

Лабораторная работа

Анализ работы протокола ARP

Топология

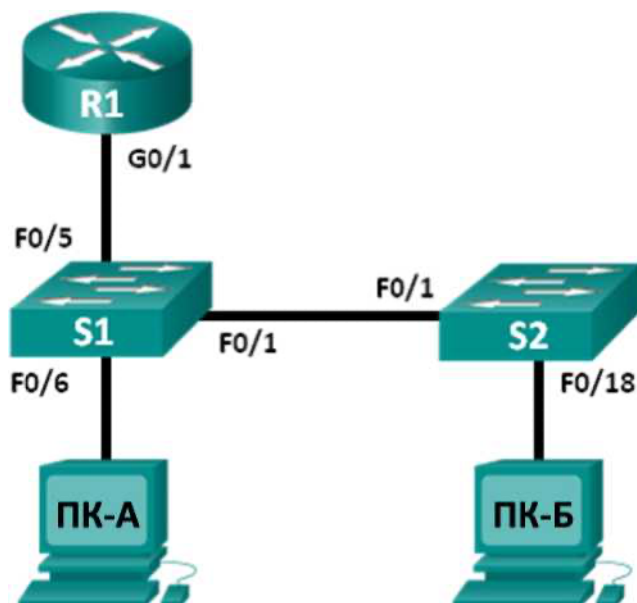


Таблица адресации

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 **MAC**-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 **MAC**-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.

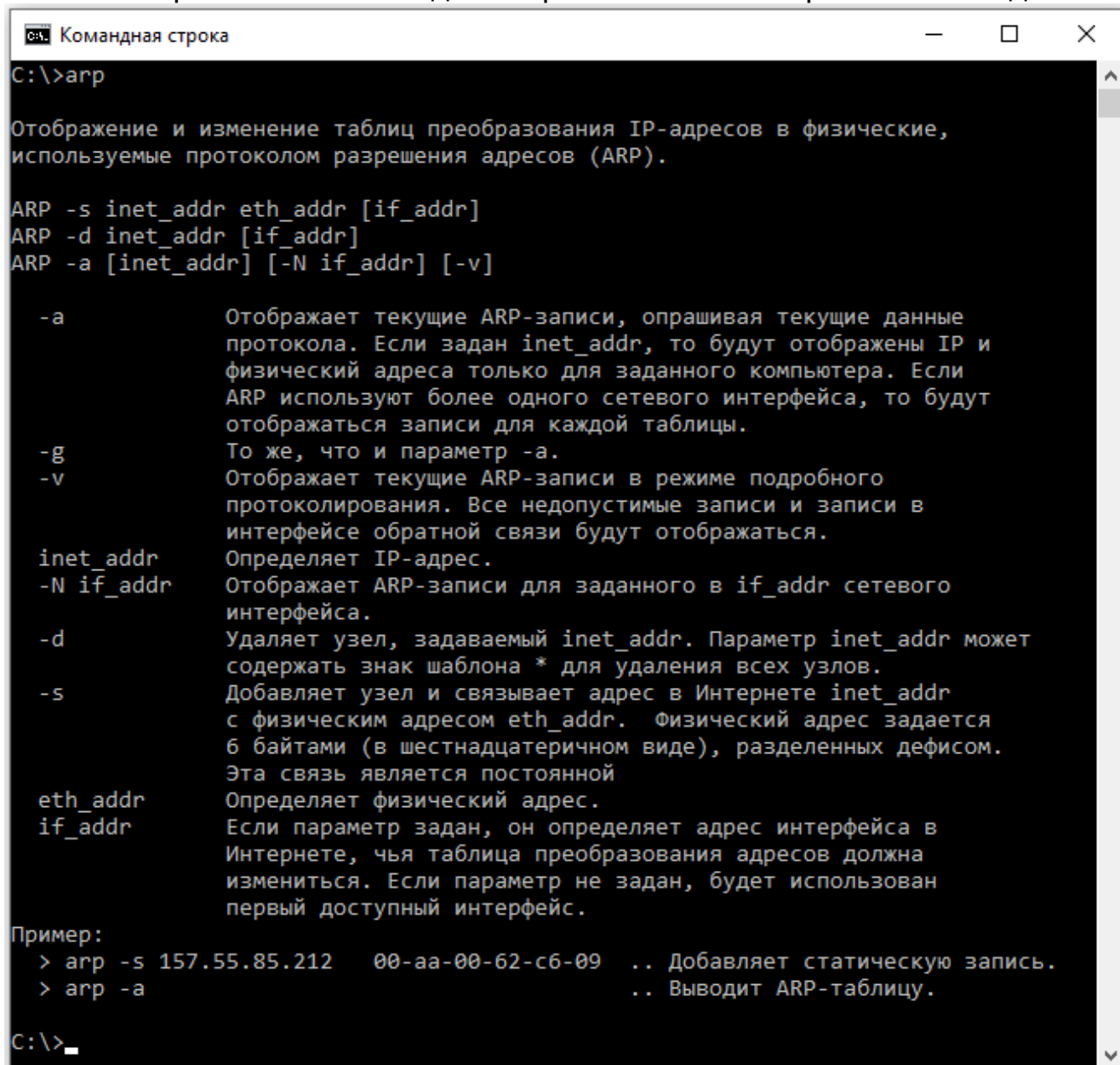
Шаг 3: Проверьте соединение, отправив из окна командной строки компьютера ПК-Б с помощью команды ping эхо-запросы на все устройства.

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.

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



```
C:\>arp

Отображение и изменение таблиц преобразования IP-адресов в физические,
используемые протоколом разрешения адресов (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Отображает текущие ARP-записи, опрашивая текущие данные
            протокола. Если задан inet_addr, то будут отображены IP и
            физический адреса только для заданного компьютера. Если
            ARP используют более одного сетевого интерфейса, то будут
            отображаться записи для каждой таблицы.
-g          То же, что и параметр -a.
-v          Отображает текущие ARP-записи в режиме подробного
            протоколирования. Все недопустимые записи и записи в
            интерфейсе обратной связи будут отображаться.
inet_addr   Определяет IP-адрес.
-N if_addr  Отображает ARP-записи для заданного в if_addr сетевого
            интерфейса.
-d          Удаляет узел, задаваемый inet_addr. Параметр inet_addr может
            содержать знак шаблона * для удаления всех узлов.
-s          Добавляет узел и связывает адрес в Интернете inet_addr
            с физическим адресом eth_addr. Физический адрес задается
            6 байтами (в шестнадцатеричном виде), разделенных дефисом.
            Эта связь является постоянной
eth_addr     Определяет физический адрес.
if_addr     Если параметр задан, он определяет адрес интерфейса в
            Интернете, чья таблица преобразования адресов должна
            измениться. Если параметр не задан, будет использован
            первый доступный интерфейс.

Пример:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .. Добавляет статическую запись.
> arp -a .. Выводит ARP-таблицу.

C:\>_
```

б. Проанализируйте полученные данные.

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

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

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

с. Введите

```
Командная строка
C:\>arp -a

Интерфейс: 192.168.1.3 --- 0x13
    адрес в Интернете      Физический адрес      Тип
192.168.1.1                ec-43-f6-d1-9f-9c      динамический
192.168.1.255              ff-ff-ff-ff-ff-ff      статический
224.0.0.2                  01-00-5e-00-00-02      статический
224.0.0.22                 01-00-5e-00-00-16      статический
224.0.0.251                01-00-5e-00-00-fb      статический
224.0.0.252                01-00-5e-00-00-fc      статический
239.255.102.18             01-00-5e-7f-66-12      статический
239.255.255.250            01-00-5e-7f-ff-fa      статический
255.255.255.255            ff-ff-ff-ff-ff-ff      статический

C:\>_
```

для отображения таблицы **ARP**.

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

d. 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.

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).

a. Из окна командной строки компьютера ПК-А с помощью команды **ping** отправьте эхо-запросы на все **IP**-адреса в **Таблице адресации**.

b. 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.

```
Командная строка
C:\>arp -a

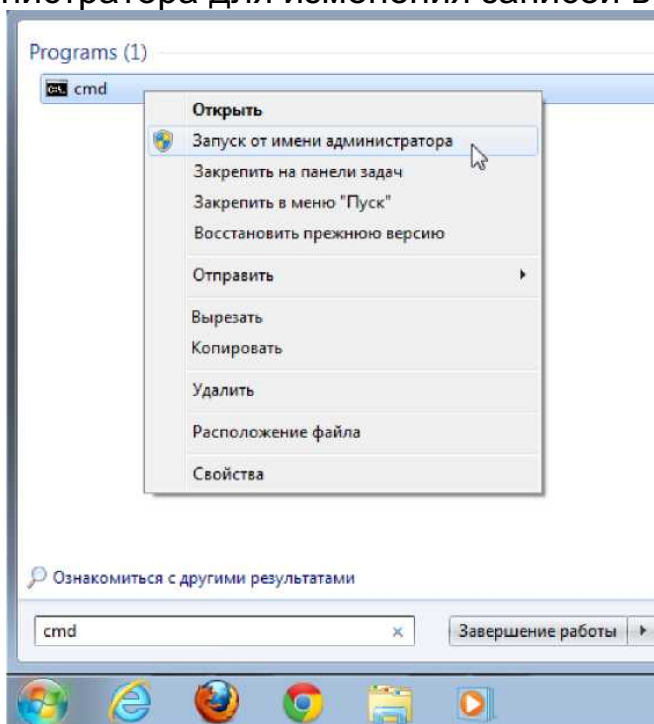
Интерфейс: 192.168.1.3 --- 0x13
    адрес в Интернете      Физический адрес      Тип
192.168.1.1                ec-43-f6-d1-9f-9c      динамический
192.168.1.2                00-50-56-be-f6-db      динамический
192.168.1.11              0c-d9-96-e0-0a-40      динамический
192.168.1.12              0c-d9-96-d2-40-40      динамический
192.168.1.255             ff-ff-ff-ff-ff-ff      статический
224.0.0.2                 01-00-5e-00-00-02      статический
224.0.0.22                01-00-5e-00-00-16      статический
224.0.0.251               01-00-5e-00-00-fb      статический
224.0.0.252               01-00-5e-00-00-fc      статический
239.255.102.18            01-00-5e-7f-66-12      статический
239.255.255.250           01-00-5e-7f-ff-fa      статический
255.255.255.255           ff-ff-ff-ff-ff-ff      статический

C:\>_
```

с. 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.

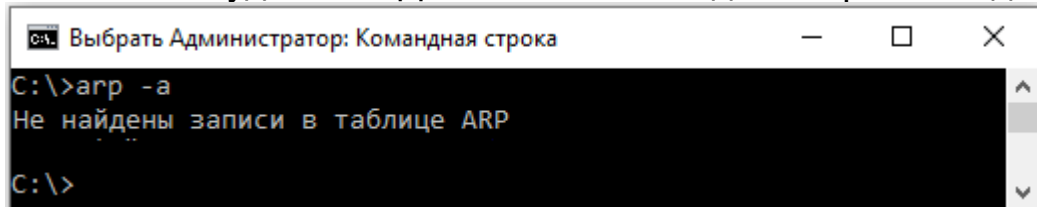


d. В окне командной строки введите

```
Администратор: Командная строка
C:\>arp -d *
C:\>_
```

Данная команда удаляет все записи из **ARP**-кэша. Убедитесь, что все

записи из **ARP**-кэша удалены. Для этого в командной строке введите:

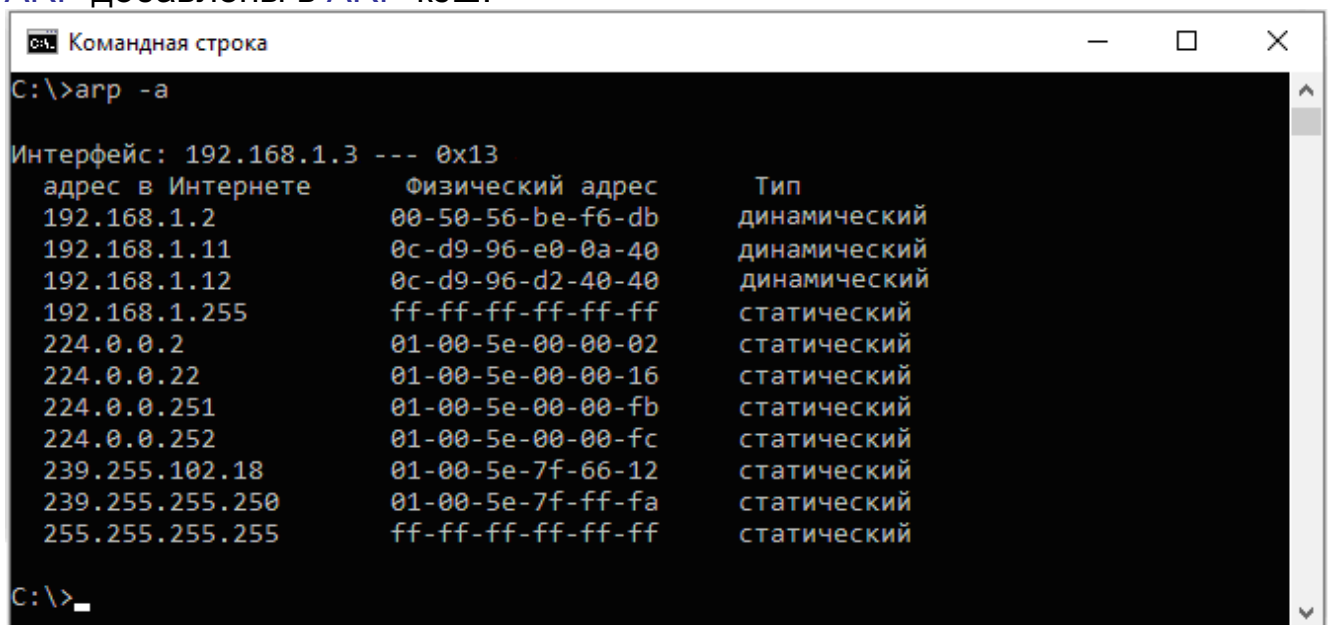


```
Выбрать Администратор: Командная строка
C:\>arp -a
Не найдены записи в таблице ARP
C:\>
```

е. Подождите несколько минут. Протокол обнаружения соседей снова начнет заполнять **ARP**-кэш.

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

ф. 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.



```
Командная строка
C:\>arp -a

Интерфейс: 192.168.1.3 --- 0x13
    адрес в Интернете      Физический адрес      Тип
192.168.1.2                00-50-56-be-f6-db     динамический
192.168.1.11               0c-d9-96-e0-0a-40     динамический
192.168.1.12               0c-d9-96-d2-40-40     динамический
192.168.1.255              ff-ff-ff-ff-ff-ff     статический
224.0.0.2                  01-00-5e-00-00-02     статический
224.0.0.22                 01-00-5e-00-00-16     статический
224.0.0.251                01-00-5e-00-00-fb     статический
224.0.0.252                01-00-5e-00-00-fc     статический
239.255.102.18             01-00-5e-7f-66-12     статический
239.255.255.250            01-00-5e-7f-ff-fa     статический
255.255.255.255            ff-ff-ff-ff-ff-ff     статический

C:\>_
```

г. Запишите физический адрес коммутатора **S2**.

h. 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**.

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


```
Командная строка
C:\>arp -a

Интерфейс: 192.168.1.3 --- 0x13
    адрес в Интернете      Физический адрес      Тип
192.168.1.2                00-50-56-be-f6-db     динамический
192.168.1.11               0c-d9-96-e0-0a-40     динамический
192.168.1.255              ff-ff-ff-ff-ff-ff     статический
224.0.0.2                  01-00-5e-00-00-02     статический
224.0.0.22                 01-00-5e-00-00-16     статический
224.0.0.251                01-00-5e-00-00-fb     статический
224.0.0.252                01-00-5e-00-00-fc     статический
239.255.102.18             01-00-5e-7f-66-12     статический
239.255.255.250            01-00-5e-7f-ff-fa     статический
255.255.255.255            ff-ff-ff-ff-ff-ff     статический

C:\>_
```

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.

```
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#
```

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.

a. Отправьте с помощью команды `ping` эхо-запрос на IP-адрес виртуального интерфейса коммутатора 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
```

b. Проверьте, что запись ARP для IP-адреса виртуального интерфейса коммутатора S1 добавлена в ARP-таблицу 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#
```

Шаг 3: Просмотрите содержимое таблицы 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#
```

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.

a. Отправьте с помощью команды **ping** эхо-запрос на **IP**-адрес виртуального интерфейса 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
```

b. Проверьте, что запись для **IP**-адреса виртуального интерфейса коммутатора **S2** добавлена в **ARP**-таблицу 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#
```

Часть 4. Анализ сообщений ARP с помощью программы Wireshark

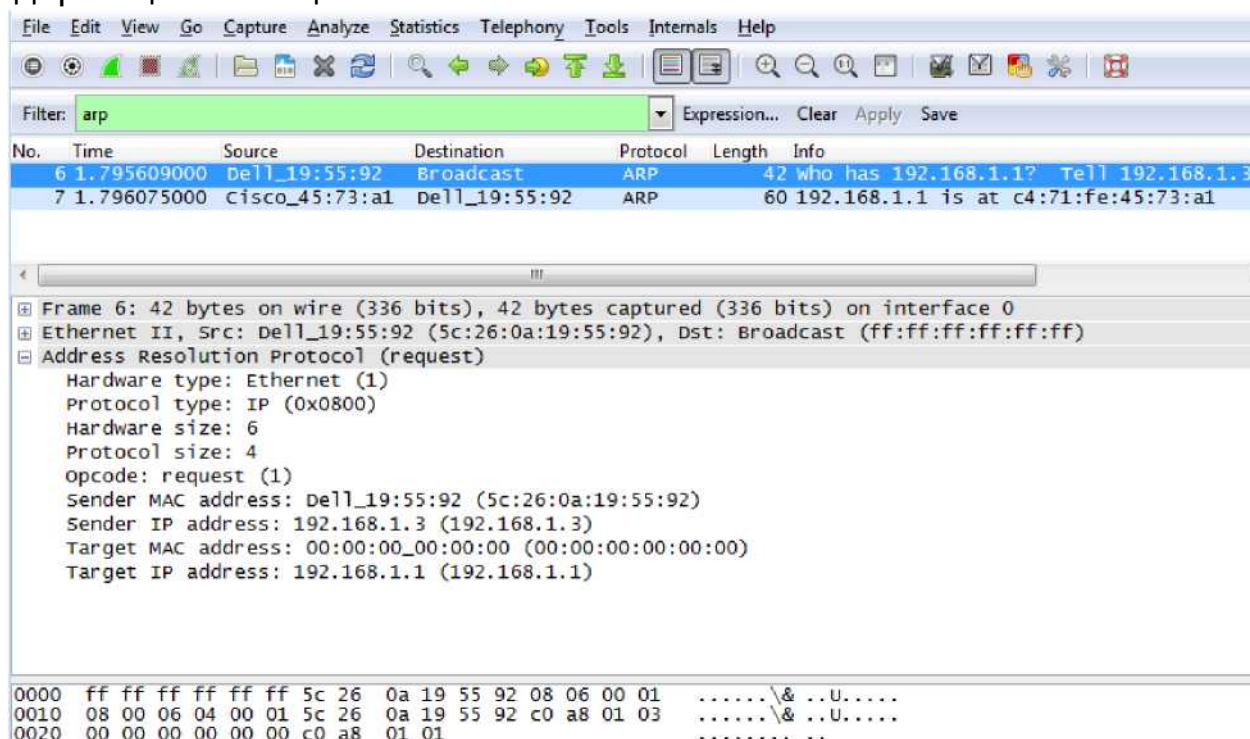
В этой части необходимо проанализировать обмен сообщениями **ARP**, используя для их захвата и анализа программу **Wireshark**. А также оценить задержки сети, вызванные обменом **ARP**-сообщениями между устройствами.

Шаг 1. Настройте программу Wireshark для захвата кадров.

- Запустите на компьютере ПК-А программу **Wireshark**.
- Выберите соответствующий сетевой интерфейс компьютера ПК-А, который будет использоваться для захвата сообщений **ARP**.

Шаг 2. Захватите и проанализируйте сообщения ARP.

- Начните захват кадров в программе **Wireshark**. Используйте фильтр, для отображения кадров, содержащих только сообщения **ARP**.
- Очистите **ARP**-кэш с помощью команды:
arp -d *
- Проверьте, что **ARP**-кэш очищен.
- Из окна командной строки с помощью команды **ping** отправьте эхо-запрос на **IP**-адрес основного шлюза.
- Остановите захват кадров программой **Wireshark**.
- В Панели сведений о захваченных кадрах, найдите кадры, содержащие сообщения **ARP**.

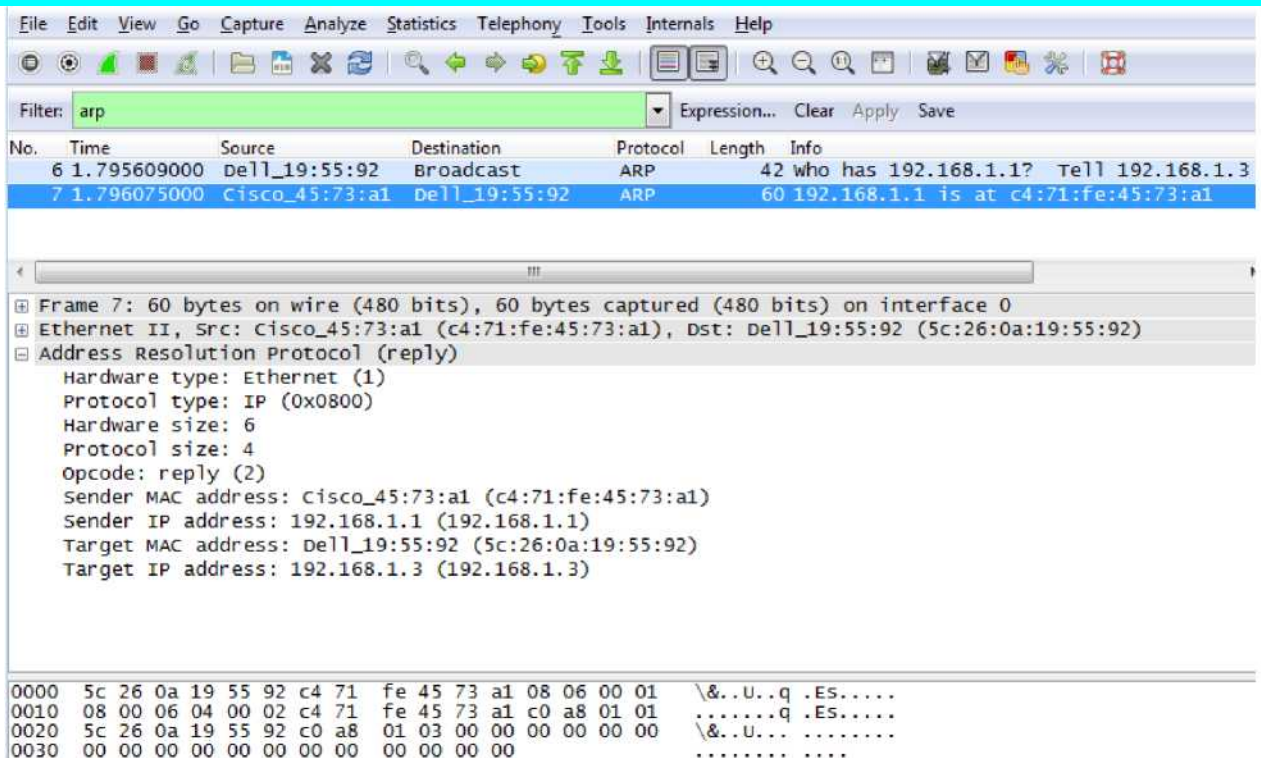


Какой кадр, содержащий **ARP** был захвачен первым?

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

Поле	Значение поля
MAC-адрес источника	
IP-адрес источника	
MAC-адрес назначения	
IP-адрес назначения	

Какой кадр, содержащий **ARP** был захвачен вторым?



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

Поле	Значение поля
MAC-адрес источника	
IP-адрес источника	
MAC-адрес назначения	
IP-адрес назначения	

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

- Очистите **ARP**-кэш на компьютере ПК-А.
- Начните захват кадров программой **Wireshark**.
- 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**.


```

C:\>ping 192.168.1.12

Обмен пакетами с 192.168.1.12 по 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 192.168.1.12: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.12: число байт=32 время=2мс TTL=64
Ответ от 192.168.1.12: число байт=32 время=2мс TTL=64

Статистика Ping для 192.168.1.12:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1
    (25% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 3 мсек, Среднее = 2 мсек

C:\>

```

d. Остановите захват кадров программой [Wireshark](#). Используйте фильтр для отображения только данных протоколов [ARP](#) и [ICMP](#).

e. 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 [MAC](#)-адреса. Во время обмена данными эхо-запрос, отправленный с помощью команды [ping](#), не получил ответ за отведенное 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.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
Filter: arp or icmp Expression... Clear Apply Save						
No.	Time	Source	Destination	Protocol	Length	Info
8	1.649929000	Dell_19:55:92	Broadcast	ARP	42	who has 192.168.1.12? Tell 192.168.1.3
9	1.651202000	Cisco_59:91:c0	Dell_19:55:92	ARP	60	192.168.1.12 is at 00:23:5d:59:91:c0
10	1.651489000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1874
11	1.653790000	Cisco_59:91:c0	Broadcast	ARP	60	who has 192.168.1.3? Tell 192.168.1.12
12	1.653999000	Dell_19:55:92	Cisco_59:91:c0	ARP	42	192.168.1.3 is at 5c:26:0a:19:55:92
26	6.562409000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1874
27	6.564426000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1874
30	7.560977000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1874
31	7.563586000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1874
32	8.559352000	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=1874
33	8.560466000	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1874

Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
Ethernet II, Src: Dell_19:55:92 (5c:26:0a:19:55:92), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IP (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: Dell_19:55:92 (5c:26:0a:19:55:92)						
Sender IP address: 192.168.1.3 (192.168.1.3)						
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.1.12 (192.168.1.12)						

0000	ff ff ff ff ff ff 5c 26 0a 19 55 92 08 06 00 01\& ..U.....
0010	08 00 06 04 00 01 5c 26 0a 19 55 92 c0 a8 01 03\& ..U.....
0020	00 00 00 00 00 00 c0 a8 01 0c

Вопросы на повторение

1. Когда удаляются статические записи из ARP-кэша?

2. Зачем добавлять в ARP-кэш статические записи?

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