Практическая работа по дисциплине  
“Сети и телекоммуникации”

№5

Выполнил:

Студент группы 606-12  
Демьянцев В.В.

# Задание “9.1.3”

## Часть 1: Сбор информации PDU для локальной сети связи

a.     Нажмите на **172.16.31.5**и откройте окно **Command Prompt (Командная строка)**.

б.     ведите команду **ping 172.16.31.2.**

в.     Перейдите в режим моделирования и повторите команду **ping 172.16.31.2**. Единица данных протокола (PDU) будет показана рядом с **172.16.31.5.**

г.     Нажмите единицу данных протокола (PDU) и запишите следующие данные на вкладке **OSI Model** и **Outbound PDU Layer**.

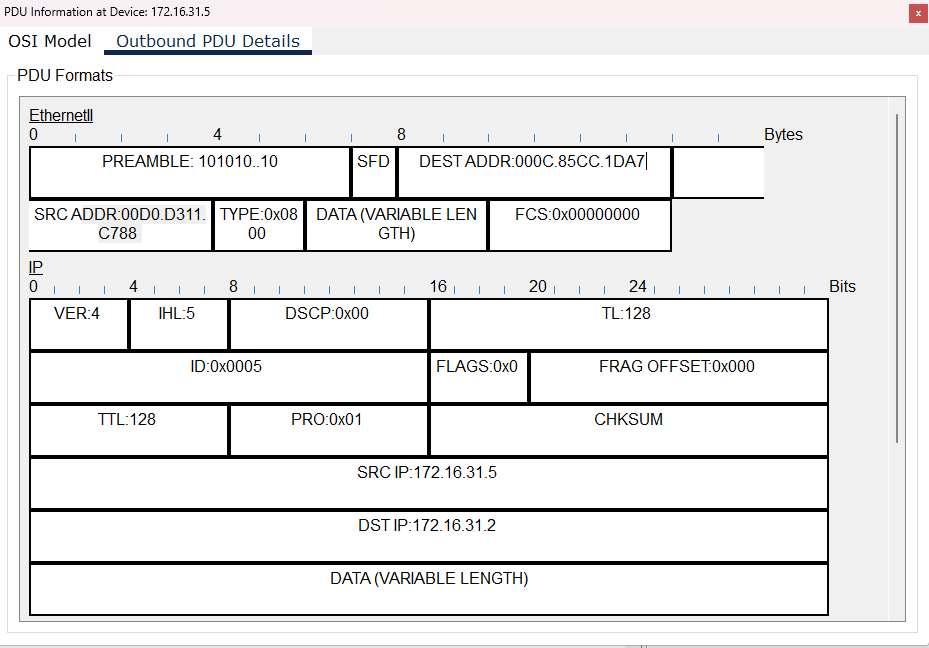
o MAC-адресназначения: **000C:85CC:1DA7**

o MAC-адресисточника: **00D0:D311:C788**

o IP-адресисточника: **172.16.31.5**

o IP-адресназначения: **172.16.31.2**

oНа устройстве: **172.16.31.5**



д.     Нажмите **Capture/Forward (стрелка вправо с вертикальной чертой), чтобы переместить** единицу данных протокола (PDU) на следующее устройство. Соберите аналогичные сведения из шага 1Г. Повторяйте процедуру до тех пор, пока единица данных протокола (PDU) не достигнет места назначения. Запишите полученные сведения о единице данных протокола (PDU) в электронную таблицу в формате, показанном в таблице ниже.

| **На устройстве** | **Адрес MAC-адрес** | **MAC-адрес источника** | **IPv4-адрес источника** | **IPv4-адрес назначения** |
| --- | --- | --- | --- | --- |
| 172.16.31.5 | 000C:85CC:1DA7 | 00D0:D311:C788 | 172.16.31.5 | 172.16.31.2 |
| Switch1 | 000C:85CC:1DA7 | 00D0:D311:C788 | SRC IP:172.16.31.2 | DST IP:172.16.31.5 |
| узел | DEST ADDR:00D0.D311.C788 | SRC ADDR:000C.85CC.1DA7 | SRC IP:172.16.31.2 | DST IP:172.16.31.5 |
| 172.16.31.2 | 00D0:D311:C788 | 000C:85CC:1DA7 | 172.16.31.2 | 172.16.31.5 |

### Шаг 2.     Соберите дополнительные сведения о единице данных протокола (PDU) из других эхо-запросов

Повторите процедуру, описанную в шаге 1, и соберите сведения для следующих проверок.

·         Эхо-запрос с 172.16.31.2 на адрес 172.16.31.3

| **На устройстве** | **Адрес MAC-адрес** | **MAC-адрес источника** | **IPv4-адрес источника** | **IPv4-адрес назначения** |
| --- | --- | --- | --- | --- |
| 172.16.31.2 | DEST ADDR:00D0.D311.C788 | SRC ADDR:000C.85CC.1DA7 | SRC IP:172.16.31.2 | DST IP:172.16.31.5 |
| узел | DEST ADDR:00D0.D311.C788 | SRC ADDR:000C.85CC.1DA7 | SRC IP:172.16.31.2 | DST IP:172.16.31.5 |
| Switch1 | DEST ADDR:000C.85CC.1DA7 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.2 |
| 172.16.31.5 | DEST ADDR:000C.85CC.1DA7 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.2 |
| Switch1 | DEST ADDR:000C.85CC.1DA7 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.2 |
| узел | DEST ADDR:000C.85CC.1DA7 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.2 |
| 172.16.31.3 | DEST ADDR:000C.85CC.1DA7 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.2 |

·         Эхо-запрос с 172.16.31.4 на адрес 172.16.31.5

| **На устройстве** | **Адрес MAC-адрес** | **MAC-адрес источника** | **IPv4-адрес источника** | **IPv4-адрес назначения** |
| --- | --- | --- | --- | --- |
| 172.16.31.4 | DEST ADDR:00D0.D311.C788 | SRC ADDR:000C.CF0B.BC80 | SRC IP:172.16.31.4 | DST IP:172.16.31.5 |
| Switch1 | DEST ADDR:00D0.D311.C788 | SRC ADDR:000C.CF0B.BC80 | SRC IP:172.16.31.4 | DST IP:172.16.31.5 |
| 172.16.31.5 | DEST ADDR:000C.CF0B.BC80 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.4 |
| Switch1 | DEST ADDR:000C.CF0B.BC80 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.4 |
| 172.16.31.4 | DEST ADDR:000C.CF0B.BC80 | SRC ADDR:00D0.D311.C788 | SRC IP:172.16.31.5 | DST IP:172.16.31.4 |

## Часть 2: Сбор информации PDU для удаленной сетевойсвязи

### Шаг 1: Соберите сведения о единице данных протокола (PDU) по мере перемещения пакета с адреса 172.16.31.5 в адрес 10.10.10.2.

a.     Нажмите на **172.16.31.5**и откройте окно **Command Prompt (Командная строка)**.

б.     ведите команду **ping 10.10.10.2.**

в.     Перейдите в режим моделирования и повторите команду **ping 10.10.10.2**. Единица данных протокола (PDU) будет показана рядом с **172.16.31.5.**

г.     Нажмите единицу данных протокола (PDU) и запишите следующие данные на вкладке **Outbound PDU Layer** (Уровень исходящей PDU).

·         MAC-адрес назначения: 00D0:BA8E:741A

· MAC-адрес источника: 00D0:D311:C788

·         IP-адрес источника: 172.16.31.5

·         IP-адрес назначения: 10.10.10.2

· На устройстве: 172.16.31.5

#### **Вопрос:**

Какое устройство имеет MAC-адрес назначения , который отображается?

д.     Нажмите **Capture/Forward (стрелка вправо с вертикальной чертой), чтобы переместить** единицу данных протокола (PDU) на следующее устройство. Соберите аналогичные сведения из шага 1Г. Повторяйте процедуру до тех пор, пока единица данных протокола (PDU) не достигнет места назначения. Запишите полученные сведения о единице данных протокола (PDU) после пингования 172.16.31.5 в электронную таблицу в формате, показанном в таблице ниже.

| **На устройстве** | **Адрес MAC-адрес** | **MAC-адрес источника** | **IPv4-адрес источника** | **IPv4-адрес назначения** |
| --- | --- | --- | --- | --- |
| 172.16.31.5 | 00D0:BA8E:741A | 00D0:D311:C788 | 172.16.31.5 | 10.10.10.2 |
| Коммутатор 1 | 00D0:BA8E:741A | 00D0:D311:C788 | SRC IP:172.16.31.5 | DST IP:10.10.10.2 |
| Маршрутизатор | 0060:2F84:4AB6 | 00D0:588C:2401 | 172.16.31.5 | 10.10.10.2 |
| Switch0 | 0060:2F84:4AB6 | 00D0:588C:2401 | SRC IP:172.16.31.5 | DST IP:10.10.10.2 |
| Точка доступа | DEST ADDR:0060.2F84.4AB6 | SRC ADDR:00D0.588C.2401 | SRC IP:172.16.31.5 | DST IP:10.10.10.2 |
| 10.10.10.2 | 00D0:588C:2401 | 0060:2F84:4AB6 | 10.10.10.2 | 172.16.31.5 |

# Задание “9.2.9”

## Часть 1. Анализ ARP-запроса

### Шаг 1. Создайте ARP-запросы, отправив эхо-запросы на адрес 172.16.31.3 с 172.16.31.2.

*Откройте командную строку.*

a.     Нажмите **172.16.31.2**и откройте окно **Command Prompt** (Командная строка).

b.     Выполните команду **arp -d**, чтобы очистить таблицу ARP.



*Закройте командную строку.*

c.     Перейдите в режим **Simulation** (Моделирование) и выполните команду **ping 172.16.31.3**. Будет создано две единицы данных протокола PDU. Команда **ping** не может отправить ICMP-пакет, не зная MAC-адрес назначения. Поэтому компьютер отправляет широковещательный кадр ARP, чтобы найти MAC-адрес назначения.

d.     Нажмите кнопку **Capture/Forward** (Захватить/переадресовать) один раз. Единица данных протокола (PDU) ARP перемещается на **Switch1** (Коммутатор 1), а единица данных протокола (PDU) ICMP исчезает, ожидая ARP-ответ. Откройте единицу данных протокола (PDU) и запишите MAC-адрес назначения.

SOURCE MAC :000C.85CC.1DA7

#### **Вопрос:**

Этот адрес есть в таблице выше?



***Введите ваш ответ здесь.***

e.     Нажмите **Capture / Forward** (Захватить/переадресовать), чтобы переместить единицу данных протокола (PDU) на следующее устройство.

#### **Вопрос:**

Сколько копий единицы данных протокола (PDU) создал **Switch1**?

3

***Введите ваш ответ здесь.***

Какой IP-адрес имеет устройство, которое приняло единицу данных протокола (PDU)?

**172.16.31.3**

***Введите ваш ответ здесь.***

f.       Откройте единицу данных протокола (PDU) и изучите уровень 2.

#### **Вопрос:**

Что произошло с MAC-адресами источника и назначения?

DEST ADDR:000C.85CC.1DA7

SRC ADDR:0060.7036.2849

***Введите ваш ответ здесь.***

g.     Нажимайте кнопку **Capture/Forward** (Захватить/переадресовать) до тех пор, пока единица данных протокола (PDU) не вернется на узел **172.16.31.2**.

#### **Вопрос:**

Сколько копий единицы данных протокола (PDU) создал коммутатор для ответа на ARP-запрос?

1

### Шаг 2. Изучите таблицу ARP.

a.     Обратите внимание, что ICMP-пакет снова появился. Откройте единицу данных протокола (PDU) и взгляните на MAC-адрес.

#### **Вопрос:**

MAC-адреса источника и назначения соответствуют их IP-адресам?

SOURCE MAC :0060.7036.2849

SOURCE IP :172.16.31.3

TARGET MAC:000C.85CC.1DA7

TARGET IP:172.16.31.2

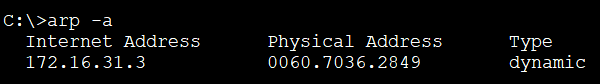
***Введите ваш ответ здесь.***

b.     Вернитесь обратно в режим **реального времени**, и команда ping завершится.

c.     Нажмите **172.16.31.2**и выполните команду **arp –a**.

#### **Вопрос:**

Какому IP-адресу соответствует запись MAC-адреса?

***Введите ваш ответ здесь.*** ******

В общем случае, когда оконечное устройство отправляет ARP-запрос?

ARP-запрос отправляется в том случае, когда устройству требуется MAC-адрес, связанный с IPv4-адресом, но в его таблице ARP нет данных о IPv4-адресе. Сообщения ARP-запроса инкапсулируются непосредственно в кадре Ethernet. Заголовок IPv4 отсутствует. ARP-запрос инкапсулируется в кадре Ethernet со следующей информацией в заголовке.

## Часть 2. Изучение таблицы MAC-адресов коммутатора

### Шаг 1. Сгенерируйте дополнительный трафик для заполнения таблицы MAC-адресов коммутатора.

*Откройте командную строку.*

a.     На узле **172.16.31.2** выполните команду **ping 172.16.31.4**.

b.     Нажмите кнопку **10.10.10.**2 и откройте **командную строку**.

c.     Введите команду **ping 10.10.10.3**.

#### **Вопрос:**

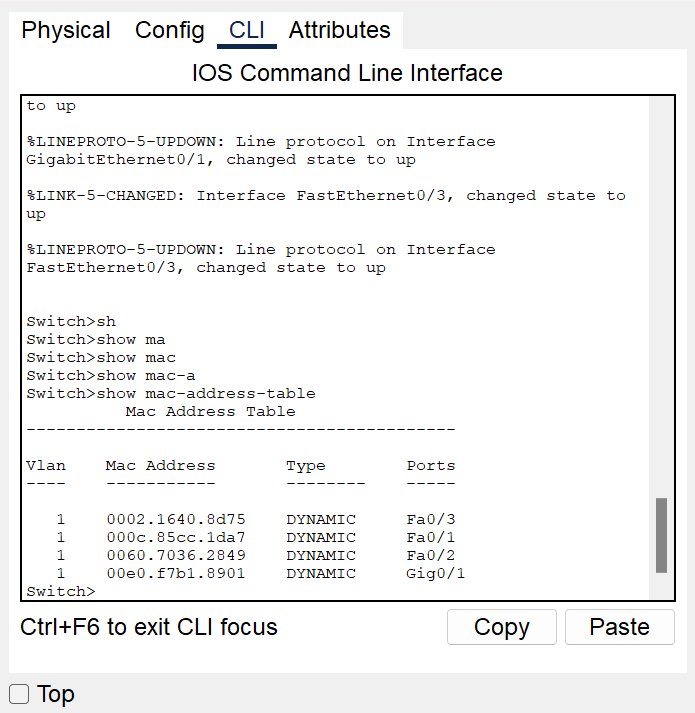
Сколько ответов было отправлено и получено?

По 4

### Шаг 2. Изучите таблицу MAC-адресов на коммутаторах.

a.     Нажмите **Switch1**(Коммутатор 1) и откройте вкладку **CLI** (Интерфейс командной строки). Выполните команду **show mac-address-table**.

#### **Вопрос:**



Совпадают ли записи с указанными в таблице выше?

Да

***Введите ваш ответ здесь.***

b.     Нажмите **Switch0** (Коммутатор 0) и откройте вкладку **CLI** (Интерфейс командной строки). Выполните команду **show mac-address-table**.

#### **Вопросы**

#### **:**

Совпадают ли записи с указанными в таблице выше?

Да, совпадают.

Почему два MAC-адреса связаны с одним портом?

## Часть 3. Анализ процесса ARP в удаленных подключениях

### Шаг 1. Сгенерируйте трафик ARP.

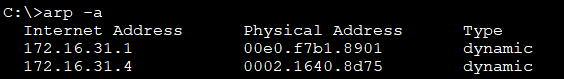
*Откройте командную строку.*

a.     Нажмите **172.16.31.2**и откройте окно **Command Prompt** (Командная строка).

b.     Введите команду **ping 10.10.10.1**.

c.     Введите **arp –a**.

#### **Вопрос:**



Какой IP-адрес имеет новая запись в таблице ARP?

***Введите ваш ответ здесь.***

d.     Выполните команду **arp -d**, чтобы очистить таблицу ARP и перейти в режим **моделирования**.

e.     Повторите команду ping для адреса 10.10.10.1.

#### **Вопрос:**

Сколько единиц данных протокола (PDU) появилось?

2

*Закройте командную строку.*

f.       Нажмите кнопку **Capture/Forward** (Захватить/переадресовать). Нажмите единицу данных протокола (PDU), которая теперь находится на **Switch1**.

#### **Вопрос:**

Какой IP-адрес назначения ARP-запроса?

TARGET IP: 172.16.31.1

g.     IP-адрес назначения не 10.10.10.1.

#### **Вопрос:**

Почему?

Потому что коммутатор передает пакет не 10.10.10.1, а роутеру с ip 172.16.31.1

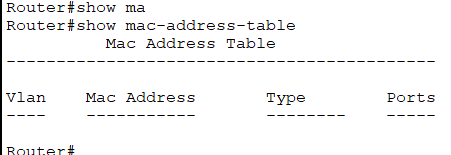
### Шаг 2. Проанализируйте таблицу ARP на Router1.

a.     Перейдите в режим **реального времени**. Нажмите **Router1** (Маршрутизатор 1) и откройте вкладку **CLI** (Интерфейс командной строки).

b.     Войдите в привилегированный режим EXEC и выполните команду **show mac-address-table**.

#### **Вопрос:**

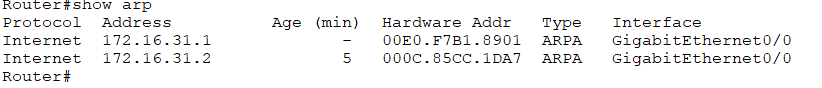
Сколько MAC-адресов в таблице? Почему?



c.     Выполните команду **show arp**.

#### **Вопросы:**

Есть ли запись для **172.16.31.2**?



Что происходит с первым эхо-запросом, когда маршрутизатор отвечает на ARP-запрос?

Когда маршрутизатор отвечает на ARP-запрос, исходное устройство получает его MAC-адрес, чтобы отправить ему эхо-запрос.

# Задание “9.3.4”

## Часть 1: Обнаружение соседних IPv6 устройств

в локальной сети

В части 1 этого задания вы сможете получить MAC-адрес устройства назначения в той же сети, что и вы.

### Шаг 1. Проверьте маршрутизатор на наличие любых соседей, которые он обнаружил.

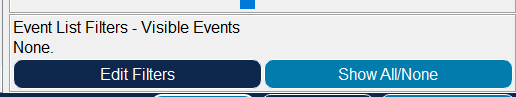
a.     Нажмите на маршрутизатор RTA. Выберите вкладку CLI и выполните команду **show ipv6 neighbors**из привилегированного режима exec. Если отображаются какие-либо записи, удалите их с помощью команды **clear ipv6 neighbors**.

б.     Нажмите на **PCA1**, выберите вкладку Desktop и нажмите на значок **Command Prompt** (командной строки).

### Шаг 2. Переключитесь в режим моделирования для захвата событий.

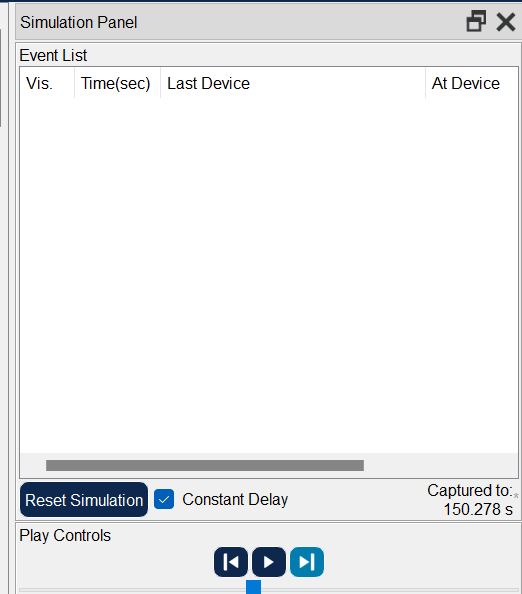
в. Нажмите кнопку **Моделирование в правом нижнем углу окна Топологии Packet Tracer .**

**г. Нажмите кнопку «Show All/None» в левой нижней части панели моделирования. Убедитесь, что Event List Filters – Visible Events показывает None.**

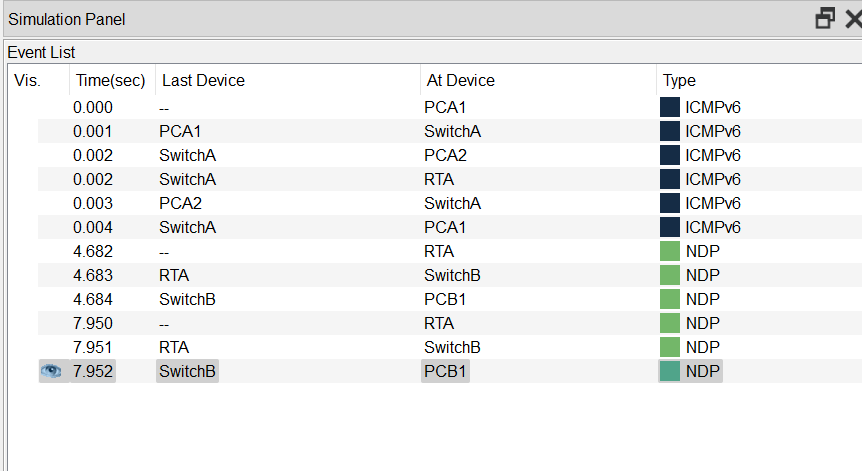
****

**д. В командной строке на PCA1выполните команду ping —n 1 2001:db8:acad:1::b. Это запустит процесс пингования PCA2.**

**е. Нажмите кнопку Play Capture Forward , которая отображается в виде стрелки, указывающей вправо с вертикальной полоской в окне «Управление воспроизведением». В строке состояния над элементами управления воспроизведением должно быть указано «Захвачен» до 150. (Точное число может отличаться.)**

****

**ж. Нажмите кнопку Edit (Изменить). Выберите вкладку IPv6 вверху и установите флажки для ICMPv6 и NDP. нажмите красный значок X в правом верхнем углу окна Редактировать фильтры ACL. Теперь необходимо перечислить захваченные события. В окне должно быть около 12 записей.**

****

#### **Вопрос:**

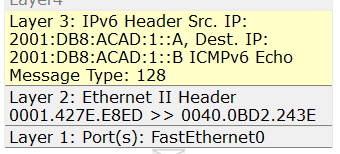
**Почему присутствуют ND PDU?**

**NDP (Neighbor Discovery Protocol) используется в сетях IPv6 для обнаружения соседей и управления маршрутизацией. При выполнении ICMPv6 команд, таких как ping, устройства отправляют NDP пакеты для определения MAC-адресов соседей. Таким образом, присутствие NDP PDU в захвате связано с процессом обмена данными в сети IPv6 во время выполнения команды ping.**

**з. Нажмите квадрат в столбце Тип для первого события, которое должно быть ICMPv6.**

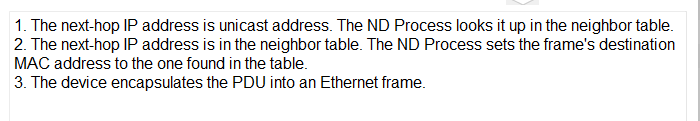
#### **Вопрос:**

**Поскольку сообщение начинается с этого события, существует только исходящий PDU. На вкладке Модель OSI, какой тип сообщения указан для ICMPv6?**

****

**Message type: 128 обозначает ICMPv6 Echo Request сообщение. Это сообщение используется при выполнении команды ping в сети IPv6. Когда узел отправляет ICMPv6 Echo Request, он запрашивает у соседнего устройства (обычно маршрутизатора или хоста) отправку ответного ICMPv6 Echo Reply сообщения, чтобы проверить доступность сетевого узла.**

**Обратите внимание, что нет адресации уровня 2. Нажмите кнопку Next Layer >>, чтобы получить объяснение процесса ND (Neighbor Discovery).**

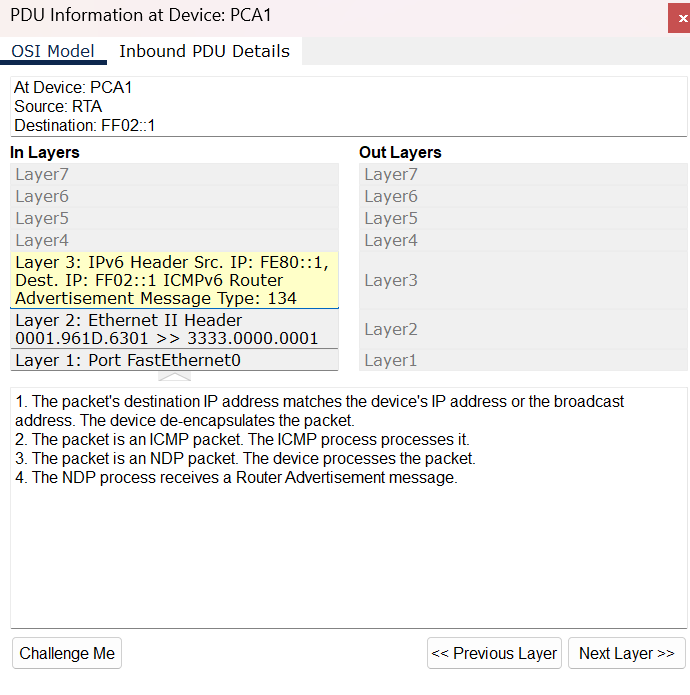
****

**и. нажмите квадрат рядом со следующим событием на панели моделирования. Он должен быть на устройстве PCA1 и тип должен быть NDP.**

#### **Вопросы:**

**Что изменилось в адресации уровня 3?**

**Какие адреса уровня 2 отображаются?**

****

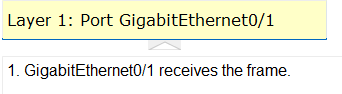
**Если узел не знает MAC-адрес назначения, специальный MAC-адрес многоадресной рассылки используется IPv6 Neighbor Discovery в качестве адреса назначения уровня 2.**

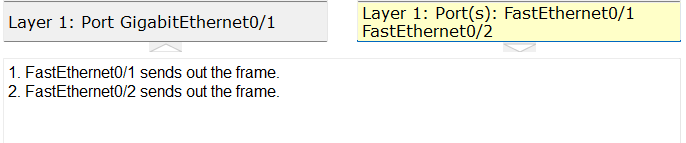
**Если узел не знает MAC-адрес назначения, то используется специальный MAC-адрес многоадресной рассылки, который представляет собой FF:FF:FF:FF:FF:FF.**

**к. Выберите первое событие NDP в SwitchA.**

#### **Вопрос:**

**Есть ли разница между "In Layers" и "Out Layers" для уровня 2?**

****

****

**л. Выберите первое событие NDP на PCA2. нажмите вкладку Outbound PDU Details (Сведения об исходящей PDU).**

#### **Вопрос:**

**Какие адреса отображаются для следующего?**

**Примечание. Адреса в полях могут быть обернуты, отрегулировать размер окна PDU, чтобы сделать адресную информацию проще для чтения.**

**Ethernet II DEST ADDR:** 3333.0000.0001

**Ethernet II SRC ADDR:** 0001.961D.6301

**IPv6 SRC IP:** :FE80::1

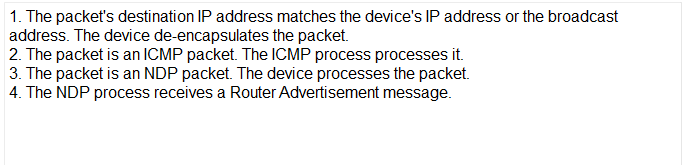
**IPv6 DST IP:** FF02::1

#### **Вопрос:**

**м. Выберите первое событие NDP на PCA2. Почему нет Out Layers?**

**На PCA2 нет Out Layers, потому что NDP сообщения обрабатываются на уровне 2 и не создают новые уровни данных.**

**н. Нажмите кнопку Next Layer >> до конца и прочитайте шаги с 4 по 7 для получения дальнейших разъяснений.**

****

**о. нажмите по следующему событию ICMPv6 на PCA1.**

#### **Вопрос:**

**Имеет ли PCA1 всю необходимую информацию для связи с PCA2?**

**Из сообщений ICMPv6 на PCA1 можно узнать IPv6 адрес PCA2, но PCA1 не имеет информации о MAC-адресе PCA2.**

**п. нажмите по последнему событию ICMPv6 на PCA1. Обратите внимание, что это последнее сообщение в списке.**

#### **Вопрос:**

**Что такое ICMPv6 Echo MessageType?**

**ICMPv6 Echo MessageType - это тип сообщения в протоколе ICMPv6, используемый для проверки доступности сетевого узла в сети IPv6. Он используется, например, при выполнении команды ping для определения доступности других устройств в сети.**

**п. нажмите Reset Simulation на панели «Simulation». Из командной строки PCA1 повторите ping на PCA2. (Подсказка: вы должны иметь возможность нажать стрелку вверх, чтобы вернуть предыдущую команду.)**

**q. Нажмите кнопку Capture Forward 5 раз, чтобы завершить процесс ping.**

#### **Вопрос:**

**Почему не было событий NDP?**

**Если не было событий NDP во время процесса ping, то это может быть связано с тем, что MAC-адрес PCA2 уже был известен PCA1, и не потребовалось выполнение NDP процесса для его обнаружения.**

## Часть 2: Удаленная сеть

**обнаружения соседей IPv6**

**В части 2 этого действия будут выполняться действия, аналогичные тем, которые приведены в части 1, за исключением того, что узел назначения находится в другой локальной сети. Обратите внимание, как процесс обнаружения соседей отличается от процесса, наблюдаемого в части 1. Обратите внимание на некоторые дополнительные шаги адресации, которые происходят, когда устройство взаимодействует с устройством, которое находится в другой сети.**

**Обязательно нажмите кнопку « Reset Simulation », чтобы очистить предыдущие события.**

### Шаг 1. Захват событий для удаленной связи.

**a. Отображение и очистите все записи в таблице соседних устройств IPv6, как это было сделано в части I.**

**б.     Перейдите в режим Simulation (Моделирование). Нажмите кнопку « Show All/None » в левой нижней части панели моделирования. Убедитесь, что Event List Filters – Visible Events показывает None.**

**в. Из командной строки на PCA1 выполните команду ping —n 1 2001:db8:acad:2::a на хост PCB1.**

**г. Нажмите кнопку Play Capture Forward , которая отображается в виде стрелки, указывающей вправо с вертикальной полоской в окне «Управление воспроизведением». В строке состояния над элементами управления воспроизведением должно быть указано «Захвачен» до 150. (Точное число может отличаться.)**

**д. Нажмите кнопку Edit (Изменить). Выберите вкладку IPv6 вверху и установите флажки для ICMPv6 и NDP. Щелкните красный значок X в правом верхнем углу окна Редактировать фильтры ACL. Теперь должны быть перечислены все предыдущие события. Вы должны заметить, что на этот раз значительно больше записей.**

**е. нажмите квадрат в столбце типа для первого события, которое должно быть ICMPv6. Поскольку сообщение начинается с этого события, существует только исходящий PDU. Обратите внимание, что в нем отсутствует информация о слое 2, как это было в предыдущем сценарии.**

**ж. нажмите первое событие NDP на устройстве PCA1 .**

#### **Вопрос:**

**Какой адрес используется как IP-адрес Src во входящем PDU?**

SRC IP:2001:DB8:ACAD:1::A

**Обнаружение соседей IPv6 определяет следующий пункт назначения для пересылки сообщения ICMPv6.**

**з.     нажмите по второму событию ICMPv6 для PCA1. PCA1 теперь имеет достаточно информации для создания эхо-запроса ICMPv6.**

#### **Вопрос:**

**Какой MAC-адрес используется как MAC-адреса назначения?**

DEST ADDR:0001.427E.E8ED

**и. нажмите следующее событие ICMPv6 на устройстве RTA. Обратите внимание, что исходящий PDU от RTA не имеет адреса уровня назначения 2. Это означает, что RTA снова должен выполнить обнаружение соседей для интерфейса, который имеет сеть 2001:db8:acad:2::: потому что он не знает MAC-адреса устройств на локальной сети G0/0/1.**

**к. Перейдите к первому событию ICMPv6 для устройства PCB1.**

#### **Вопрос:**

**Что отсутствует в исходящей информации уровня 2?**

**В исходящей информации уровня 2 отсутствует MAC-адрес, так как PCB1 не знает MAC-адреса устройства, на которое он отправляет ICMPv6 Echo Request, и должен выполнить обнаружение соседей для получения этой информации.**

**л. Следующие несколько** событий **NDP связывают оставшиеся адреса IPv6 с MAC-адресами. Предыдущие события NDP связывали MAC-адреса с локальными адресами связи.**

**м. Перейдите к последнему набору событий ICMPv6 и обратите внимание, что все адреса были изучены. Необходимая информация теперь известна, поэтому PCB1 может отправлять эхо-ответные сообщения на PCA1.**

**н. нажмите Reset Simulation на панели «Simulation». Из командной строки PCA1 повторите команду ping PCB1.**

**о. Нажмите кнопку Capture Forward девять раз, чтобы завершить процесс ping.**

#### **Вопрос:**

**Почему не было событий NDP?**

**п. нажмите единственное событие PCB1 в новом списке.**

#### **Вопросы:**

**Что соответствует MAC-адресу назначения?**

DEST ADDR:0001.961D.6302

**Почему PCB1 использует MAC-адрес интерфейса маршрутизатора для создания ICMP PDU?**

**Почему PCB1 использует MAC-адрес интерфейса маршрутизатора для создания ICMP PDU? - Это происходит потому, что PCB1 не знает MAC-адреса устройства, на которое он отправляет ICMPv6 Echo Request, и использует MAC-адрес интерфейса маршрутизатора в качестве временного адреса назначения, пока не будет выполнено обнаружение соседей.**

### Шаг 2. Проверьте выводы маршрутизатора.

**a. Вернитесь в режим реального времени (Realtime).**

**б. Нажмите кнопку RTA и выберите вкладку CLI. В командной строке маршрутизатора введите команду show ipv6 neighbors.**

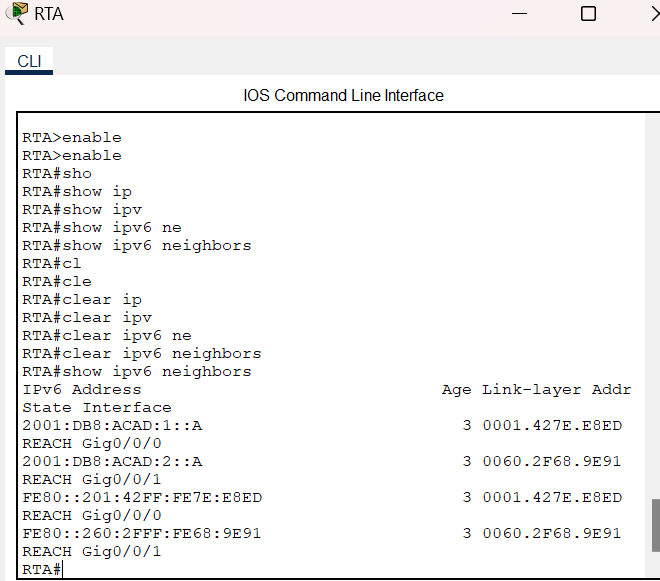
#### **Вопросы:**

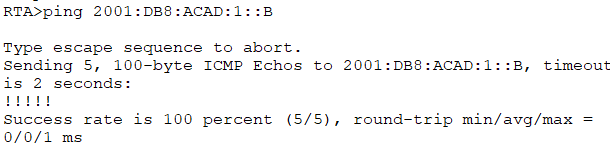
**Сколько адресов в списке?**

**С какими устройствами связаны эти адреса?**

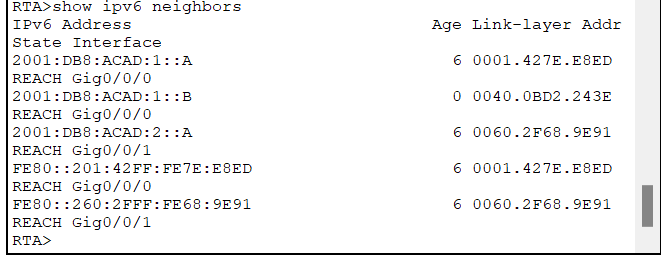
**Имеются ли какие-либо записи для PCA2 (почему или почему нет)?**

**Запустите эхо-запрос до PCA2 с маршрутизатора.**

****

****

**в.     Выполните команду show ipv6 neighbors .**

****

#### **Вопрос:**

**Существуют ли записи для PCA2?**

# Вопросы для повторения

**1.     Когда устройство требует процесса обнаружения соседей IPv6?**

**Устройство требует процесса обнаружения соседей IPv6, когда оно не знает MAC-адрес соседнего устройства на локальной сети, и ему необходимо выполнить обмен данными с этим устройством, например, при отправке ICMPv6 сообщений, таких как Neighbor Solicitation.**

**2. Как маршрутизатор помогает минимизировать объем трафика IPv6 Neighbor Discovery в сети?**

**Маршрутизатор может помочь минимизировать объем трафика IPv6 Neighbor Discovery в сети, кэшируя информацию о соседних узлах и пересылая только необходимые сообщения NDP по необходимости. Он также может использовать механизмы, такие как IPv6 Neighbor Unreachability Detection (NUD), чтобы проверять доступность соседних узлов и поддерживать актуальность информации в кэше соседей.**

**Как IPv6 минимизирует влияние процесса ND на сетевые узлы?**

**IPv6 также минимизирует влияние процесса ND на сетевые узлы, предоставляя различные механизмы оптимизации, такие как Duplicate Address Detection (DAD), которые позволяют узлам эффективно обнаруживать дублирующиеся адреса без создания избыточного трафика.**

**3. Чем отличается процесс обнаружения соседей, когда узел назначения находится в одной локальной сети и когда он находится в удаленной локальной сети?**

**Когда узел назначения находится в одной локальной сети, процесс обнаружения соседей происходит непосредственно через отправку NDP сообщений на все узлы в сегменте сети. Когда узел назначения находится в удаленной локальной сети, процесс обнаружения соседей может включать механизмы, такие как IPv6 Neighbor Unreachability Detection и протоколы маршрутизации, чтобы определить путь к удаленному узлу и получить его MAC-адрес.**