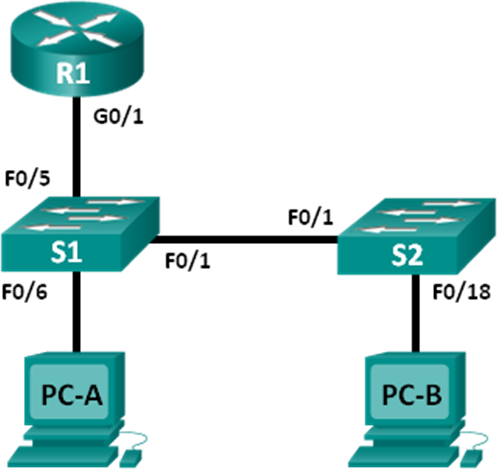
Лабораторная работа. Изучение протокола ARP с помощью интерфейса командной строки Windows, интерфейса командной строки IOS и Wireshark РИ 340003

1. Топология

****

1. Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети | Шлюз по умолчанию |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | — |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| PC-B | NIC | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |

1. Задачи

Часть 1. Создание и настройка сети

Часть 2. Использование команды ARP в ОС Windows

Часть 3. Использование команды show arp в IOS

Часть 4. Анализ обмена сообщениями ARP с помощью программы Wireshark

1. Общие сведения/сценарий

Протокол разрешения адресов (ARP) используется протоколом TCP/IP для сопоставления IP-адреса уровня 3 с МАС-адресом уровня 2. Когда кадр помещается в сеть, он должен содержать MAC-адрес назначения. Для динамического определения MAC-адреса устройства назначения по локальной сети отправляется широковещательный запрос ARP. Устройство, которое содержит IP-адрес назначения, отвечает, и MAC-адрес записывается в ARP-кэш. Каждое устройство в локальной сети имеет собственный ARP-кэш — небольшой участок в ОЗУ, где хранятся результаты ARP. Таймер ARP-кэша удаляет ARP-записи, которые не использовались в течение определенного периода времени.

ARP — яркий пример компромисса с точки зрения производительности. При отсутствии кэша протокол ARP должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети. И наоборот, неограниченное время хранения записей может привести к ошибкам при работе с устройствами, которые покидают сеть или меняют адрес 3 уровня.

Хотя в своей работе сетевой администратор не обязательно будет постоянно взаимодействовать с ARP, иметь представление о протоколе ARP всё же необходимо. ARP — это протокол, который позволяет сетевым устройствам обмениваться данными с протоколом TCP/IP. Без него невозможно эффективно построить датаграмму для адреса назначения уровня 2. Однако, ARP может создавать риски для безопасности. Хакеры используют ARP-спуфинг, или «отравление» ARP-кэша, для внедрения в сети неверных МАС-адресов. Злоумышленник генерирует ложный MAC-адрес устройства, в результате чего кадры передаются на неверный адрес назначения. Ручная настройка статических связей ARP — это один из способов предотвращения атак на основе протокола ARP. И наконец, для предотвращения несанкционированного доступа к сети на устройствах Cisco можно настроить список авторизованных МАС-адресов.

В данной лабораторной работе вам предстоит отобразить таблицу ARP с помощью команд ARP в маршрутизаторах Windows и Cisco. Кроме того, вы очистите ARP-кэш и добавите статические записи ARP.

**Примечание**. В практических лабораторных работах CCNA используются маршрутизаторы с интегрированными сервисами Cisco 1941 (ISR) под управлением Cisco IOS версии 15.2(4) M3 (образ universalk9). Также используются коммутаторы Cisco Catalyst 2960 с операционной системой Cisco IOS версии 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Точные идентификаторы интерфейсов см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание**. Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены, обратитесь к инструктору.

1. Необходимые ресурсы

* 1 маршрутизатор (Cisco 1941 с операционной системой Cisco IOS 15.2(4)M3 (универсальный образ) или аналогичная модель)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (Windows 7, Vista или XP с программой эмуляции терминала, например, Tera Term, и установленной программой Wireshark)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты
* Кабели Ethernet, расположенные в соответствии с топологией.

**Примечание.** Интерфейсы Fast Ethernet на коммутаторах Cisco 2960 определяют тип подключения автоматически, поэтому между коммутаторами S1 и S2 можно использовать прямой кабель Ethernet. При использовании коммутатора Cisco другой модели может потребоваться перекрестный кабель Ethernet.

1. Создание и настройка сети
   1. Подключите сеть в соответствии с топологией.
   2. Настройте IP-адреса устройств в соответствии с таблицей адресации.
   3. Проверьте подключение к сети, отправив с PC-B эхо-запросы с помощью команды ping на все устройства.
2. Использование команды ARP в ОС Windows

Команда **arp** позволяет пользователю просматривать и изменять ARP-кэш в ОС Windows. Команда вводится в командную строку Windows.

* 1. Отобразите ARP-кэш.
     1. Откройте окно командной строки на PC-A и введите **arp**.

C:\Users\User1> **arp**

Displays and modifies the IP-to-Physical address translation tables used by

address resolution protocol (ARP).

ARP -s inet\_addr eth\_addr [if\_addr]

ARP -d inet\_addr [if\_addr]

ARP -a [inet\_addr] [-N if\_addr] [-v]

-a Displays current ARP entries by interrogating the current

protocol data. If inet\_addr is specified, the IP and Physical

addresses for only the specified computer are displayed. If

more than one network interface uses ARP, entries for each ARP

table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid

entries and entries on the loop-back interface will be shown.

inet\_addr Specifies an internet address.

-N if\_addr Displays the ARP entries for the network interface specified

by if\_addr.

-d Deletes the host specified by inet\_addr. inet\_addr may be

wildcarded with \* to delete all hosts.

-s Adds the host and associates the Internet address inet\_addr

with the Physical address eth\_addr. The Physical address is

given as 6 hexadecimal bytes separated by hyphens. The entry

is permanent.

eth\_addr Specifies a physical address.

if\_addr If present, this specifies the Internet address of the

interface whose address translation table should be modified.

If not present, the first applicable interface will be used.

Example:

> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.

> arp -a .... Displays the arp table.

* + 1. Изучите выходные данные.

Какая команда позволяет отобразить все записи в ARP-кэше?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Какая команда позволяет удалить все записи в ARP-кэше (очистить ARP-кэш)?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Какая команда позволяет удалить все записи в ARP-кэше для 192.168.1.11?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Введите **arp —a**, чтобы отобразить таблицу ARP.

C:\Users\User1> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.1 d4-8c-b5-ce-a0-c1 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

**Примечание**. В ОС Windows XP таблица ARP будет пустой (как показано ниже).

C:\Documents and Settings\User1> **arp -a**

No ARP Entries Found.

* + 1. Отправьте команду ping с PC-A на PC-B для динамического добавления записей в ARP-кэш.

C:\Documents and Settings\User1> **ping 192.168.1.2**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.2 00-50-56-be-f6-db dynamic

Назовите физический адрес узла с IP-адресом 192.168.1.2.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Настройте записи в ARP-кэше вручную.

Чтобы удалить записи из ARP-кэша, выполните команду **arp –d {inet-addr | \*}**. Можно удалить адреса по отдельности, указав соответствующие IP-адреса, либо стереть сразу все записи с помощью подстановочного знака \*.

Убедитесь в том, что ARP-кэш содержит следующие записи: шлюз по умолчанию R1 G0/1 (192.168.1.1), PC-B (192.168.1.2) и оба коммутатора (192.168.1.11 и 192.168.1.12).

* + 1. С PC-A отправьте эхо-запросы с помощью команды ping на все адреса в таблице адресов.
    2. Убедитесь в том, что все адреса добавлены в ARP-кэш. Если адрес в ARP-кэше отсутствует, отправьте команду ping на адрес назначения и проверьте, добавлен ли адрес в ARP-кэш.

C:\Users\User1> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.1 d4-8c-b5-ce-a0-c1 dynamic

192.168.1.2 00-50-56-be-f6-db dynamic

192.168.1.11 0c-d9-96-e8-8a-40 dynamic

192.168.1.12 0c-d9-96-d2-40-40 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

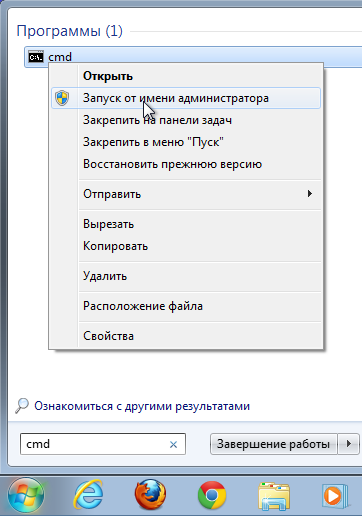
224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

* + 1. Откройте командную строку от имени администратора. Нажмите кнопку **Пуск** и в поле *Найти программы и файлы* введите **cmd**. Когда появится значок **cmd**, нажмите на него правой кнопкой мыши и выберите параметр **Запуск от имени администратора**. Нажмите кнопку **Да**, чтобы разрешить этой программе вносить изменения.

**Примечание**. Пользователям Windows XP для изменения записей в ARP-кэше права администратора не требуются.



* + 1. В окне командной строки администратора введите **arp –d \***. Эта команда удалит все записи из ARP-кэша. Убедитесь в том, что все записи из ARP-кэша удалены. Для этого в командной строке введите **arp –a**.

C:\windows\system32> **arp –d \***

C:\windows\system32> **arp –a**

No ARP Entries Found.

* + 1. Подождите несколько минут. Протокол поиска соседей Neighbor Discovery снова начинает заполнять ARP-кэш.

C:\Users\User1> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.255 ff-ff-ff-ff-ff-ff static

**Примечание**. В Windows XP протокол Neighbor Discovery не работает.

* + 1. С PC-A отправьте команду ping на PC-B (192.168.1.2) и коммутаторы (192.168.1.11 и 192.168.1.12), чтобы добавить записи ARP. Убедитесь в том, что все записи ARP добавлены в кэш.

C:\Users\User1> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.2 00-50-56-be-f6-db dynamic

192.168.1.11 0c-d9-96-e8-8a-40 dynamic

192.168.1.12 0c-d9-96-d2-40-40 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

* + 1. Запишите физический адрес коммутатора S2.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Чтобы удалить отдельную запись в ARP-кэше, введите команду **arp- d inet-addr**. Чтобы удалить запись ARP для коммутатора S2, в командной строке введите **arp -d 192.168.1.12**.

C:\windows\system32> **arp –d 192.168.1.12**

* + 1. Чтобы проверить, удалена ли запись ARP для коммутатора S2 из ARP-кэша, введите **arp –a.**

C:\Users\User1> **arp –a**

Interface: 192.168.1.3 --- 0xb

Internet Address Physical Address Type

192.168.1.2 00-50-56-be-f6-db dynamic

192.168.1.11 0c-d9-96-e8-8a-40 dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

* + 1. Чтобы добавить отдельную запись в ARP-кэш, введите команду **arp –s *inet\_addr mac\_addr***. В данном примере будут использоваться IP- и MAC-адреса для коммутатора S2. Используйте MAC-адрес, записанный в шаге Ж.

C:\windows\system32> **arp –s 192.168.1.12 0c-d9-96-d2-40-40**

* + 1. Запись ARP для коммутатора S2 должна добавиться в кэш.

1. Использование команды show arp в IOS

В Cisco IOS ARP-кэш маршрутизаторов и коммутаторов можно также отображать с помощью команд **show arp** или **show ip arp**.

* 1. Отобразите записи ARP на маршрутизаторе R1.

R1# **show arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.1 - d48c.b5ce.a0c1 ARPA GigabitEthernet0/1

Internet 192.168.1.2 0 0050.56be.f6db ARPA GigabitEthernet0/1

Internet 192.168.1.3 0 0050.56be.768c ARPA GigabitEthernet0/1

R1#

Обратите внимание на то, что первая запись интерфейса маршрутизатора G0/1 (шлюз по умолчанию для локальной сети) не имеет срока жизни. Срок жизни — это количество минут (мин), на протяжении которых запись содержалась в ARP-кэше. Для других записей это значение увеличивается. Протокол обнаружения соседей Neighbor Discovery заполняет записи IP- и МАС-адресов на PC-A и PC-B.

* 1. Добавьте записи ARP на маршрутизатор R1.

Записи ARP можно добавлять в ARP-таблицу маршрутизатора, отправляя команду ping на другие устройства.

* + 1. Отправьте команду ping на коммутатор S1.

R1# **ping 192.168.1.11**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms

* + 1. Убедитесь в том, что запись ARP для коммутатора S1 добавлена в таблицу ARP маршрутизатора R1.

R1# **show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.1 - d48c.b5ce.a0c1 ARPA GigabitEthernet0/1

Internet 192.168.1.2 6 0050.56be.f6db ARPA GigabitEthernet0/1

Internet 192.168.1.3 6 0050.56be.768c ARPA GigabitEthernet0/1

Internet 192.168.1.11 0 0cd9.96e8.8a40 ARPA GigabitEthernet0/1

R1#

* 1. Отобразите записи ARP на коммутаторе S1.

S1# **show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.1 46 d48c.b5ce.a0c1 ARPA Vlan1

Internet 192.168.1.2 8 0050.56be.f6db ARPA Vlan1

Internet 192.168.1.3 8 0050.56be.768c ARPA Vlan1

Internet 192.168.1.11 - 0cd9.96e8.8a40 ARPA Vlan1

S1#

* 1. Добавьте записи ARP на коммутатор S1.

Записи ARP можно также добавлять в ARP-таблицу коммутатора, отправляя команду ping на другие устройства.

* + 1. С коммутатора S1 отправьте команду ping на коммутатор S2.

S1# **ping 192.168.1.12**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms

* + 1. Убедитесь в том, что запись ARP для коммутатора S2 добавлена в таблицу ARP коммутатора S1.

S1# **show ip arp**

Protocol Address Age (min) Hardware Addr Type Interface

Internet 192.168.1.1 5 d48c.b5ce.a0c1 ARPA Vlan1

Internet 192.168.1.2 11 0050.56be.f6db ARPA Vlan1

Internet 192.168.1.3 11 0050.56be.768c ARPA Vlan1

Internet 192.168.1.11 - 0cd9.96e8.8a40 ARPA Vlan1

Internet 192.168.1.12 2 0cd9.96d2.4040 ARPA Vlan1

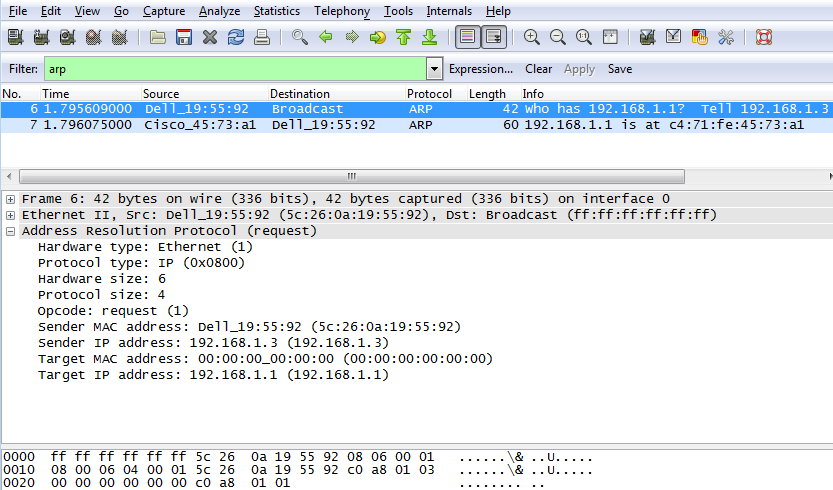
S1#

1. Анализ обмена сообщениями ARP с помощью программы Wireshark

В части 4 вам предстоит изучить обмен сообщениями ARP, используя программу Wireshark для их захвата и оценки. Кроме того, вы проанализируете задержки сети, вызванные обменом сообщениями ARP между устройствами.

* 1. Настройте программу Wireshark для захвата пакетов.
     1. Запустите программу Wireshark.
     2. Выберите сетевой интерфейс, который будете использовать для захвата сообщений ARP.
  2. Захватите и оцените сообщения ARP.
     1. Начните захват пакетов в программе Wireshark. Воспользуйтесь фильтром и отобразите только пакеты ARP.
     2. Очистите ARP-кэш, набрав в командной строке команду **arp –d \***.
     3. Убедитесь в том, что ARP-кэш очищен.
     4. Отправьте команду ping на шлюз по умолчанию с помощью команды **ping 192.168.1.1**.
     5. После отправки команды ping на шлюз по умолчанию остановите захват данных программой Wireshark.
     6. В захваченных данных найдите сообщения ARP в панели сведений о пакетах.

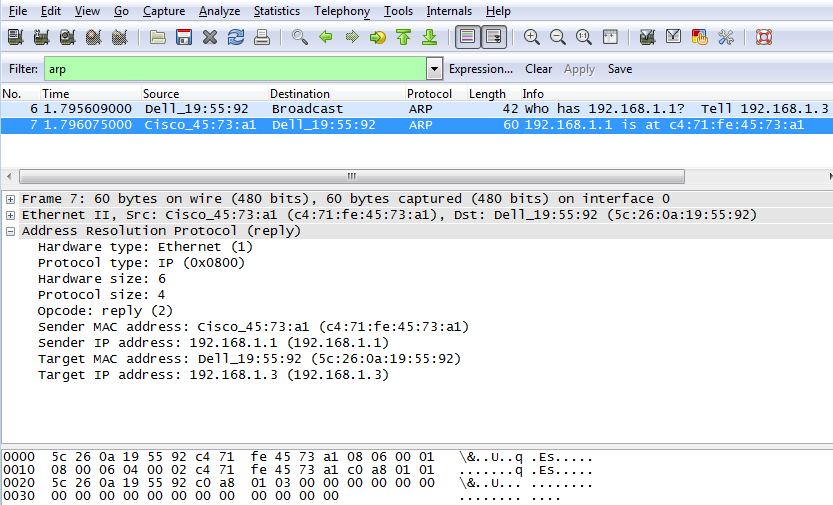
Какой пакет ARP был первым? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Внесите в приведенную ниже таблицу данные первого захваченного пакета ARP.

|  |  |
| --- | --- |
| Поле | Значение |
| **MAC-адрес отправителя** |  |
| **IP-адрес отправителя** |  |
| **MAC-адрес назначения** |  |
| **IP-адрес назначения** |  |

Какой пакет ARP был вторым? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_



Внесите в приведенную ниже таблицу данные второго захваченного пакета ARP.

|  |  |
| --- | --- |
| Поле | Значение |
| **MAC-адрес отправителя** |  |
| **IP-адрес отправителя** |  |
| **MAC-адрес назначения** |  |
| **IP-адрес назначения** |  |

* 1. Проанализируйте задержки сети, вызванные ARP.
     1. Очистите записи ARP на PC-A.
     2. Начните захват данных программой Wireshark.
     3. Отправьте команду ping на коммутатор S2 (192.168.1.12). Отправка команды ping после первого эхо-запроса должна быть успешной.

**Примечание**. Если все эхо-запросы успешны, необходимо перезагрузить коммутатор S1, чтобы просмотреть задержки сети из-за ARP.

C:\Users\User1> **ping 192.168.1.12**

Request timed out.

Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Reply from 192.168.1.12: bytes=32 time=2ms TTL=255

Ping statistics for 192.168.1.12:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

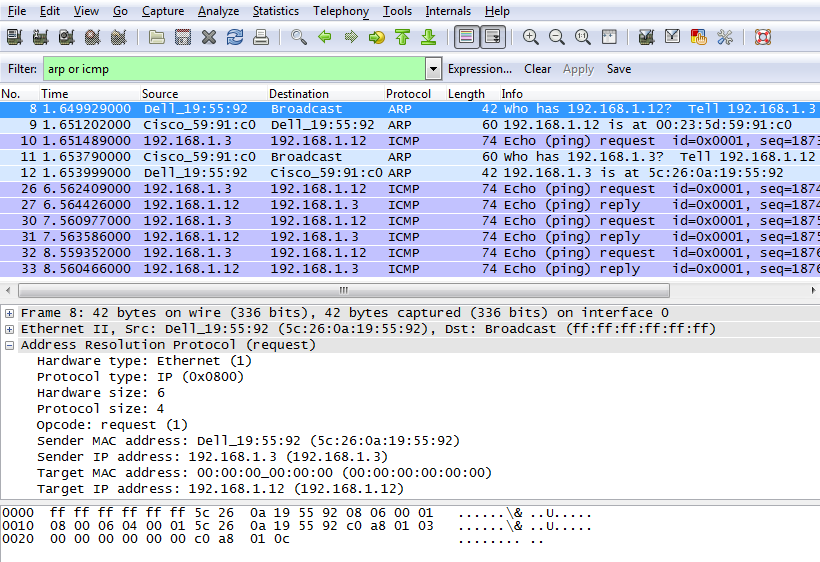
Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 3ms, Average = 2ms

* + 1. После отправки команды ping остановите захват данных программой Wireshark. Воспользуйтесь фильтром программы Wireshark и отобразите только пакеты ARP. В поле **Filter:** (Фильтр) программы Wireshark введите **arp** или **icmp**.
    2. Изучите данные, захваченные Wireshark. В данном примере кадр 10 — это первый ICMP-запрос, отправленный с PC-A на коммутатор S1. Поскольку для коммутатора S1 нет записи ARP, на IP-адрес управления коммутатора S1 был отправлен ARP-запрос на получение МАС-адреса. В процессе обмена данными ARP отправка команды ping не получила отклик за отведенное время (кадры 8–12).

После добавления записи ARP для коммутатора S1 в ARP-кэш последние три обмена данными ICMP были успешны, о чем свидетельствуют кадры 26, 27 и 30–33.

Как показано в захвате данных Wireshark, ARP — это яркий пример компромисса с точки зрения производительности. При отсутствии кэша протокол ARP должен непрерывно запрашивать трансляцию адресов каждый раз при помещении кадра в сеть. В этом случае для установления связи прибавляется время ожидания, что может вызвать перегрузку локальной сети.



1. Вопросы для повторения
   1. Как и когда удаляются статические записи ARP?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Зачем добавить статические записи ARP в кэш?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. Если ARP-запросы способны вызывать задержки сети, почему не рекомендуется снимать ограничения на время хранения записей ARP?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Сводная таблица по интерфейсам маршрутизаторов

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Сводная таблица по интерфейсам маршрутизаторов | | | | |
| Модель маршрутизатора | Интерфейс Ethernet № 1 | Интерфейс Ethernet № 2 | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Примечание**. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса. | | | | |