

プロキシアドレス解決プロトコル(ARP)について

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[プロキシ ARP の動作](#)

[ネットワーク図](#)

[プロキシ ARP の利点](#)

[プロキシ ARP の欠点](#)

[関連情報](#)

はじめに

このドキュメントでは、ルーティングやデフォルトゲートウェイを設定せずに、サブネット上のマシンがリモートサブネットに到達するためにプロキシARPがどのように役立つかについて説明します。

前提条件

要件

このドキュメントを読むには、プロキシアドレス解決プロトコル(ARP)とイーサネット環境を理解している必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS®ソフトウェアリリース12.2(10b)
- Cisco 2500 シリーズ ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

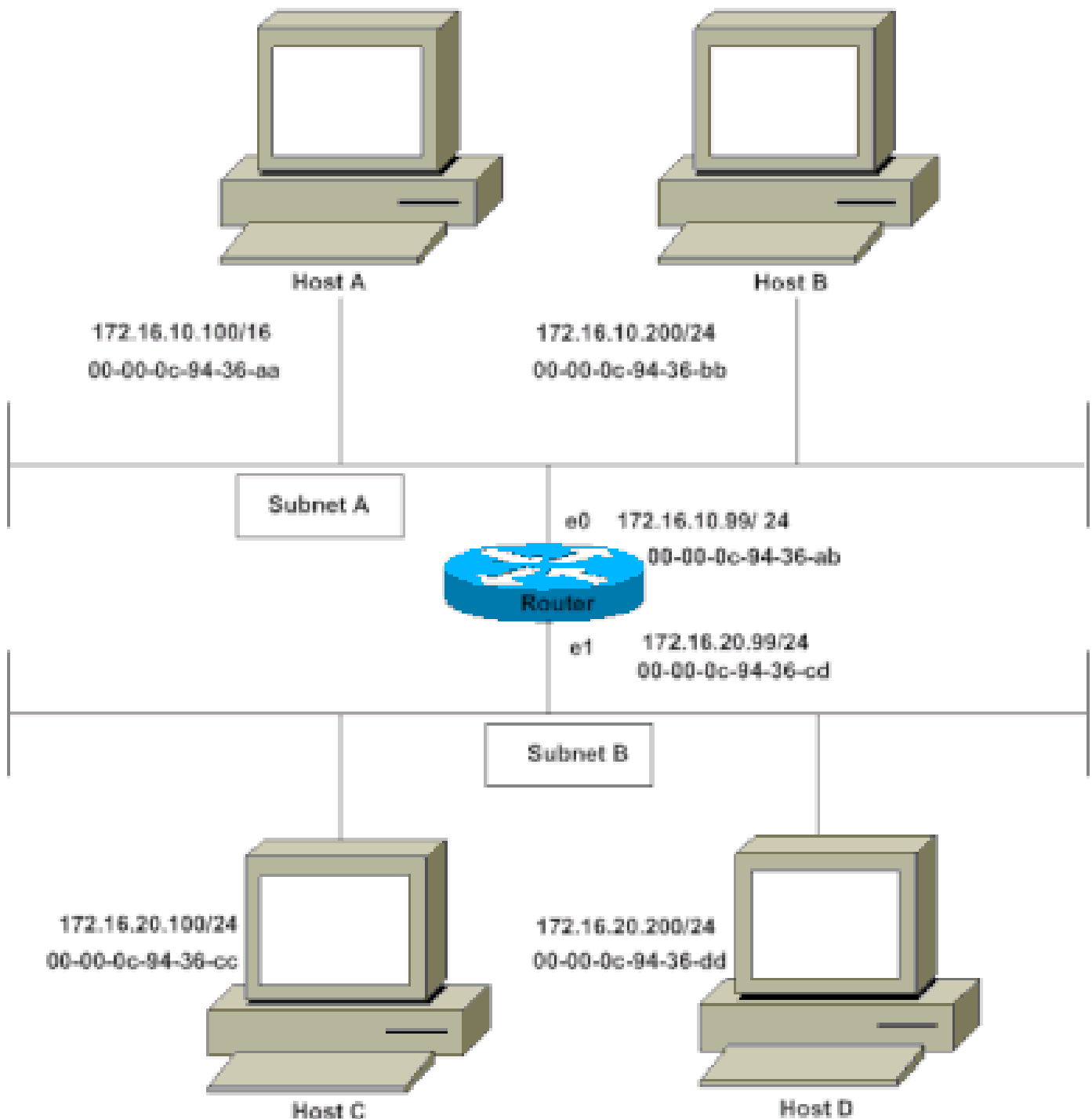
背景説明

このドキュメントでは、プロキシ Address Resolution Protocol (ARP) の概念について説明します。プロキシ ARP とは、あるホスト (通常はルータ) が、別のマシンに宛てられた ARP 要求に応答する技法です。IDを偽装すると、ルータは「実際の」宛先にパケットをルーティングする責任を引き受けます。プロキシ ARP を使用すると、ルーティングやデフォルト ゲートウェイを設定しなくても、サブネット上のマシンがリモートのサブネットに容易に到達できるようになります。プロキシ ARP は、RFC 1027 で定義されています。

プロキシ ARP の動作

次に、プロキシ ARP の動作原理の例を示します。

ネットワーク図



ネットワーク図

サブネット A 上のホスト A (172.16.10.100) から、サブネット B 上のホスト D (172.16.20.200) にパケットを送信する必要があります。ダイアグラムに示されているように、ホスト A のサブネット マスクは /16 です。つまり、ホスト A は、ネットワーク 172.16.0.0 のすべてのデバイスに直接接続されていると認識しています。ホスト A は、直接接続されていると認識しているデバイスと通信する必要がある場合には、宛先に ARP 要求を送信します。したがって、ホスト A は、ホスト D にパケットを送信する必要がある場合には、ホスト D が直接接続されていると認識しているため、ホスト D に ARP 要求を送信します。

ホスト D (172.16.20.200) に到達するためには、ホスト A はホスト D の MAC アドレスを認識する必要があります。

したがって、次に示すように、ホスト A はサブネット A に ARP 要求をブロードキャストします。

送信元MACアドレス	送信元IPアドレス	ターゲットMACアドレス	ターゲットIPアドレス
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

この ARP 要求で、ホスト A (172.16.10.100) はホスト D (172.16.20.200) に MAC アドレスを送信するように要求します。この ARP 要求パケットは、ホスト A の MAC アドレスを送信元アドレスとして、ブロードキャスト (FFFF.FFFF.FFFF) を宛先アドレスとして、イーサネットフレームにカプセル化されます。ARP 要求はブロードキャストであるため、サブネット A 上のすべてのノード (ルータの e0 インターフェイスを含む) に到達しますが、ホスト D には到達しません。ブロードキャストはホスト D に到達しません。ルータは、デフォルトでは、ブロードキャストを転送しないためです。

ルータは、ターゲットアドレス (172.16.20.200) が別のサブネット上にあり、ホスト D に到達できることを認識しているため、自身の MAC アドレスをホスト A に返送します。

送信元MACアドレス	送信元IPアドレス	ターゲットMACアドレス	ターゲットIPアドレス
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

これはルータがホスト A に送信するプロキシ ARP 応答です。プロキシ ARP 応答パケットは、ルータの MAC アドレスを送信元アドレスとして、ホスト A の MAC アドレスを宛先アドレスとして、イーサネットフレームにカプセル化されます。ARP 応答は常に元の要求元へのユニキャストです。

ホスト A は、このARP応答を受け取ると、ARP テーブルを次のように更新します。

IP アドレス	MAC アドレス
172.16.20.200	00-00-0c-94-36-ab

これ以降、ホスト A は、172.16.20.200 (ホスト D) に送信するすべてのパケットを MAC アドレス 00-00-0c-94-36-ab (ルータ) に転送します。ルータは、ホスト D に到達する方法を認識しているため、受け取ったパケットをホスト D に転送します。サブネット A のホストの ARP キャッシュにルータの MAC アドレスが追加されます。そのため、サブネット B 宛てのすべてのパケットがルータに送信されます。ルータは、これらのパケットをサブネット B のホストに転送します。

次の表に、ホスト A の ARP キャッシュを示します。

IP アドレス	MAC アドレス
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

注：複数のIPアドレスが1つのMACアドレス（このルータのMACアドレス）にマッピングされています。これはプロキシARPが使用されていることを示します。

シスコのインターフェイスは、プロキシ ARP を受け入れて応答するように設定されている必要があります。このコマンドはデフォルトで有効になっています。 `no ip proxy-arp` コマンドは、ISPルータに接続されているルータのインターフェイスで設定する必要があります。プロキシARPは、次に示すように、インターフェイスコンフィギュレーションコマンド `no ip proxy-arp` を使用して、各インターフェイスで個別に無効にできます。

```
<#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#

インターフェイスでプロキシARPをイネーブルにするには、**ip proxy-arp**インターフェイス設定コマンドを発行します。



注：サブネットA上のホストB(172.16.10.200/24)がサブネットB上の宛先ホストD(172.16.20.200)にパケットを送信しようとする、ホストBは自身のIPルーティングテーブルを調べて、それに応じてパケットをルーティングします。ホストB (172.16.10.200/24) は、ホスト D の IP アドレス 172.16.20.200 に対して ARP を実行しません。ホスト D は、ホスト B のイーサネット インターフェイス 172.16.20.200/24 に設定されているものとは異なるサブネットに属しているためです。

プロキシ ARP の利点

プロキシ ARP の主な利点は、ネットワーク上の 1 台のルータに追加でき、ネットワーク上の他のルータのルーティング テーブルを阻害しないことです。

IP ホストにデフォルト ゲートウェイが設定されていないネットワークや、IP ホストがインテリジェントなルーティング機能を備えていないネットワークでは、プロキシ ARP を使用する必要があります。

プロキシ ARP の欠点

ホストはネットワークの物理的な詳細を認識せず、ARP 要求を送信すれば宛先に到達できるフラットネットワークであると想定します。すべてを ARP で処理する場合には、デメリットがあります。次に、プロキシ ARP の欠点をいくつか列挙します。

- セグメント上の ARP トラフィック量が増大します。
- IP と MAC のアドレス マッピングを処理するために、ホストに大きな ARP テーブルが必要になります。
- セキュリティが脆弱化するおそれがあります。マシンが別のマシンを名乗ってパケットを傍受できます。これは「スプーフィング」と呼ばれる行為です。
- アドレス解決に ARP を使用していないネットワークでは機能しません。
- あらゆるネットワーク トポロジで汎用的に使用できるものではありません。たとえば、2 つの物理ネットワークを複数のルータで接続しているトポロジでは使用できません。

関連情報

- [IP サポート リソース](#)
- [NAT に関するサポート ページ](#)
- [ツールとリソース](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。