Analyse des Proxy Address Resolution Protocol (ARP)

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Proxy-ARP Computer in einem Subnetz dabei unterstützt, entfernte Subnetze zu erreichen, ohne dass Routing oder ein Standard-Gateway konfiguriert werden müssen.

Voraussetzungen

Anforderungen

In diesem Dokument werden Kenntnisse über das Proxy Address Resolution Protocol (ARP) und die Ethernet-Umgebung vorausgesetzt.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco IOS® Softwareversion 12.2 (10b)
- Router der Cisco 2500 Serie

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

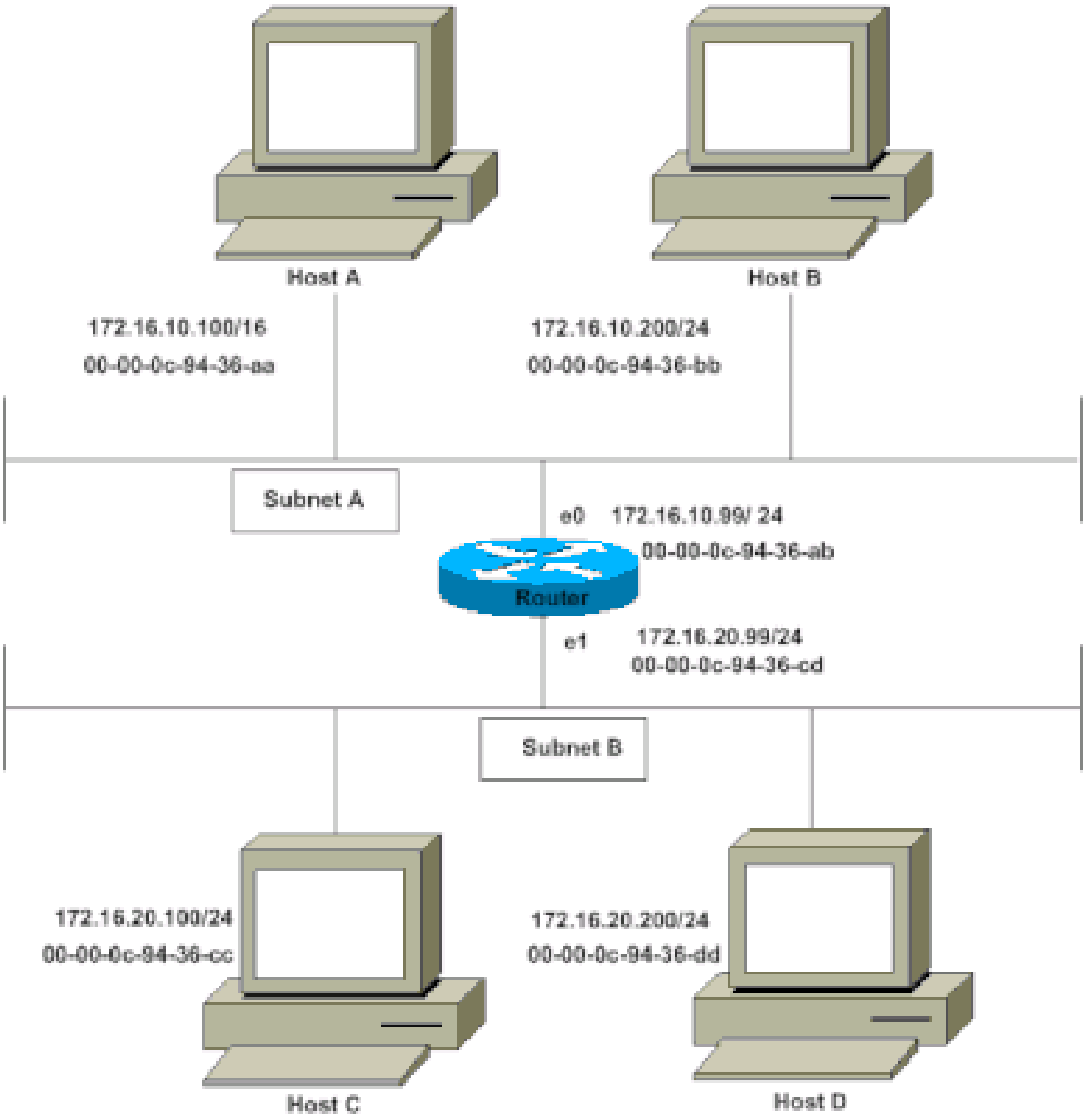
Hintergrundinformationen

In diesem Dokument wird das Konzept des Proxy Address Resolution Protocol (ARP) erläutert. Proxy-ARP ist das Verfahren, bei dem ein Host (in der Regel ein Router) ARP-Anforderungen beantwortet, die für einen anderen Rechner bestimmt sind. Wenn Sie seine Identität vortäuschen, übernimmt der Router die Verantwortung für das Routing von Paketen an das "echte" Ziel. Proxy-ARP kann Computer in einem Subnetz dabei unterstützen, entfernte Subnetze zu erreichen, ohne dass Routing oder ein Standard-Gateway konfiguriert werden müssen. Proxy ARP wird in RFC 1027 definiert.

Wie funktioniert Proxy-ARP?

Dies ist ein Beispiel für die Funktionsweise von Proxy-ARP:

Netzwerkdiagramm



Netzwerkdiagramm

Host A (172.16.10.100) in Subnetz A muss Pakete an Host D (172.16.20.200) in Subnetz B senden. Wie im Diagramm gezeigt, verfügt Host A über eine /16-Subnetzmaske. Das bedeutet, dass Host A glaubt, direkt mit dem gesamten Netzwerk 172.16.0.0 verbunden zu sein. Wenn Host A mit Geräten kommunizieren muss, die seiner Meinung nach direkt verbunden sind, sendet er eine ARP-Anforderung an das Ziel. Wenn Host A ein Paket an Host D senden muss, glaubt Host A, dass Host D direkt verbunden ist, und sendet daher eine ARP-Anforderung an Host D.

Um Host D (172.16.20.200) zu erreichen, benötigt Host A die MAC-Adresse von Host D.

Host A sendet daher eine ARP-Anforderung an Subnetz A, wie dargestellt:

MAC-Adresse des Absenders	Absender-IP-Adresse	MAC-Zieladresse	Target IP address

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

In dieser ARP-Anforderung fordert Host A (172.16.10.100) an, dass Host D (172.16.20.200) seine MAC-Adresse sendet. Das ARP-Anforderungspaket wird dann in einem Ethernet-Frame mit der MAC-Adresse von Host A als Quelladresse und einer Broadcast-Adresse (FFFF.FFFF.FFFF) als Zieladresse gekapselt. Da es sich bei der ARP-Anforderung um eine Broadcast-Anforderung handelt, erreicht sie alle Knoten im Subnetz A, das die e0-Schnittstelle des Routers enthält, jedoch nicht Host D. Der Broadcast erreicht Host D nicht, da die Router standardmäßig keine Broadcasts weiterleiten.

Da der Router weiß, dass sich die Zieladresse (172.16.20.200) in einem anderen Subnetz befindet und Host D erreichen kann, antwortet er mit seiner eigenen MAC-Adresse auf Host A.

MAC-Adresse des Absenders	Absender-IP-Adresse	MAC-Zieladresse	Target IP address
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Dies ist die Proxy-ARP-Antwort, die der Router an Host A sendet. Das Proxy-ARP-Antwortpaket wird in einem Ethernet-Frame mit der MAC-Adresse des Routers als Quelladresse und der MAC-Adresse von Host A als Zieladresse eingekapselt. Die ARP-Antworten werden immer als Unicast an den ursprünglichen Anforderer gesendet.

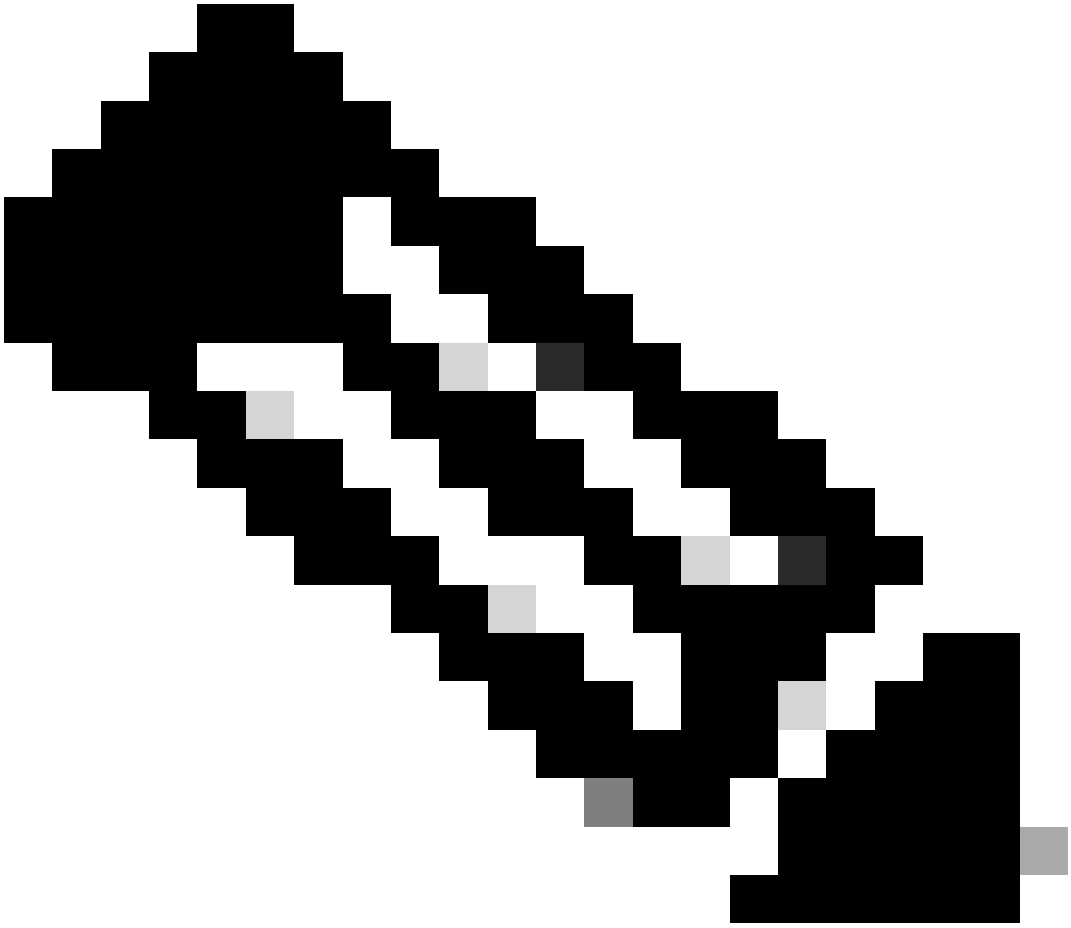
Nach Erhalt dieser ARP-Antwort aktualisiert Host A seine ARP-Tabelle wie folgt:

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

Von nun an leitet Host A alle Pakete, die 172.16.20.200 (Host D) erreichen sollen, an die MAC-Adresse 00-00-0c-94-36-ab (Router) weiter. Da der Router weiß, wie er Host D erreicht, leitet der Router das Paket an Host D weiter. Der ARP-Cache auf den Hosts in Subnetz A wird mit der MAC-Adresse des Routers für alle Hosts in Subnetz B gefüllt. Daher werden alle Pakete, die an Subnetz B gerichtet sind, an den Router gesendet. Der Router leitet diese Pakete an die Hosts in Subnetz B weiter.

Der ARP-Cache von Host A ist in der folgenden Tabelle dargestellt:

IP-Adresse	MAC-Adresse
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



Hinweis: Einer einzelnen MAC-Adresse, der MAC-Adresse dieses Routers, werden mehrere IP-Adressen zugeordnet. Dies zeigt an, dass Proxy-ARP verwendet wird.

Die Cisco-Schnittstelle muss so konfiguriert werden, dass sie Proxy-ARP akzeptiert und darauf reagiert. Dies ist standardmäßig aktiviert. Der **no ip proxy-arp**Befehl muss auf der Schnittstelle des Routers konfiguriert werden, der mit dem ISP-Router verbunden ist. Proxy-ARP kann auf jeder Schnittstelle einzeln mithilfe des Schnittstellenkonfigurationsbefehls deaktiviert werden**no ip proxy-arp** , wie dargestellt:

<#root>

Router#

configure terminal

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

```
 interface ethernet 0
```

```
Router(config-if)#
```

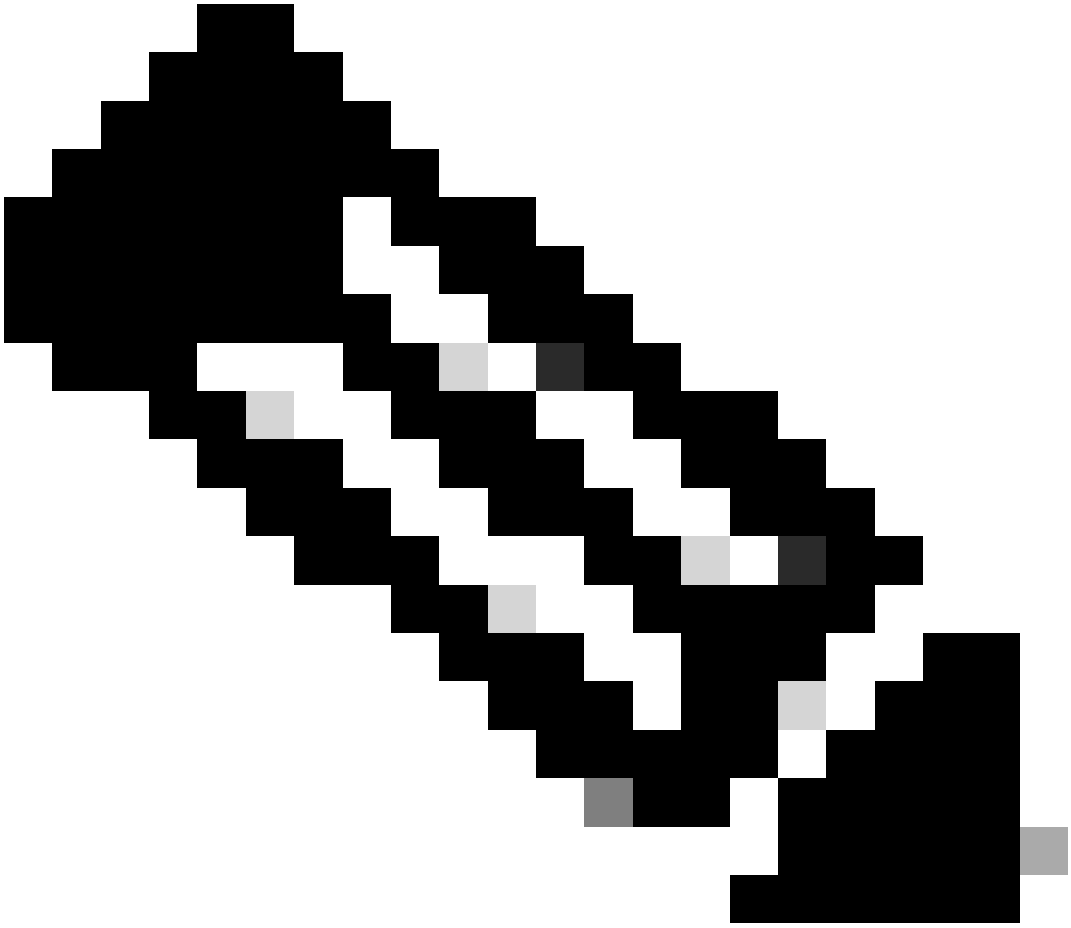
```
 no ip proxy-arp
```

```
Router(config-if)#
```

```
^Z
```

```
Router#
```

Um den Proxy-ARP für eine Schnittstelle zu aktivieren, geben Sie den Schnittstellenkonfigurationsbefehl **ip proxy-arp**ein.



Hinweis: Wenn Host B (172.16.10.200/24) in Subnetz A versucht, Pakete an den Ziel-Host D (172.16.20.200) in Subnetz B zu senden, prüft er dessen IP-Routing-Tabelle und leitet das Paket entsprechend weiter. Host B (172.16.10.200/24) führt für die IP-Adresse von Host D (172.16.20.200) kein ARP aus, da er zu einem anderen Subnetz gehört als das, was auf der Host-B-Ethernet-Schnittstelle 172.16.20.200/24 konfiguriert ist.

Vorteile von Proxy-ARP

Der Hauptvorteil des Proxy-ARP besteht darin, dass es einem einzelnen Router in einem Netzwerk hinzugefügt werden kann und die Routing-Tabellen der anderen Router im Netzwerk nicht stört.

Proxy-ARP muss im Netzwerk verwendet werden, in dem IP-Hosts nicht mit einem Standard-Gateway konfiguriert sind oder über keine intelligenten Routingfunktionen verfügen.

Nachteile von Proxy-ARP

Hosts haben keine Ahnung von den physischen Details ihres Netzwerks und nehmen an, dass es sich um ein flaches Netzwerk handelt, in dem sie jedes Ziel erreichen können, wenn sie eine ARP-Anfrage senden. Wenn Sie ARP für alles verwenden, gibt es Nachteile. Dies sind einige der Nachteile:

- Dies erhöht den ARP-Datenverkehr in Ihrem Segment.
- Hosts benötigen größere ARP-Tabellen, um IP-MAC-Adresszuordnungen handhaben zu können.
- Sicherheit kann untergraben werden. Eine Maschine kann behaupten, eine andere zu sein, um Pakete abzufangen, ein Vorgang, der "Spoofing" genannt wird.
- Dies funktioniert nicht in Netzwerken, die ARP nicht für die Adressauflösung verwenden.
- Es wird nicht für alle Netzwerktopologien verallgemeinert. Beispiel: mehr als ein Router, der zwei physische Netzwerke verbindet.

Zugehörige Informationen

- **IP-Supportressourcen**
- **NAT-Support-Seite**
- **Tools und Ressourcen**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.