Протокол прокси-ARP

Содержание

Введение

В этом документе объяснено понятие протокола разрешения адресов (ARP) прокси. 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 - протокол преобразования адресов может помочь машинам на подсети достигать удаленных подсетей без потребности настроить маршрутизацию или шлюз 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 обеспечения и оборудования:

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

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

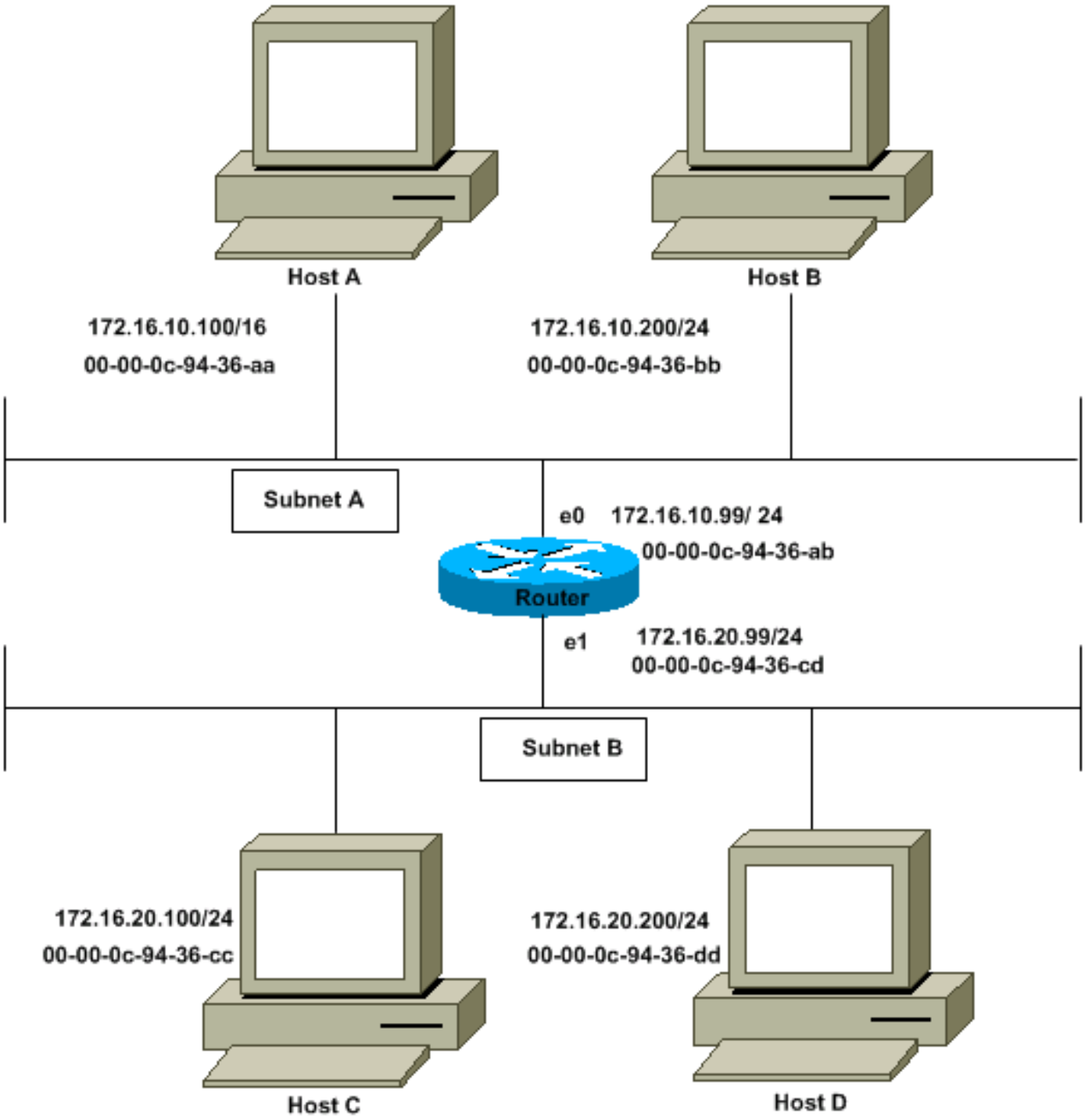
Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Как работает ARP-прокси?

Это - пример того, как работает прокси - протокол преобразования адресов:

Схема сети



Хост A (172.16.10.100) на Подсети потребности передать пакеты Хосту D (172.16.20.200) на Подсети B. Как показано в схеме, Хост A имеет/16 маску подсети. Это значит, что узел A

предполагает, что он непосредственно подключен ко всем адресам 172.16.0.0 в сети. Когда Хост A должен связаться с любыми устройствами, он верит, напрямую подключаются, он передает запрос ARP назначению. Таким образом, если хосту A требуется отправит пакет на хост D, который считается подключенным напрямую, хост A отправляет хосту D запрос ARP.

Для достижения Хоста D (172.16.20.200) Хосту A нужен MAC-адрес Хоста D.

Поэтому Хост A передает запрос ARP на Подсети A, как показано:

MAC-адрес отправителя	IP адрес отправителя	MAC-адрес назначения	Target IP address
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

В этом запросе ARP, Хост A (172.16.10.100) запросы, чтобы Хост D (172.16.20.200) передал свой MAC-адрес. Пакет запроса ARP тогда инкапсулируется во Фрейме Ethernet с MAC-адресом Хоста A как адрес источника и широковещание (FFFF.FFFF.FFFF) как адрес назначения (DA). Так как запрос ARP является широковещанием, он достигает всех узлов в Подсети A, который включает e0 интерфейс маршрутизатора, но не достигает Хоста D. Широковещание не достигает Хоста D, потому что маршрутизаторы, по умолчанию, не передают широковещательные сообщения.

Так как маршрутизатор знает, что целевой адрес (172.16.20.200) находится на другой подсети и может достигнуть Хоста D, это отвечает с его собственным MAC-адресом на Хост A.

MAC-адрес отправителя	IP адрес отправителя	MAC-адрес назначения	Target IP address
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

Это - Ответ прокси ARP, который маршрутизатор передает к Хосту A. Пакет ответа ARP прокси-сервера инкапсулируется во Фрейме Ethernet с MAC-адресом маршрутизатора как адрес источника и MAC-адрес Хоста A как адрес назначения (DA). ARP-ответы являются одноадресными и посылаются узлу, инициировавшему запрос.

По получении этого ответа ARP Хост A обновляет свою таблицу ARP, как показано:

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

С этого времени Хост A передает все пакеты, которых он хочет достигнуть 172.16.20.200 (Хост D) MAC-адреса 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 показывают в этой таблице:

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 - адресовы сопоставлены с одиночным MAC-адресом, MAC-адресом этого маршрутизатора, который указывает, что используется прокси - протокол преобразования адресов.

Интерфейс Cisco должен быть настроен, чтобы принять и ответить на прокси - протокол преобразования адресов. Это значение используется по умолчанию. Команда **no ip proxy-arp** должна быть настроена на интерфейсе маршрутизатора, связанного с маршрутизатором ISP. Прокси - протокол преобразования адресов может быть отключен на каждом интерфейсе индивидуально с **no ip proxy-arp** команды настройки интерфейса, как показано:

```
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#
```

Для включения прокси - протокола преобразования адресов на интерфейсе выполните команду настройки интерфейса **ip proxy-arp**.

Примечание: Когда Хост B (172.16.10.200/24) на Подсети попытки передать пакеты адресату D (172.16.20.200) на Подсети B, это изучает свою таблицу IP-маршрутизации и направляет пакет соответственно. Хост B (172.16.10.200/24) не делает ARP для IP-адреса Хоста D 172.16.20.200, потому что это принадлежит другой подсети, чем, что настроено на интерфейсе Ethernet Хоста B 172.16.20.200/24.

Преимущества прокси ARP

Основное преимущество прокси - протокола преобразования адресов - то, что он может быть добавлен к одиночному маршрутизатору в сети и не нарушает таблицы маршрутизации других маршрутизаторов в сети.

Прокси - протокол преобразования адресов должен использоваться в сети, где IP-узлы не настроены со шлюзом по умолчанию или не имеют никаких логических функций маршрутизации.

Недостатки агента ARP

Узлы не осведомлены о физических особенностях сети и полагают, что это однородная сеть, в которой они могут достичь любого получателя с помощью ARP-запроса. Но использование ARP для всего имеет недостатки. Это некоторые недостатки:

- Это увеличивает объем ARP трафика в вашем сегменте.
- Размещает потребность большие таблицы ARP для обработки сопоставлений IP К MAC-АДРЕСУ.
- Безопасность можно подорвать. Один компьютер может выдавать себя за другой, чтобы

перехватить пакеты. Это называется "спуфингом"."
- Это не относится к сетям, которые не используют ARP для разрешения адресов.
- Это не делает вывод ко всем топологиям сети. Например, несколько маршрутизаторов, которые подключают две физических сети.

См. раздел Прокси - протокола преобразования адресов Включения IP-адресации Настройки для получения дополнительной информации о настройке прокси - протокола преобразования адресов.

Дополнительные сведения

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