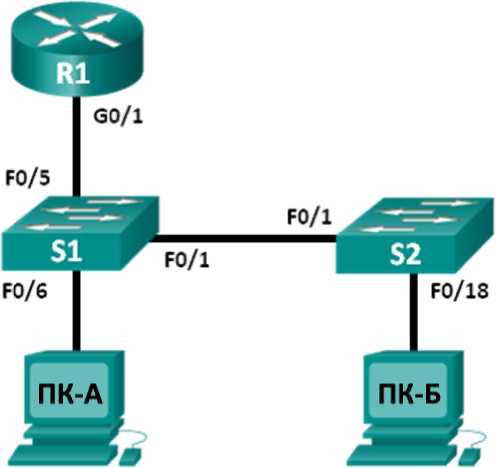
**Лабораторная работа**

**Анализ работы протокола ARP**

**Топология**



**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Основной шлюз** |
| 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 |
| ПК-А | Сетевой адаптер | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |
| ПК-Б | Сетевой адаптер | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |

**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

**Общие сведения**

Протокол разрешения адресов (ARP) используется для сопоставления адреса сетевого уровня (IP-адрес) с физическим адресом канального уровня (MAC-адрес). В кадре, помещаемом в сеть, должен содержаться MAC-адрес узла назначения. Для динамического определения MAC-адреса узла назначения по локальной сети отправляется широковещательный ARP-запрос. Узел, которому присвоен IP-адрес назначения, отвечает на этот запрос, и его MAC-адрес записывается в ARP-кэш. Каждый узел в локальной сети имеет собственный ARP-кэш (область ОЗУ, где хранятся результаты выполненных ARP-запросов). Таймер ARP-кэша удаляет записи ARP, которые не использовались в течение заданного промежутка времени (время жизни).

ARP — пример компромисса производительности. Если бы кэш отсутствовал, протокол ARP должен был бы каждый раз запрашивать сопоставление адресов, перед помещением кадра в сеть. И при установлении соединения всегда добавлялось бы время ожидания ответа, что вызвало бы увеличение трафика в локальной сети. В другом случае, использование неограниченного времени жизни записей ARP-кэша могло привести к ошибкам из-за устройств, которые выходят из сети или динамически изменяют сетевой адрес.

Протокол ARP может создавать уязвимости в системе безопасности сети. Злоумышленники используют ARP-спуфинг, или «отравление» ARP-кэша, для распространения в сети фальшивых МАС-адресов. Злоумышленник отвечает на ARP-запрос фальшивым MAC-адресом узла, вследствие чего кадры передаются на ложный адрес назначения. Одним из способов предотвращения подобных атак является использование статических записей ARP-кэша. Кроме того, для предотвращения несанкционированного доступа к сети со стороны злоумышленников, на устройствах Cisco можно настроить список допустимых МАС-адресов.

В данной лабораторной работе необходимо изучить таблицу ARP с помощью команд **arp** в ОС Windows и **show arp** на устройствах Cisco.

Кроме того, научиться очищать ARP-кэш и добавлять статические записи ARP.

**Примечание**. В зависимости от модели устройства и версии Cisco IOS доступные команды, синтаксис и вывод их результатов может отличаться от приведенных в лабораторной работе примеров.

**Примечание**. Проверьте удаление всех настроек и файлов загрузочной конфигурации на устройствах.

**Необходимые ресурсы**

* 1 маршрутизатор Cisco с универсальным образом Cisco IOS
* 2 коммутатора Cisco, с универсальным образом Cisco IOS
* Консольные кабели для настройки устройств Cisco IOS через консольные порты
* 2 компьютера с ОС Windows, с установленными программами эмулятора терминала и Wireshark
* Кабели Ethernet для создания сети в соответствии с заданной Топологией

# Часть 1: Создание и настройка сети

**Шаг 1: Соберите сеть в соответствии с Топологией.**

**Шаг 2: Настройте IP-адреса устройств в соответствии с Таблицей адресации.**

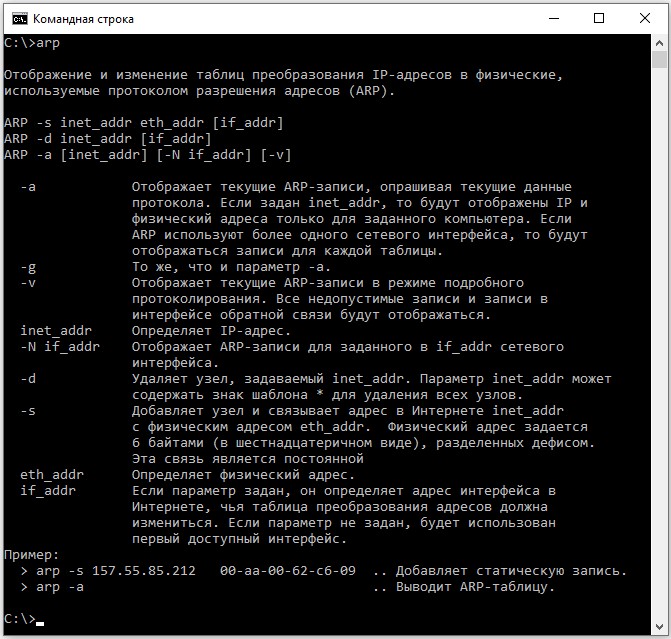
**Шаг 3: Проверьте соединение, отправив из окна командной строки компьютера ПК-Б с помощью команды ping эхо-запросы на все устройства.**

# Часть 2: Использование команды arp ОС Windows

Команда **arp** ОС Windows предназначена для просмотра и изменения содержимого ARP-кэша.

**Шаг 1: Просмотр содержимого ARP-кэша.**

1. Откройте окно командной строки на компьютере ПК-А и введите:



1. Проанализируйте полученные данные.

Какой формат команды **arp** отображает все записи ARP-кэша?

|  |
| --- |
| arp -a |

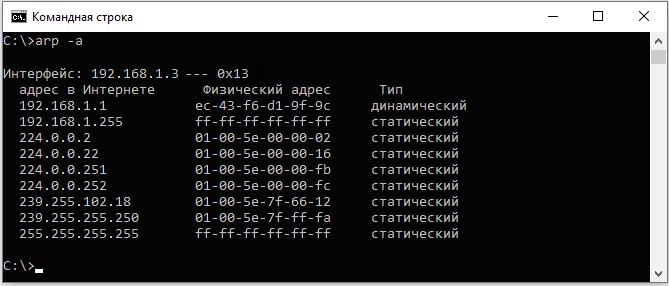
Какой формат команды **arp** удаляет все записи ARP-кэша?

|  |
| --- |
| arp -d |

Какой формат команды **arp** удаляет записи ARP-кэша для IP-адреса 192.168.1.11?

|  |
| --- |
| apr -d 192.168.1.11 |

1. Введите

для отображения таблицы ARP.

**Примечание**. В ОС Windows XP таблица ARP может быть пустой.

1. Из окна командной строки компьютера ПК-А с помощью команды **ping** отправьте эхо-запрос на IP-адрес компьютера ПК-Б для динамического добавления записи в ARP-кэш.

Запишите физический адрес компьютера ПК-Б.

|  |
| --- |
| 08-00-27-e3-cf-ea |

**Шаг 2: Ручная настройка записей в ARP-кэше.**

Для удаления записей из ARP-кэша, выполните команду:

**arp -d {ip-адрес | \*}**

Можно удалить адреса по отдельности, указав соответствующий IP-адрес, или удалить все записи сразу с помощью группового символа **\***.

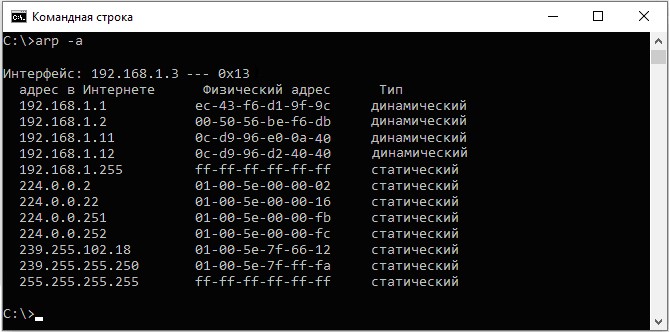
Проверьте, что ARP-кэш содержит записи для следующих IP-адресов:

основного шлюза R1 G0/1 (192.168.1.1), компьютера ПК-Б (192.168.1.2) и коммутаторов S1 (192.168.1.11) и S2 (192.168.1.12).

1. Из окна командной строки компьютера ПК-А с помощью команды

**ping** отправьте эхо-запросы на все IP-адреса в **Таблице адресации**.

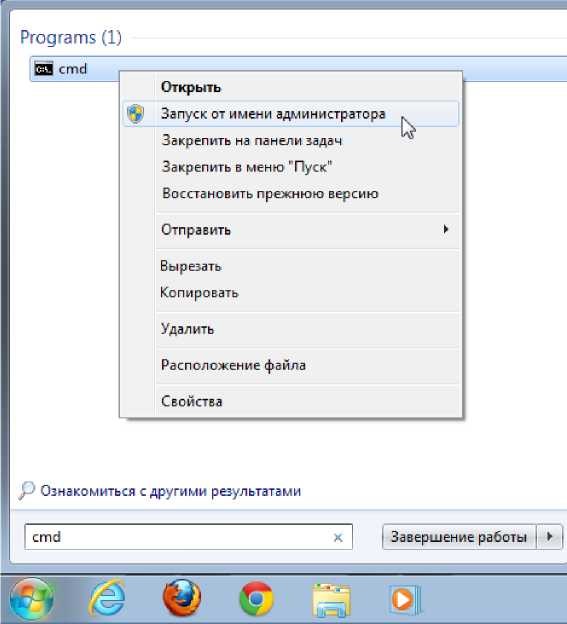
1. Убедитесь, что записи для всех IP-адресов добавлены в ARP-кэш. Если запись для IP-адреса в ARP-кэше отсутствует, с помощью команды **ping** отправьте эхо-запрос на данный IP-адрес и посмотрите, добавилась ли запись для IP-адреса в ARP-кэш.



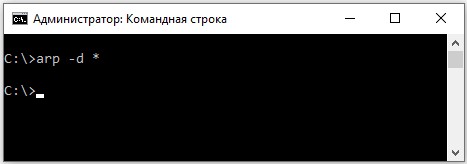
1. Откройте командную строку от имени администратора. В поле **Найти программы и файлы** введите **cmd**

Щелкните правой кнопкой мыши на появившемся значке **cmd**, и выберите в контекстном меню пункт **Запуск от имени администратора**.

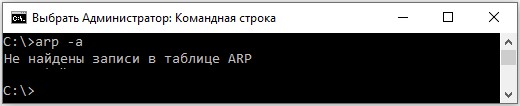
**Примечание**. Пользователям ОС Windows XP не нужны права администратора для изменения записей в ARP-кэше.



1. В окне командной строки введите



Данная команда удаляет все записи из ARP-кэша. Убедитесь, что все записи из ARP-кэша удалены. Для этого в командной строке введите:

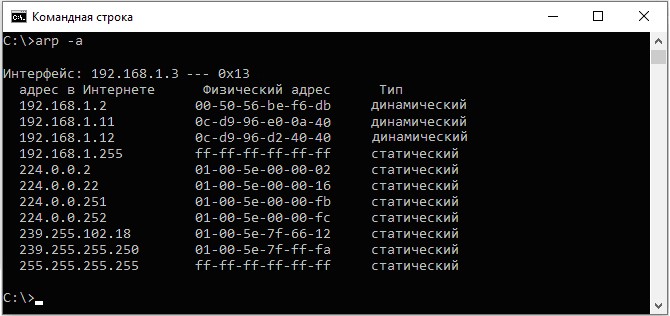


1. Подождите несколько минут. Протокол обнаружения соседей снова

начнет заполнять ARP-кэш.

**Примечание**. В ОС Windows XP протокол обнаружения соседей может не работать.

1. Из окна командной строки компьютера ПК-А с помощью команды **ping** отправьте эхо-запросы на IP-адрес компьютера ПК-Б (192.168.1.2) и на IP-адреса виртуальных интерфейсов коммутаторов S1 (192.168.1.11) и S2 (192.168.1.12), чтобы добавить записи ARP. Проверьте, что все записи ARP добавлены в ARP-кэш.



1. Запишите физический адрес коммутатора S2.

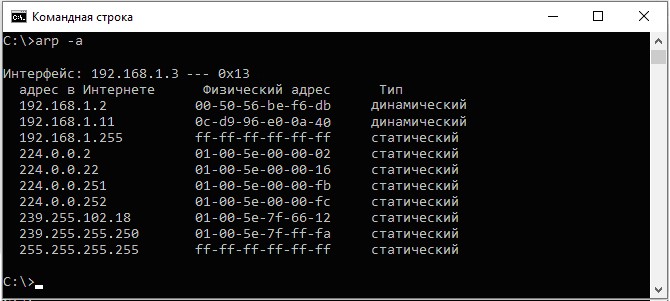
|  |
| --- |
| 00-08-30-47-e2-c0 |

1. Введите в командной строке **arp -d ip-адрес**

для удаления отдельной записи ARP. Введите в командной строке **arp -d 192.168.1.12**

для удаления записи ARP для коммутатора S2.

1. Проверьте, удалена ли запись ARP для коммутатора S2 из ARP-кэша:

**j**. Введите команду:

**arp -s ip-адрес mac-адрес**

для добавления отдельной статической записи в ARP-кэш.

Используйте IP- и MAC-адрес (записанный в шаге **g**) коммутатора S2 **arp -s 192.168.1.12 0c-d9-96-d2-40-40**

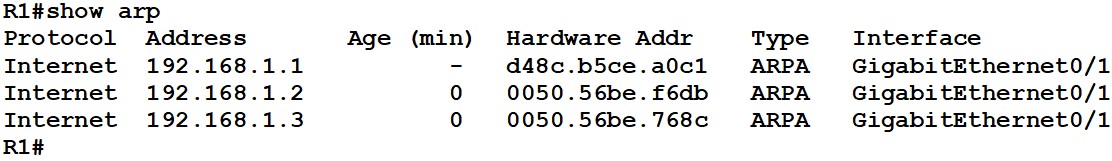
**k**. Проверьте, что статическая запись для коммутатора S2 добавилась

в ARP-кэш.

# Часть 3. Использование команды show arp на устройствах Cisco

Команды **show arp** или **show ip arp** отображают содержимое таблицы ARP на устройствах Cisco.

**Шаг 1. Просмотр содержимого таблицы ARP на маршрутизаторе R1.**

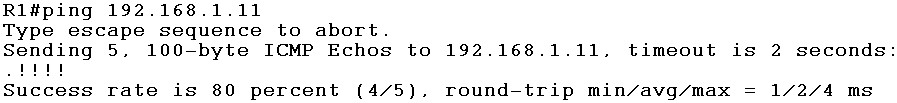


Первая запись в таблице ARP для интерфейса G0/1 маршрутизатора R1 (основной шлюз в локальной сети) не имеет срока жизни. Срок жизни — это количество минут, в течение которых запись удерживается в ARP-кэше. Для других записей это значение будет увеличиваться.

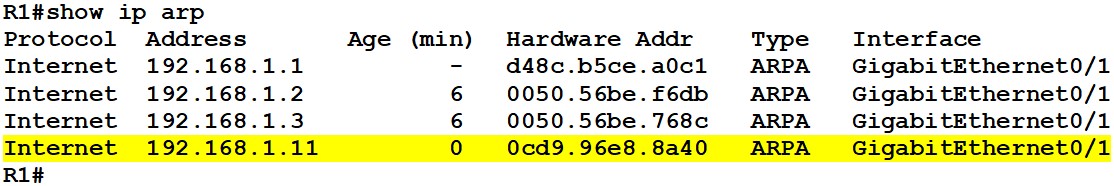
**Шаг 2. Добавьте записи в таблицу ARP на маршрутизаторе R1.**

Отправляя из командной строки с помощью команды **ping** эхо-запросы на другие устройства, можно добавлять записи в ARP-таблицу маршрутизатора.

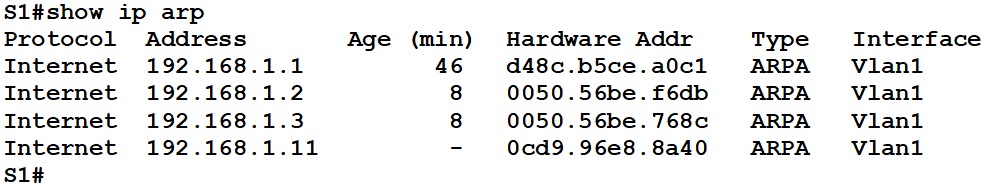
1. Отправьте с помощью команды **ping** эхо-запрос на IP-адрес виртуального интерфейса коммутатора S1.



1. Проверьте, что запись ARP для IP-адреса виртуального интерфейса коммутатора S1 добавлена в ARP-таблицу маршрутизатора R1.



**Шаг 3: Просмотрите содержимое таблицы ARP на коммутаторе S1.**

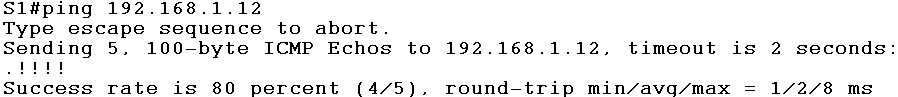


**Шаг 4: Добавьте записи в таблицу ARP на коммутаторе**

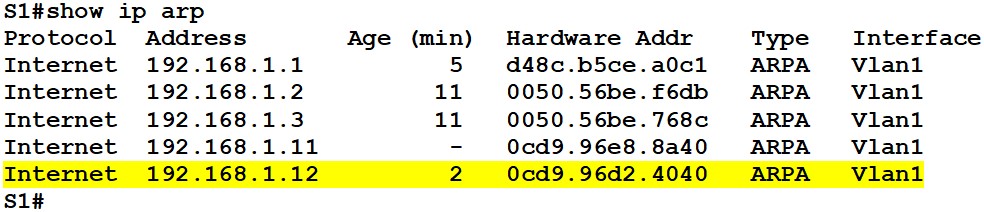
**S1.**

Отправляя из командной строки с помощью команды **ping** эхо-запросы на другие устройства, можно добавлять записи в ARP-таблицу коммутатора.

1. Отправьте с помощью команды **ping** эхо-запрос на IP-адрес виртуального интерфейса коммутатор S2.



1. Проверьте, что запись для IP-адреса виртуального интерфейса коммутатора S2 добавлена в ARP-таблицу коммутатора S1.



# Часть 4. Анализ сообщений ARP с помощью программы Wireshark

В этой части необходимо проанализировать обмен сообщениями ARP, используя для их захвата и анализа программу Wireshark. А также оценить задержки сети, вызванные обменом ARP-сообщениями между устройствами.

**Шаг 1. Настройте программу Wireshark для захвата кадров.**

1. Запустите на компьютере ПК-А программу Wireshark.
2. Выберите соответствующий сетевой интерфейс компьютера ПК-А,

который будет использоваться для захвата сообщений ARP.

**Шаг 2. Захватите и проанализируйте сообщения ARP.**

1. Начните захват кадров в программе Wireshark. Используйте

фильтр, для отображения кадров, содержащих только сообщения ARP.

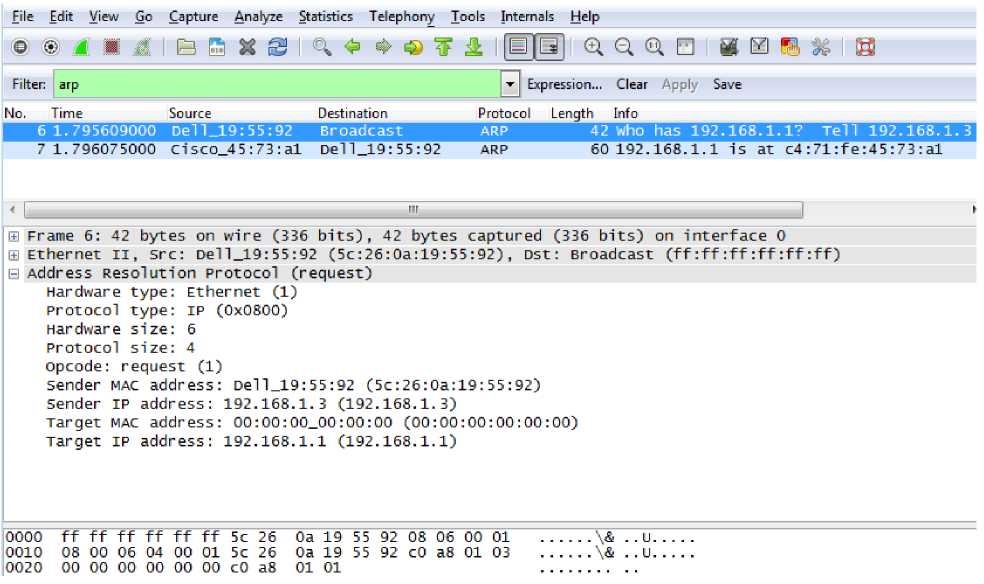
1. Очистите ARP-кэш с помощью команды:

**arp -d \*.**

1. Проверьте, что ARP-кэш очищен.
2. Из окна командной строки с помощью команды **ping** отправьте

эхо-запрос на IP-адрес основного шлюза.

1. Остановите захват кадров программой Wireshark.
2. В Панели сведений о захваченных кадрах, найдите кадры, содержащие сообщения ARP.



Какой кадр, содержащий ARP был захвачен первым?

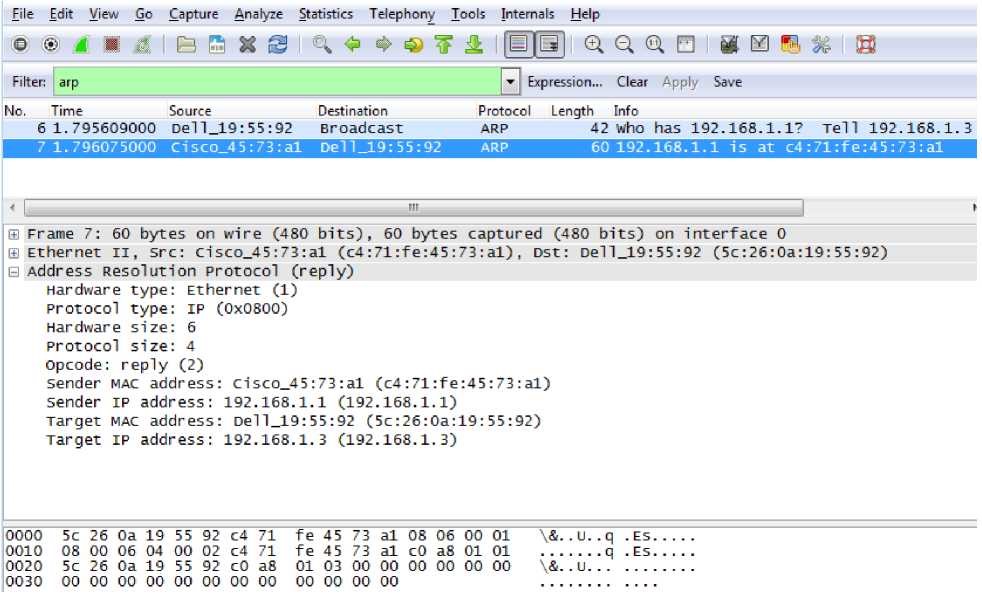
|  |
| --- |
| Broadcast ARP who has 192.168.1.1 |

Заполните таблицу данными из первого захваченного кадра, содержащего сообщение ARP.

|  |  |
| --- | --- |
| **Поле** | **Значение поля** |
| MAC-адрес источника | 08:00:27:20:52:ed |
| IP-адрес источника | 192.168.1.3 |
| MAC-адрес назначения | 00:00:00:00:00:00 |
| IP-адрес назначения | 192.168.1.1 |

Какой кадр, содержащий ARP был захвачен вторым?

|  |
| --- |
| ARP 192.168.1.1 is at a0:ec:f9:67:68:59 |



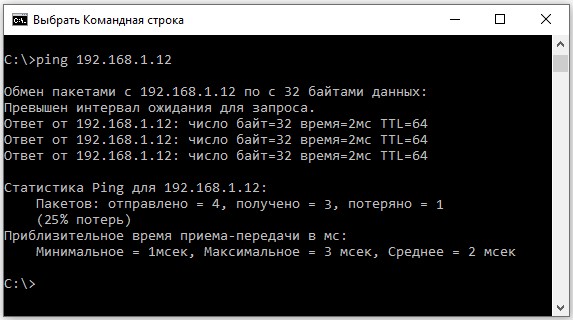
Заполните таблицу данными из второго захваченного кадра, содержащего сообщение ARP.

|  |  |
| --- | --- |
| **Поле** | **Значение поля** |
| MAC-адрес источника | a0:ec:f9:67:68:59 |
| IP-адрес источника | 192.168.1.11 |
| MAC-адрес назначения | 08:00:27:20:52:ed |
| IP-адрес назначения | 192.168.1.1 |

**Шаг 3. Проанализируйте задержки сети, вызванные сообщениями ARP.**

1. Очистите ARP-кэш на компьютере ПК-А.
2. Начните захват кадров программой Wireshark.
3. С помощью команды **ping** отправьте эхо-запрос на IP-адрес виртуального интерфейса коммутатора S2 (192.168.1.12). Второй эхо-запрос, отправленный с помощью команды **ping**, должен быть полностью (0% потерь) успешным.

**Примечание**. Если первый эхо-запрос был полностью успешный, необходимо перезагрузить коммутатор S1, чтобы посмотреть задержки сети из-за ARP.

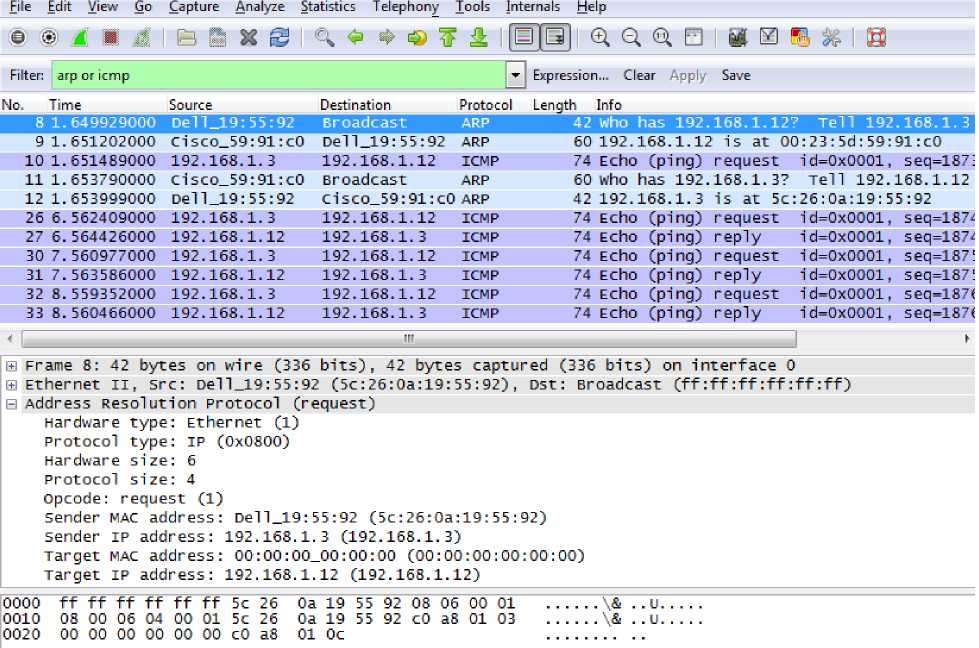


1. Остановите захват кадров программой Wireshark. Используйте

фильтр для отображения только данных протоколов ARP и ICMP.

1. Изучите захваченные кадры. В приведенном примере кадр **10** является первым ICMP-кадром, отправленным с компьютера ПК-Б на коммутатор S1. Т. к. для коммутатора S1 нет записи в ARP-кэше, на IP-адрес виртуального интерфейса коммутатора S1 был отправлен ARP-запрос для получения МАС-адреса. Во время обмена данными эхо-запрос, отправленный с помощью команды **ping**, не получил ответ за отведённое время (кадры **11**-**12**).

После добавления записи в ARP-кэш для IP-адреса виртуального интерфейса коммутатора S1, последние три обмена данными ICMP прошли успешно, что подтверждают кадры **26**, **27** и **30**-**33**.



# Вопросы на повторение

1. Когда удаляются статические записи из ARP-кэша?

|  |
| --- |
| При перезагрузке, при ручном удалении |

1. Зачем добавлять в ARP-кэш статические записи?

|  |
| --- |
| Для того чтобы не делать arp запрос |

1. Почему не следует снимать ограничения на время ожидания отклика для сообщений ARP?

|  |
| --- |
| Для того чтобы система не ждала ответа вечно при отсутствии устройства в сети |