A(172.16.10.100)는 서브넷 B의 호스트 D(172.16.20.200)로 패킷을 전송해야 합니다. 다이어그램에 나와 있는 것처럼 호스트 A에는 /16 서브넷 마스크가 있습니다. 즉, 호스트 A는 모든 네트워크 172.16.0.0에 직접 연결되어 있다고 생각합니다. 호스트 A는 직접 연결된 것으로 판단되는 디바이스와 통신해야 할 경우, ARP 요청을 대상으로 전송합니다. 따라서 호스트 A가 호스트 D에 패킷을 전송해야 하는 경우, 호스트 A는 호스트 D가 직접 연결된 것으로 간주하므로 호스트 D에 ARP 요청을 전송합니다.

호스트 D(172.16.20.200)에 연결하려면 호스트 A에는 호스트 D의 MAC 주소가 필요합니다.

따라서 호스트 A는 다음과 같이 서브넷 A에서 ARP 요청을 브로드캐스트합니다.

발신자 MAC 주소	발신자 IP 주소	대상 MAC 주소	Target IP address
------------	-----------	-----------	-------------------

00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200
-------------------	---------------	-------------------	---------------

이 ARP 요청에서 호스트 A(172.16.10.100)는 호스트 D(172.16.20.200)가 MAC 주소를 전송하도록 요청합니다. 그런 다음 ARP 요청 패킷은 호스트 A의 MAC 주소를 소스 주소로 사용하고 브로드캐스트(FFFF.FFFF.FFFF)를 대상 주소로 사용하는 이더넷 프레임에 캡슐화됩니다. ARP 요청은 브로드캐스트이므로 라우터의 e0 인터페이스를 포함하는 서브넷 A의 모든 노드에 도달하지만 호스트 D에는 도달하지 않습니다. 라우터는 기본적으로 브로드캐스트를 전달하지 않으므로 브로드캐스트는 호스트 D에 도달하지 않습니다.

라우터는 대상 주소(172.16.20.200)가 다른 서브넷에 있으며 호스트 D에 연결할 수 있음을 알고 있으므로 호스트 A에 대한 자체 MAC 주소를 사용하여 응답합니다.

발신자 MAC 주소	발신자 IP 주소	대상 MAC 주소	Target IP address
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

이는 라우터가 호스트 A로 전송하는 프록시 ARP 응답입니다. 프록시 ARP 응답 패킷은 라우터의 MAC 주소를 소스 주소로 사용하고 호스트 A의 MAC 주소를 대상 주소로 사용하여 이더넷 프레임에 캡슐화됩니다. ARP 응답은 항상 원래 요청자에게 유니캐스트됩니다.

이 ARP 응답을 수신하면 호스트 A는 다음과 같이 ARP 테이블을 업데이트합니다.

IP 주소	MAC 주소
172.16.20.200	00-00-0c-94-36-ab

이제부터 호스트 A는 172.16.20.200(호스트 D)에 도달하려는 모든 패킷을 MAC 주소 00-00-0c-94-36-ab(라우터)로 전달합니다. 라우터는 호스트 D에 연결하는 방법을 알고 있으므로 라우터는 패킷을 호스트 D로 전달합니다. 서브넷 A의 호스트에 있는 ARP 캐시는 서브넷 B의 모든 호스트에 대한 라우터의 MAC 주소로 채워집니다. 따라서 서브넷 B로 향하는 모든 패킷은 라우터로 전송됩니다. 라우터는 해당 패킷을 서브넷 B의 호스트로 전달합니다.

다음 표에는 호스트 A의 ARP 캐시가 나와 있습니다.

IP 주소	MAC 주소
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

---

참고: 여러 IP 주소가 단일 MAC 주소(이 라우터의 MAC 주소)에 매핑되며, 이는 프록시 ARP가 사용 중임을 나타냅니다.

---

시스코의 인터페이스는 프록시 ARP를 수락하고 응답하도록 설정해야 합니다. 기본적으로 활성화되어 있습니다. ISP `no ip proxy-arp` 라우터에 연결된 라우터의 인터페이스에 명령을 구성해야 합니다. 프록시 ARP는 다음과 같이 interface configuration 명령을 사용하여 각 인터페이스에서 개별적으로 비활성화할 수 `no ip proxy-arp` 있습니다.

```
<#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)#

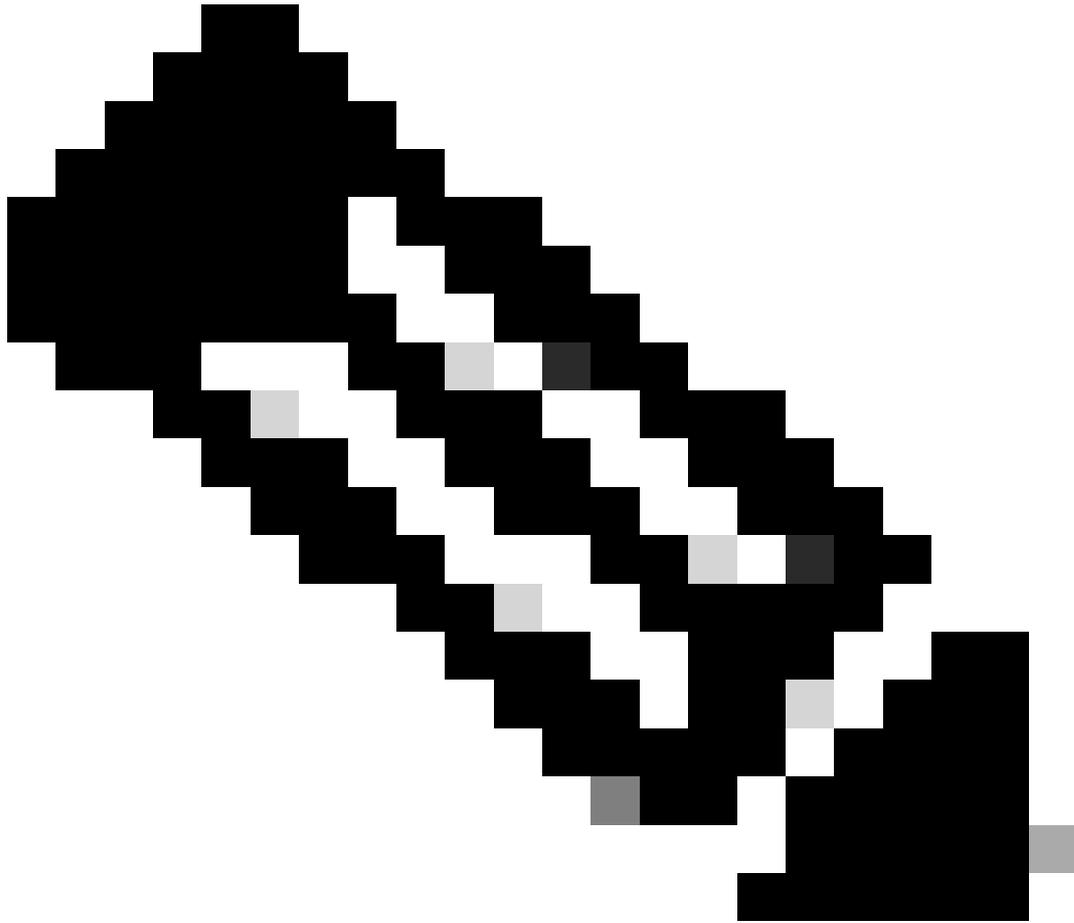
^Z

Router#

인터페이스에서 프록시 ARP를 활성화하려면 interface configuration **ip proxy-arp** 명령을 실행합니다.

---

---



참고: 서브넷 A의 호스트 B(172.16.10.200/24)가 서브넷 B의 대상 호스트 D(172.16.20.200)로 패킷을 전송하려고 시도할 때 IP 라우팅 테이블을 살펴보고 그에 따라 패킷을 라우팅합니다. 호스트 B(172.16.10.200/24)는 호스트 B 이더넷 인터페이스 172.16.20.200/24에 설정된 것과 다른 서브넷에 속해 있기 때문에 호스트 D IP 주소 172.16.20.200에 대해 ARP 하지 않습니다.

---

프록시 ARP의 장점

프록시 ARP의 주요 장점은 네트워크의 단일 라우터에 추가할 수 있으며 네트워크에 있는 다른 라우터의 라우팅 테이블을 방해하지 않는다는 것입니다.

IP 호스트가 기본 게이트웨이로 설정되지 않았거나 라우팅 인텔리전스가 없는 네트워크에서는 프록시 ARP를 사용해야 합니다.

## 프록시 ARP의 단점

호스트는 네트워크의 물리적 세부 사항을 알지 못하며 ARP 요청을 전송할 경우 어떤 목적지에도 도달할 수 있는 플랫 네트워크로 간주합니다. 모든 항목에 ARP를 사용하면 단점이 있습니다. 다음은 몇 가지 단점입니다.

- 

이는 세그먼트에서 ARP 트래픽의 양을 늘립니다.

- 

호스트가 IP-MAC 주소 매핑을 처리하기 위해서는 더 큰 ARP 테이블이 필요합니다.

- 

보안이 손상될 수 있습니다. 하나의 시스템이 패킷을 가로채기 위해 다른 시스템에 클레임할 수 있으며, 이를 "스푸핑"이라고 합니다.

- 

이는 주소 확인에 ARP를 사용하지 않는 네트워크에서는 작동하지 않습니다.

- 

모든 네트워크 토폴로지에 일반화되지는 않습니다. 예를 들어, 두 개의 물리적 네트워크를 연결하는 둘 이상의 라우터가 있습니다.

## 관련 정보

- [IP 지원 리소스](#)
- [NAT 지원 페이지](#)
- [툴 및 리소스](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.