Протокол прокси-ARP

Содержание

Введение

В этом документе объясняется понятие прокси-ARP (Протокол разрешения адресов). Прокси-ARP - это способ, с помощью которого один хост, обычно маршрутизатор, отвечает на ARP-запросы, предназначенные для другого устройства. За счет "подделки" своей идентификации маршрутизатор принимает на себя ответственность за маршрутизацию пакетов к "реальному" пункту назначения. Прокси-ARP позволяет компьютерам подсети получить доступ к удаленным подсетям без настройки маршрутизации или шлюза по умолчанию. Протокол прокси-ARP описан в разделе RFC 1027 .

Предварительные условия

Требования

Данный документ требует понимания принципов работы ARP и Ethernet.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения:

- ПО Cisco IOS® версии 12.2 (10b)
- Маршрутизаторы серии Cisco 2500

Сведения, содержащиеся в данном документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, обладают ненастроенной (заданной по умолчанию) конфигурацией. При работе в действующей сети перед применением команды необходимо изучить все возможные последствия ее выполнения.

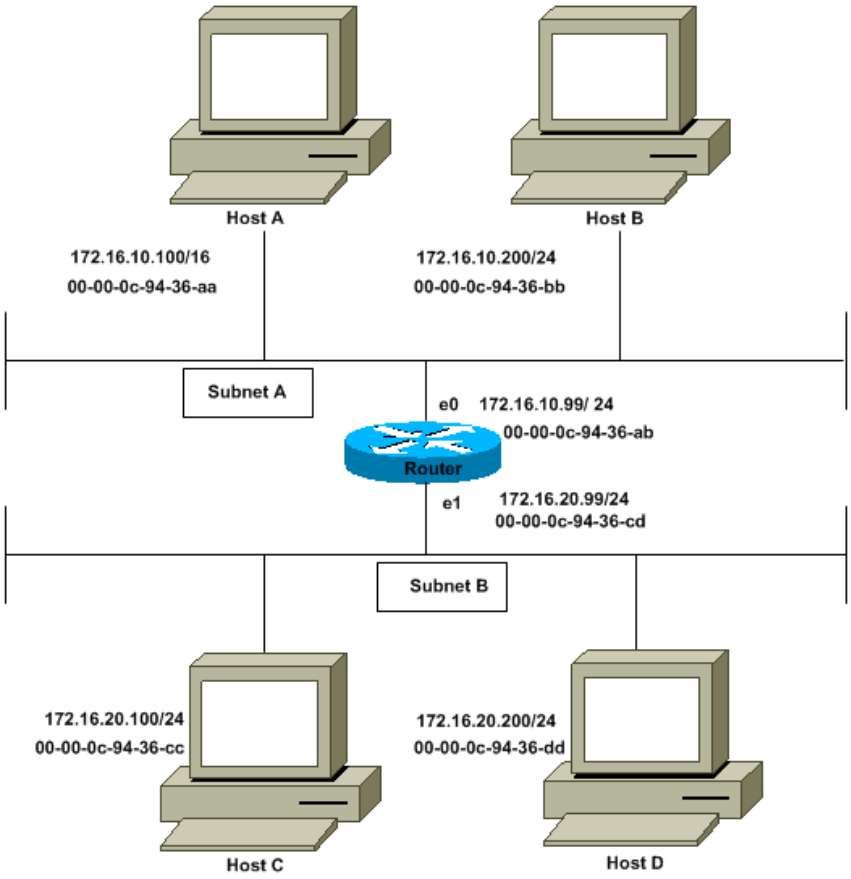
Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. в статье Условные обозначения, используемые в технической документации Cisco.

Как работает протокол прокси-ARP?

Ниже приведен пример работы прокси-ARP:

Схема сети



Хосту A (172.16.10.100) подсети A необходимо отправить пакеты хосту D (172.16.20.200) подсети B. Как показано на рисунке выше, у хоста A есть маска подсети a /16. Это значит, что узел A предполагает, что он непосредственно подключен ко всем адресам 172.16.0.0 в сети. Когда хосту A необходимо связаться с устройством, которое предположительно подключено напрямую, он посылает на это устройство ARP-запрос. Таким образом, если хосту A требуется отправить пакет на хост D, который считается подключенным напрямую, хост A отправляет хосту D ARP-запрос.

Для получения доступа к хосту D (172.16.20.200) хосту A нужен MAC-адрес хоста D.

Поэтому хост A передает ARP-запрос в широковещательном режиме на подсеть A, как показано ниже:

MAC-адрес отправителя	IP-адрес отправителя	Целевой MAC-адрес	Целевой IP-адрес
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

Хост A (172.16.10.100) в вышеуказанном запросе ARP запрашивает отправку хостом D (172.16.20.200) своего MAC-адреса. Затем указанный выше пакет запроса ARP инкапсулируется в кадре Ethernet с MAC-адресом хоста A в качестве адреса источника и широковещательной рассылкой (FFFF.FFFF.FFFF) в качестве адреса назначения. Из-за широковещательной рассылки ARP-запрос достигает всех узлов в подсети A, включая интерфейс e0 маршрутизатора, кроме хоста D. Эта рассылка не достигает хоста D, так как маршрутизаторы по умолчанию ее не отправляют.

Поскольку маршрутизатору известно, что целевой адрес (172.16.20.200) находится в другой подсети и достигает хост D, он посылает в ответ собственный MAC-адрес хосту A.

MAC-адрес отправителя	IP адрес отправителя	Целевой MAC-адрес	Целевой IP-адрес
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Выше указан ответ прокси-ARP, который маршрутизатор посылает к хосту A. Ответный пакет прокси-ARP инкапсулируется в кадр Ethernet с MAC-адресом маршрутизатора в качестве адреса источника и с MAC-адресом хоста A в качестве адреса назначения. ARP-ответы являются одноадресными и посылаются узлу, инициировавшему запрос.

При получении ответа ARP хост A обновляет таблицу ARP, как показано ниже:

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

Теперь хост A будет пересылать все пакеты, которые должны достигнуть 172.16.20.200 (хост D), на MAC-адрес 00-00-0c-94-36-ab (маршрутизатор). Так как маршрутизатору известен путь достижения хоста D, он отправляет пакет этому хосту. ARP-кэш на хостах подсети A загружен MAC-адресом маршрутизатора для всех хостов подсети B. Поэтому все пакеты, предназначенные для подсети B, отправляются маршрутизатору. Маршрутизатор пересылает эти пакеты хостам в подсеть B.

Кэш ARP хоста A представлен ниже:

IP-адрес	MAC-адрес
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

Примечание. Несколько IP-адресов сопоставляются с одним MAC-адресом (MAC-адресом маршрутизатора), что указывает на использование протокола прокси-ARP.

Интерфейс маршрутизатора Cisco должен быть настроен на прием и отправку прокси-ARP. Этот режим включен по умолчанию. Прокси-ARP отключается командой конфигурирования интерфейса **no ip proxy-arp** на уровне отдельного интерфейса, как показано ниже:

```
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#
```

Чтобы включить прокси-ARP на интерфейсе используйте команду конфигурирования интерфейса **ip proxy-arp**.

Примечание. Если хост B (172.16.10.200/24) в подсети A пытается отправить пакеты на хост D (172.16.20.200) подсети B, он обращается к таблице IP-маршрутизации и использует соответствующий адрес для маршрутизации. Хост B (172.16.10.200/24) не запускает прокси-ARP для IP-адреса 172.16.20.200 хоста D, так как он принадлежит другой подсети, отличающейся от подсети, настроенной на хосте B интерфейса ethernet 172.16.20.200/24.

Преимущества прокси-ARP

Основное преимущество использования прокси-ARP состоит в том, что этот протокол можно установить на один маршрутизатор в сети без изменения таблиц маршрутизации на остальных маршрутизаторах в той же сети.

Прокси-ARP используется в сети, где IP-хосты не настроены в шлюзе по умолчанию или не обладают интеллектуальными функциями маршрутизации.

Недостатки прокси-ARP

Хостам неизвестны физические характеристики сети - предполагается однородная сеть, в которой хосты могут достичь любого получателя с помощью ARP-запроса. Но при использовании прокси-ARP проявляются недостатки, некоторые из которых перечислены ниже:

- Это увеличивает объем ARP-трафика в вашем сегменте сети.
- Хостам необходимы большие ARP-таблицы для обработки сопоставления IP-адресов и MAC-адресов.
- Система безопасности может быть нарушена. Один компьютер может выдавать себя за другой для перехвата пакетов. Это называется "спуфингом".
- Это не относится к сетям, которые не используют ARP для разрешения адресов.
- Это не касается всех сетевых топологий (например, нескольких маршрутизаторов, соединяющих две физические сети).

Для получения более подробных сведений о настройке прокси-ARP см. раздел Включение прокси-ARP документа Настройка IP–адресов.

Дополнительные сведения

- **Поддержка IP-ресурсов**
- **Страница поддержки NAT**
- **Программные средства и ресурсы**
- **Техническая поддержка – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107536/5.shtml