

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет Программной Инженерии и Компьютерной Техники

Компьютерные сети

Лабораторная работа № 2

«Протоколы ARP и ICMP (программы ping и tracert)»

Выполнил студент

Стеберг Артём Алексеевич

Группа № P33232

Преподаватель: Болдырева Елена Александровна

г. Санкт-Петербург

2024

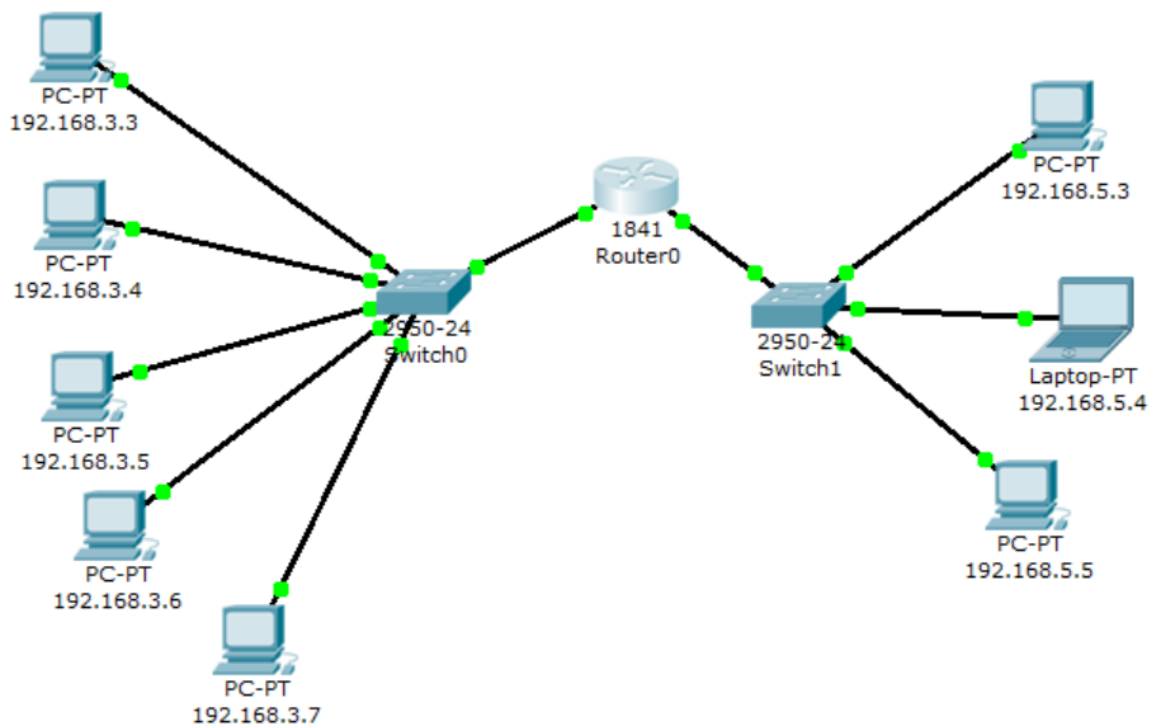
**Цель работы:** изучить режим симуляции Cisco Packet Tracer, протоколы ARP и ICMP на примере программ ping и tracert.

**Программа работы:**

1. Построение топологии сети, настройка конечных узлов;
2. Настройка маршрутизатора;
3. Проверка работы сети в режиме симуляции;
4. Посылка ping-запроса внутри сети;
5. Посылка ping-запроса во внешнюю сеть;
6. Посылка ping-запроса на несуществующий IP-адрес узла;
7. Выполнение индивидуального задания.

**Отчет:**



1. Построим топологию сети, содержащую один маршрутизатор, два коммутатора и несколько конечных узлов.



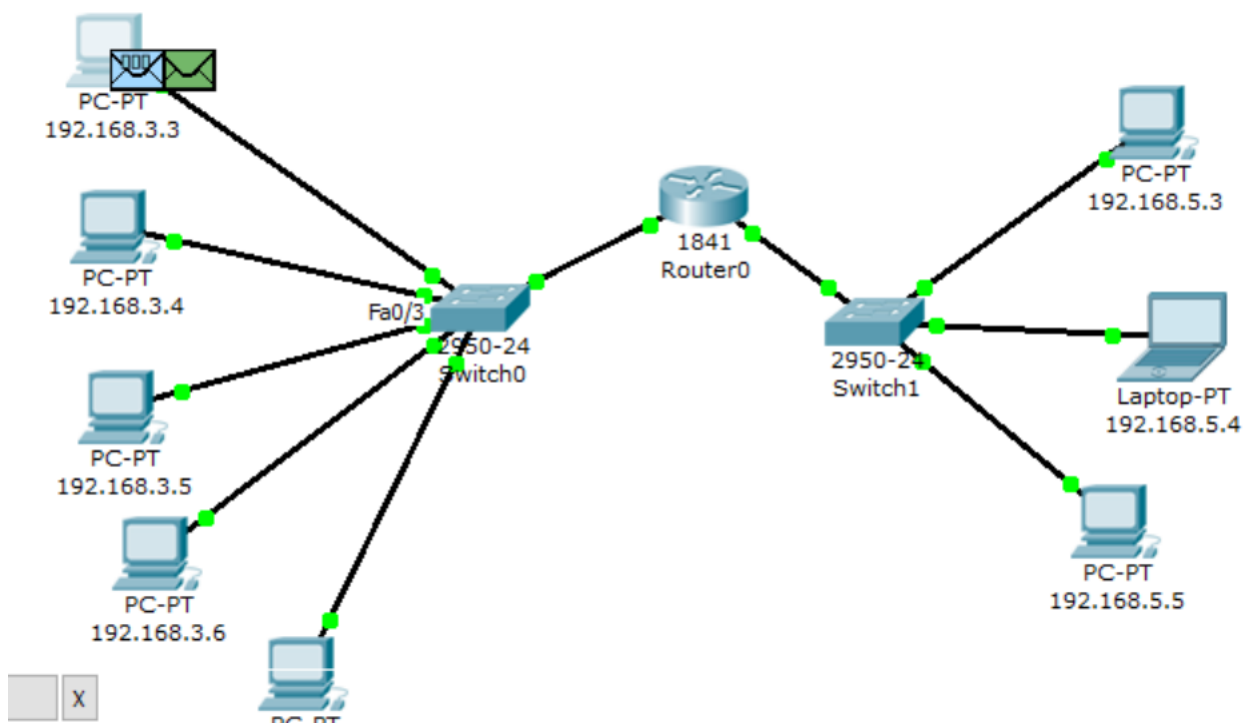
2. Настроим конечным узлам IP адреса и маски подсети таким образом чтоб сформировать две сети, содеянные маршрутизатором.

Адреса Gateway назначим на 192.168.3.1 и 192.168.5.1 для сетей соответственно.

3. Протестируем сеть через режим симуляции, предварительно выставив фильтры на отслеживаемые пакеты ARP, ICMP.

Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Period
	Successful	192.168.3.3	192.168.3.5	ICMP		0.000	N

4. Отправим пинг запрос в пределах одной локальной сети с адреса 192.168.3.3 на 192.168.3.5:

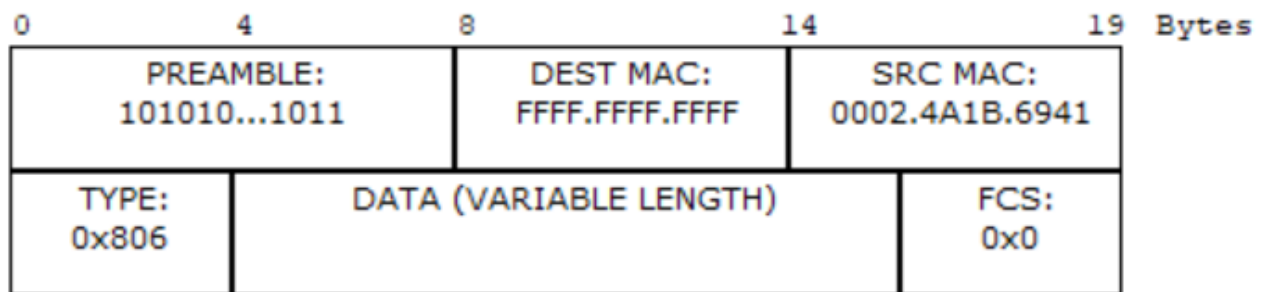


Сформировались два запроса ARP и ICMP.

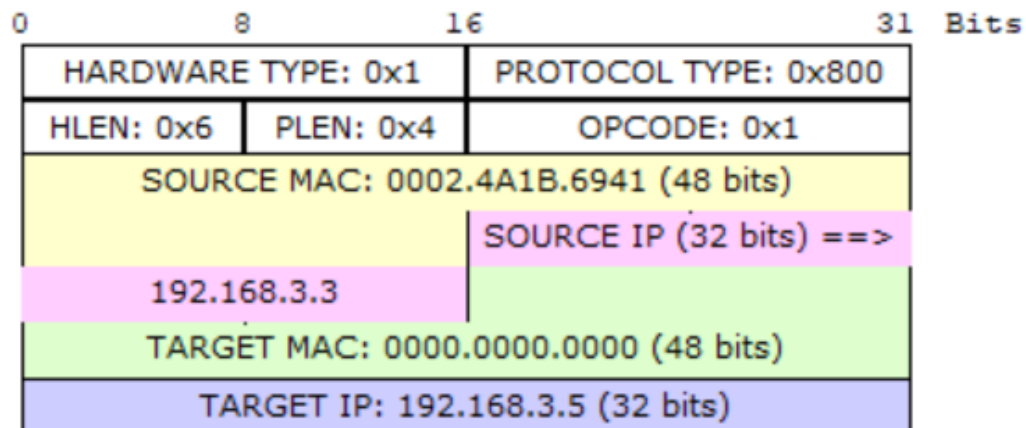
ARP запрос сформирован, так как хост не знает кому отправлять запрос.

Если детально рассмотреть структуру пакета, то увидим следующее:

## Ethernet II



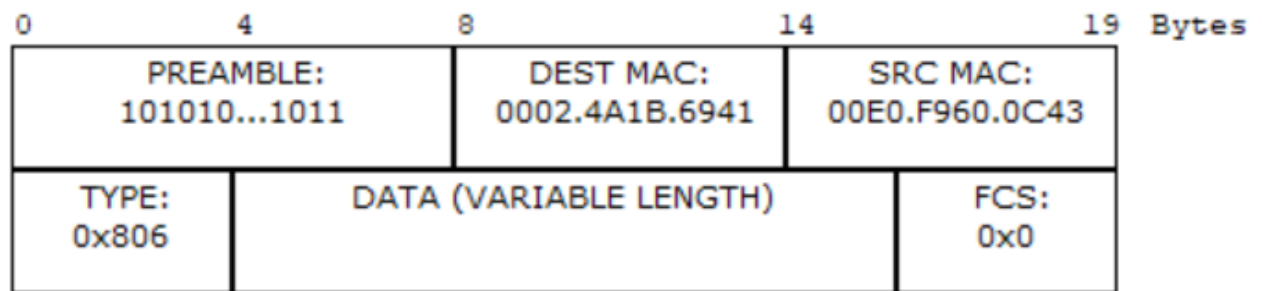
## ARP



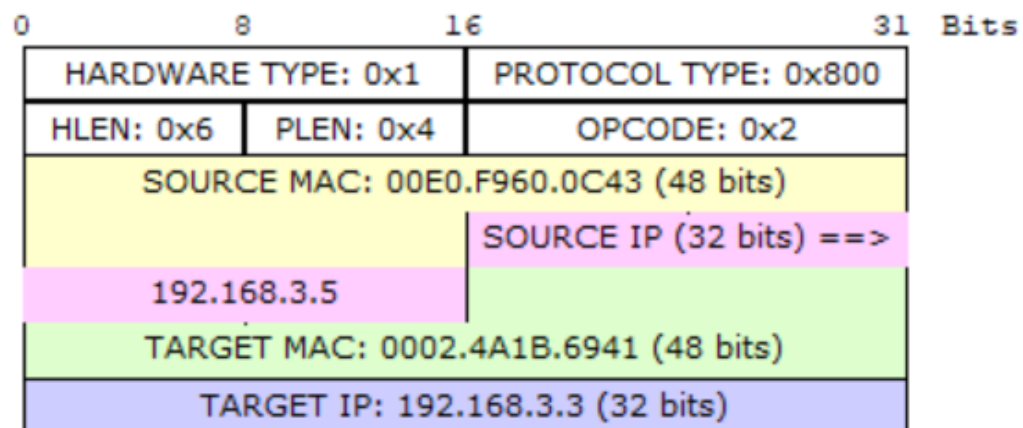
Нас интересует поля MAC адресов и IP адресов. Изначально, MAC адрес, который нам нужно найти не известен, но мы знаем IP, именно таким образом ARP протокол ищет MAC адрес.

После ответа конечного узла на ARP запрос вы получаем пакет следующего вида:

### Ethernet II



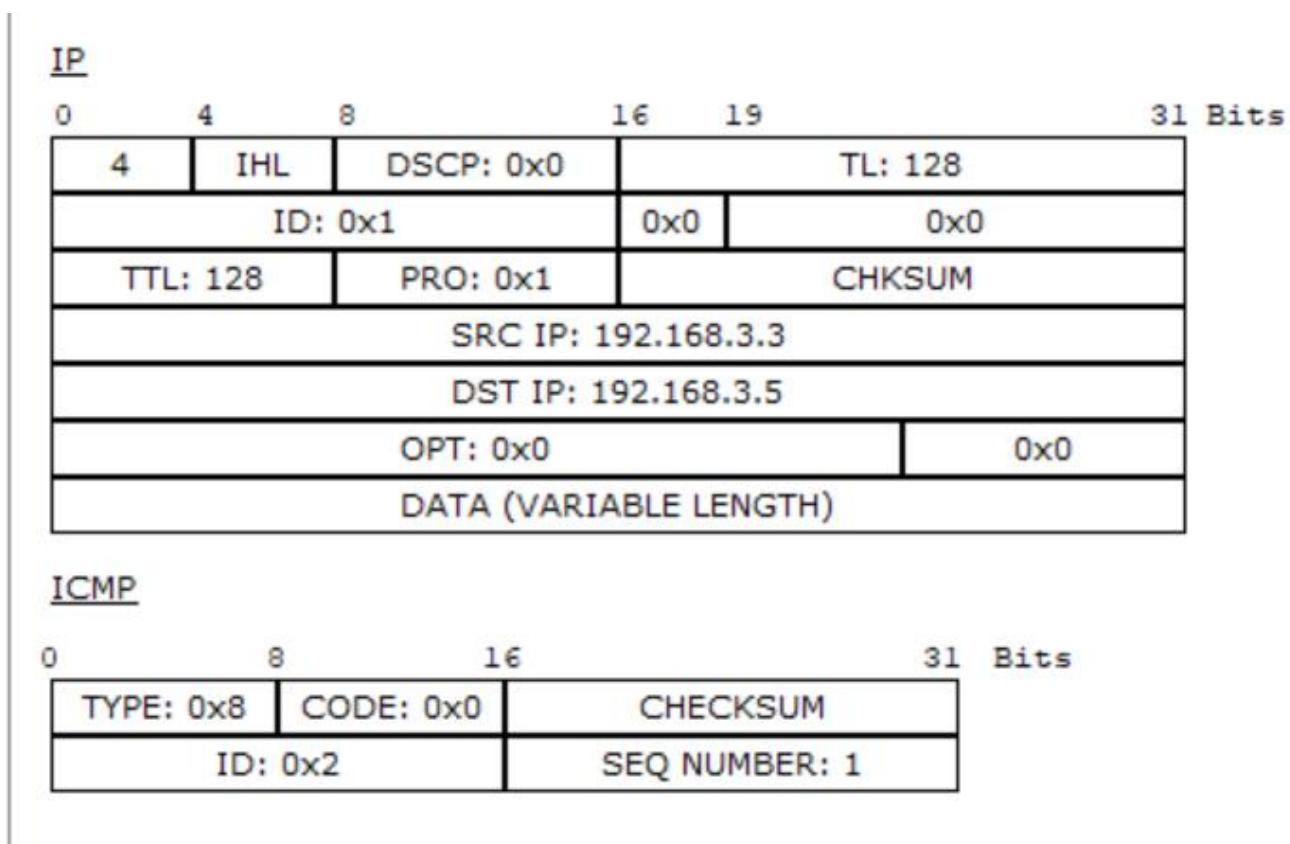
### ARP



Здесь хост получает нужный MAC адрес для отправки ICMP запроса. Также эти адрес добавятся в ARP таблицу для дальнейшего пользования:

ARP Table for 192.168.3.3		
IP Address	Hardware Address	Interface
192.168.3.5	00E0.F960.0C43	FastEthernet

Далее идет отправка ICMP запроса:



Тип запроса – эхо (0x8)

Конечный ответ ICMP запроса выглядит следующим образом:

### IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 128		
ID: 0x1			0x0	0x0	
TTL: 128		PRO: 0x1	CHKSUM		
SRC IP: 192.168.3.5					
DST IP: 192.168.3.3					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

### ICMP

0	8	16	31 Bits
TYPE: 0x0		CODE: 0x0	CHECKSUM
ID: 0x2		SEQ NUMBER: 1	

Где тип – эхо-ответ (0x0)

И вывод терминала:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=8ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128
Reply from 192.168.3.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Если повторить запрос на тот же адрес, то ARP запрос отправлен не будет:

Event List

Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.000	--	192.168.3.3	ICMP	
	0.001	192.168.3.3	Switch0	ICMP	
	0.002	Switch0	192.168.3.5	ICMP	
	0.003	192.168.3.5	Switch0	ICMP	
	0.004	Switch0	192.168.3.3	ICMP	

Reset Simulation

☒ Constant Delay

Captured to: \*  
150.014 s

Play Controls

Back

Auto Capture / Play

Capture / Forward

Event List Filters

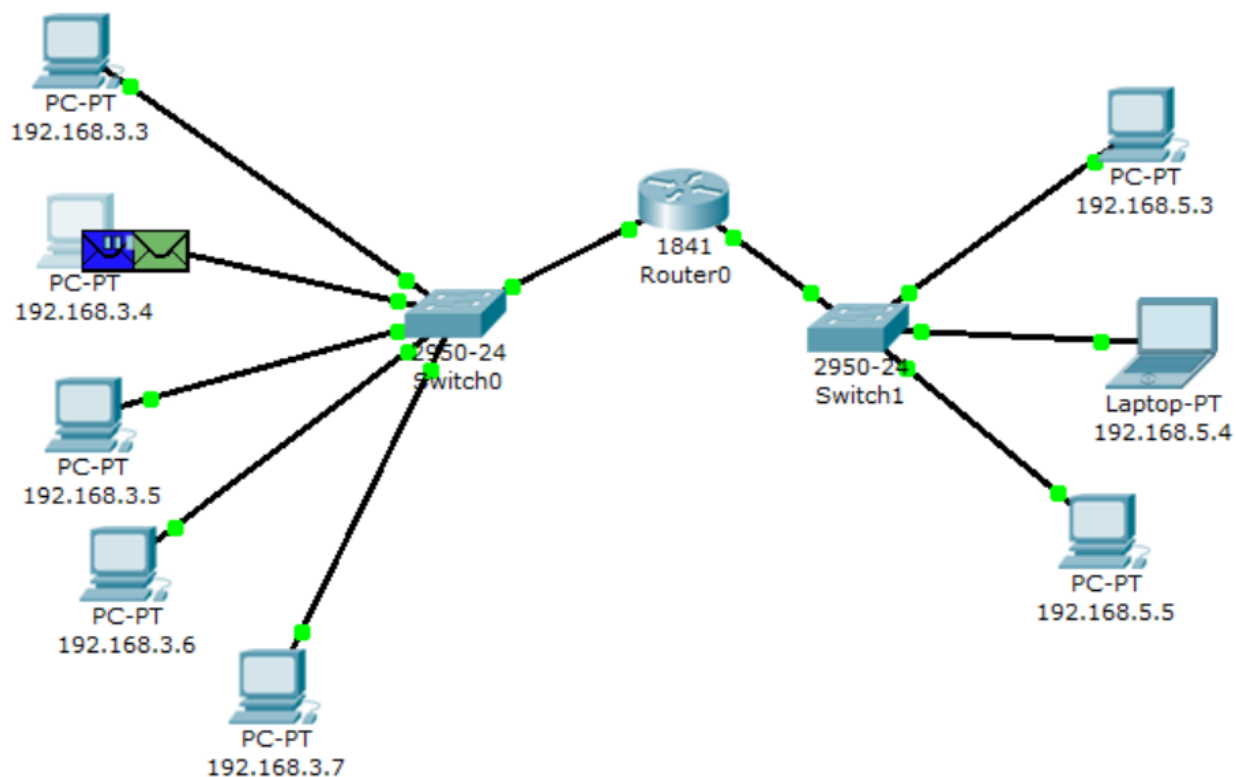
Visible Events: ARP, ICMP

Edit Filters

Show All

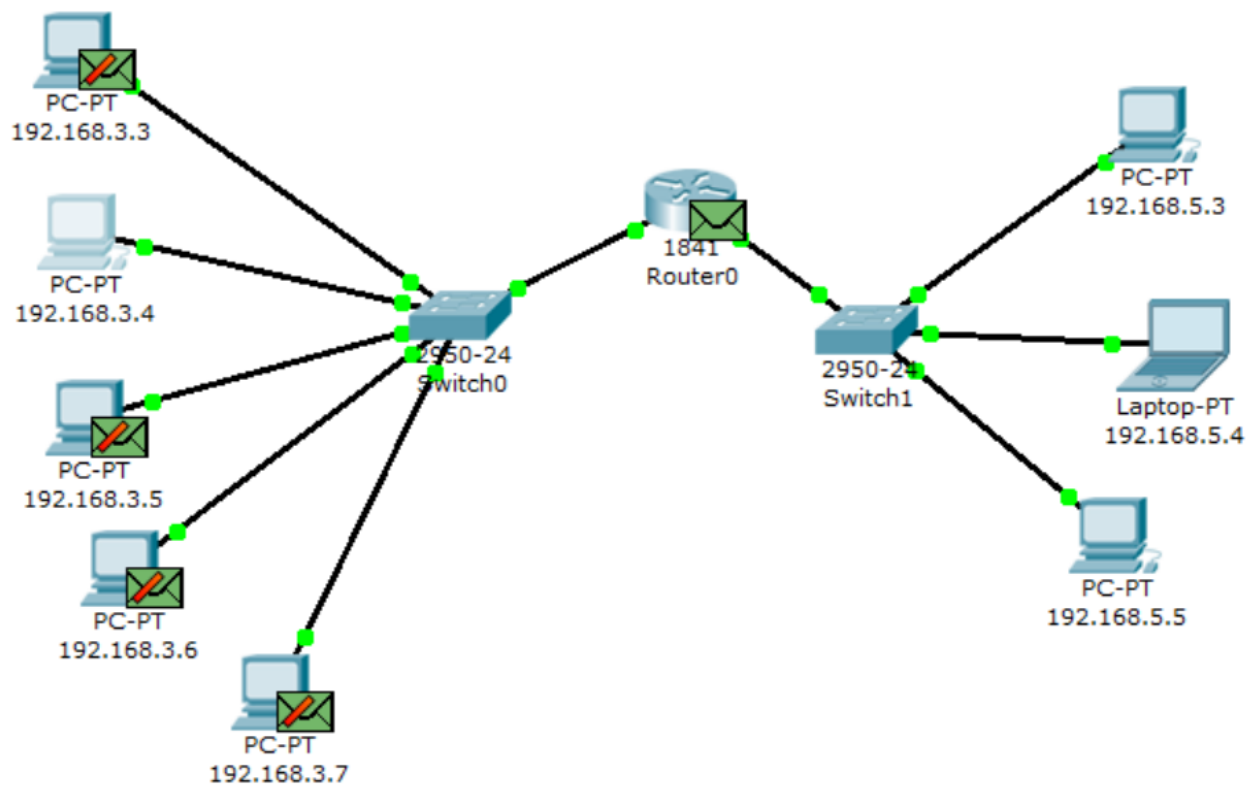
5. Теперь отправим запрос во внешнюю сеть с 192.168.3.4 до 192.168.5.5:



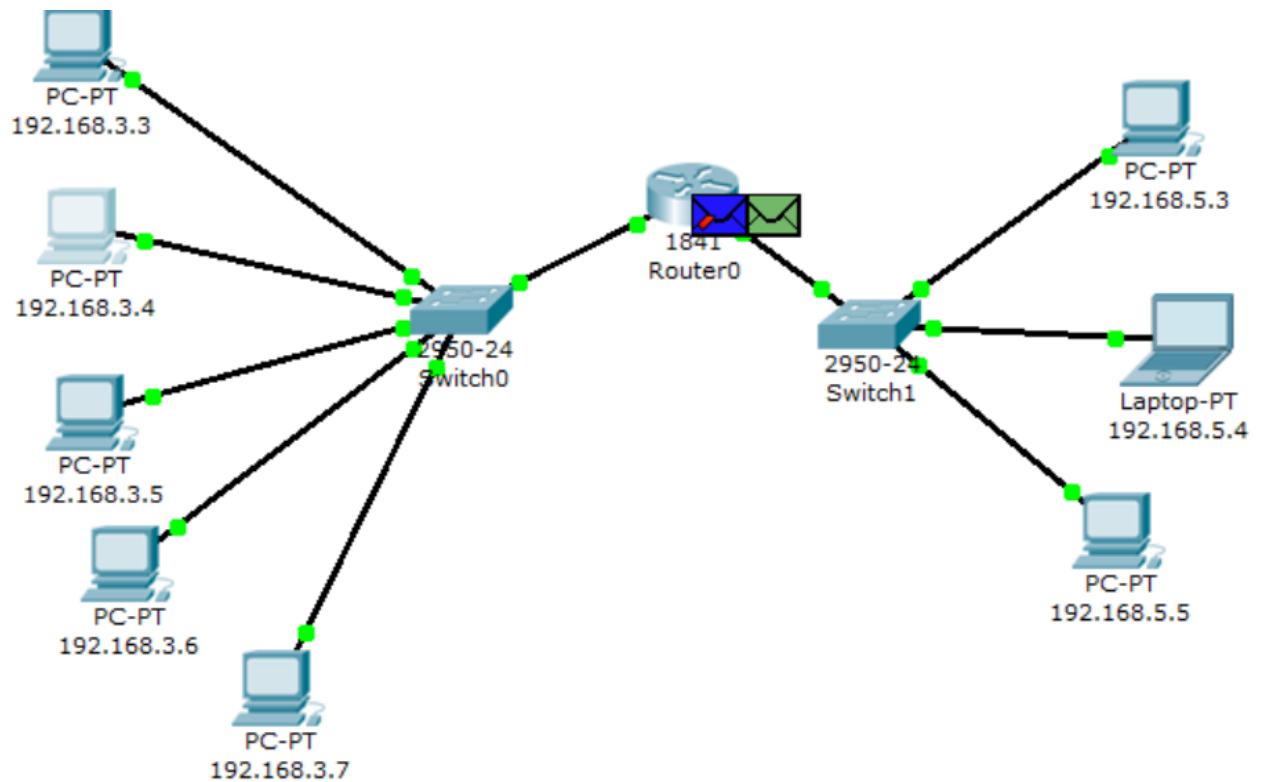


Формируются два запроса один из которых ARP, другой ICMP.

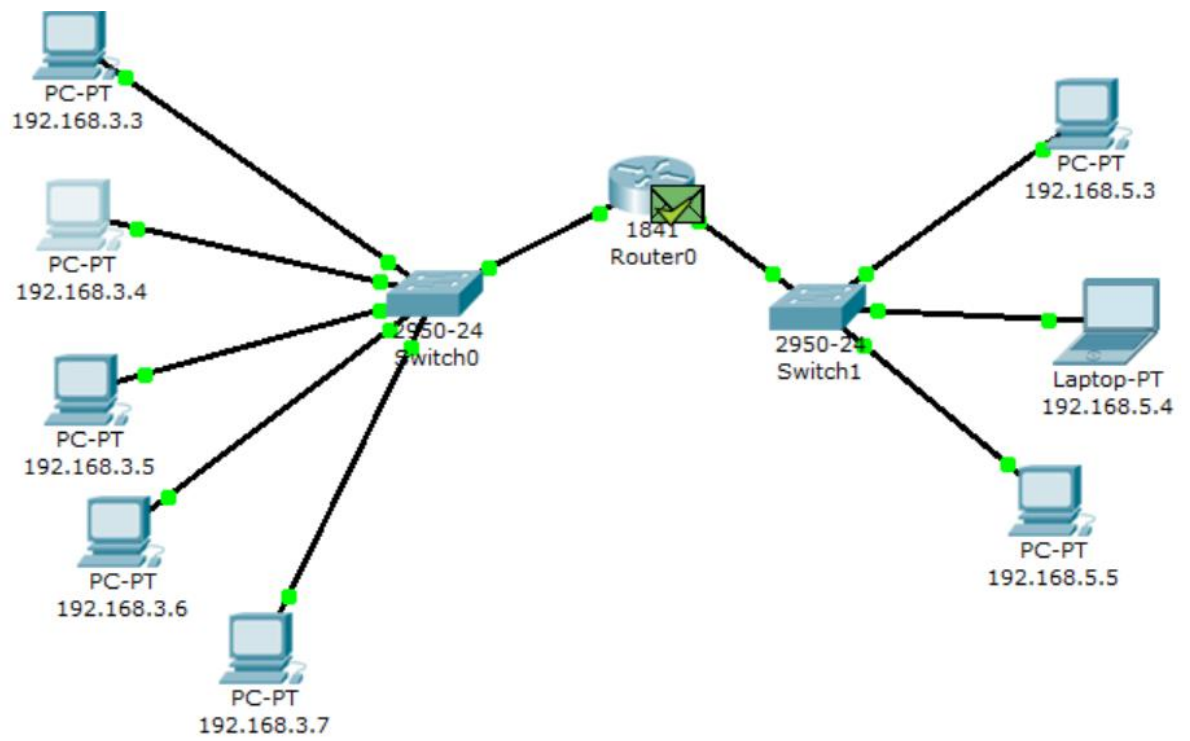
Все происходит так же, как в локальной сети, но определяется адрес маршрутизатора через протокол ARP.



Потом отправляется ICMP протокол:



Но так как нужно определить еще адрес во второй сети, то повторяем процедуру:



## PDU Formats

### Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0002.167D.6402		SRC MAC: 0010.111A.B29D	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0	

### ARP

0	8	16	31 Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800	
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2	
SOURCE MAC: 0010.111A.B29D (48 bits)		SOURCE IP (32 bits) ==>	
192.168.5.5			
TARGET MAC: 0002.167D.6402 (48 bits)			
TARGET IP: 192.168.5.1 (32 bits)			

И вот мы получили адрес конечного узла в другой сети.

Теперь отправляем ICMP запрос:

Vis.	Time (sec)	Last Device	At Device	Type	Info ^
	6.004	--	192.168.3.4	ICMP	
	6.005	192.168.3.4	Switch0	ICMP	
	6.006	Switch0	Router0	ICMP	
	6.007	Router0	Switch1	ICMP	
	6.008	Switch1	192.168.5.5	ICMP	

И получим ответ:

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Из терминала видно, что есть потеря, так как первый ICMP пакет уничтожился маршрутизатором. Который не смог направить из-за отсутствия адреса во внешней сети.

Попробуем отследить маршрут пакетов через команду tracert:

```
PC>tracert 192.168.5.4

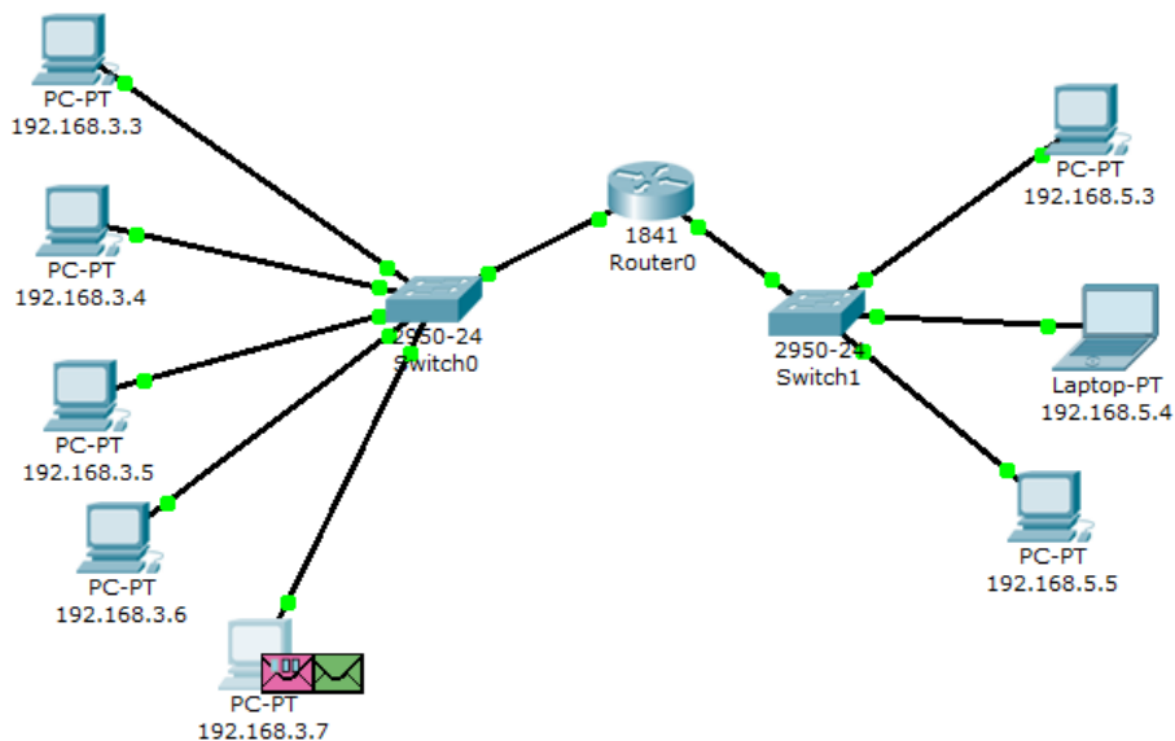
Tracing route to 192.168.5.4 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.3.1
  1  8 ms  4 ms  4 ms  192.168.5.4
  2  8 ms  8 ms  8 ms  192.168.5.4

Trace complete.
```

Очевидно, что такой маршрут содержит один маршрутизатор.

6. Отправив Ping запрос на несуществующий адрес:



Формируется вся та же пара пакетов, которая узнает адрес конечного узла.

После достижения маршрутизатора повторяется ARP запрос на определения конечного узла во внешней сети.

Поскольку такого адрес не существует, то мы и получим что время ответа вышло:

```
PC>ping 192.168.5.7

Pinging 192.168.5.7 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.7:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Попробуем отправить запрос на несуществующую сеть(или до которая не достигаема из нашей сети):

```
PC>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Итог логичен, роутер не может отправить нас на сеть, о которой не знает.

7. Индивидуальное задание:

Вариант 9

**Источник :**

192.168.3.4

192.168.3.5

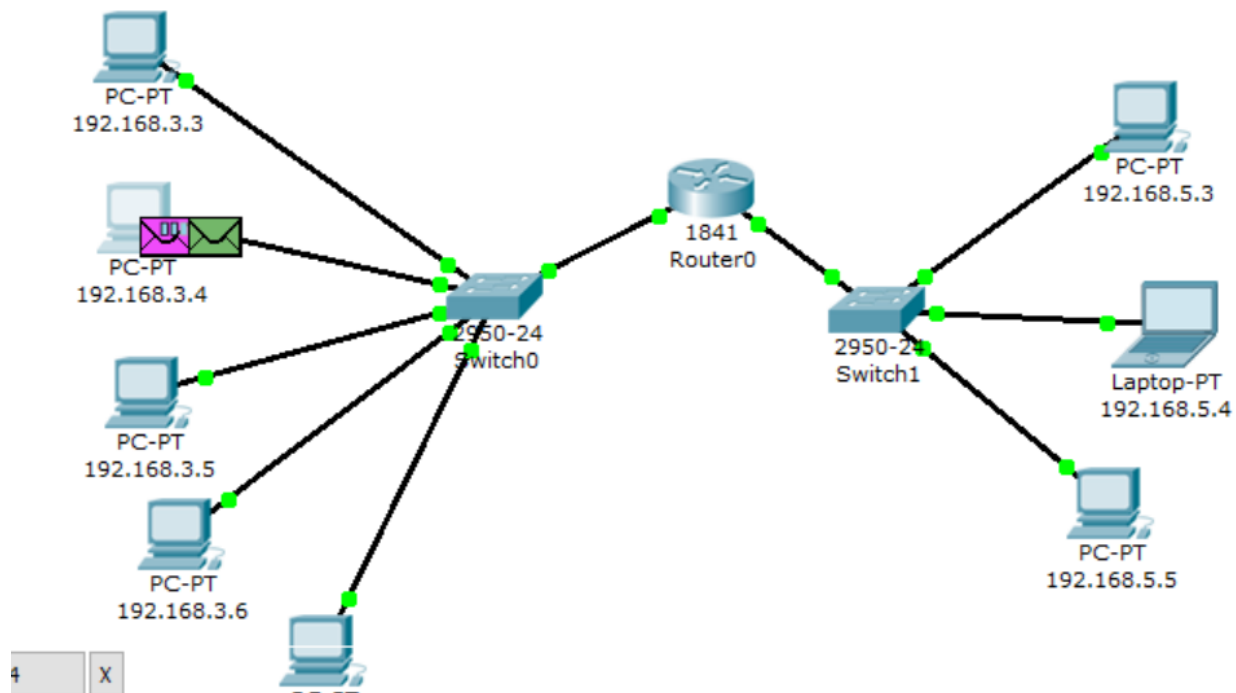
**Приемник:**

192.168.5.3

192.168.3.4

- Источник: 192.168.3.4 Приемник: 192.168.5.3

Такой запрос происходит между двумя сетями:



ARP запрос:



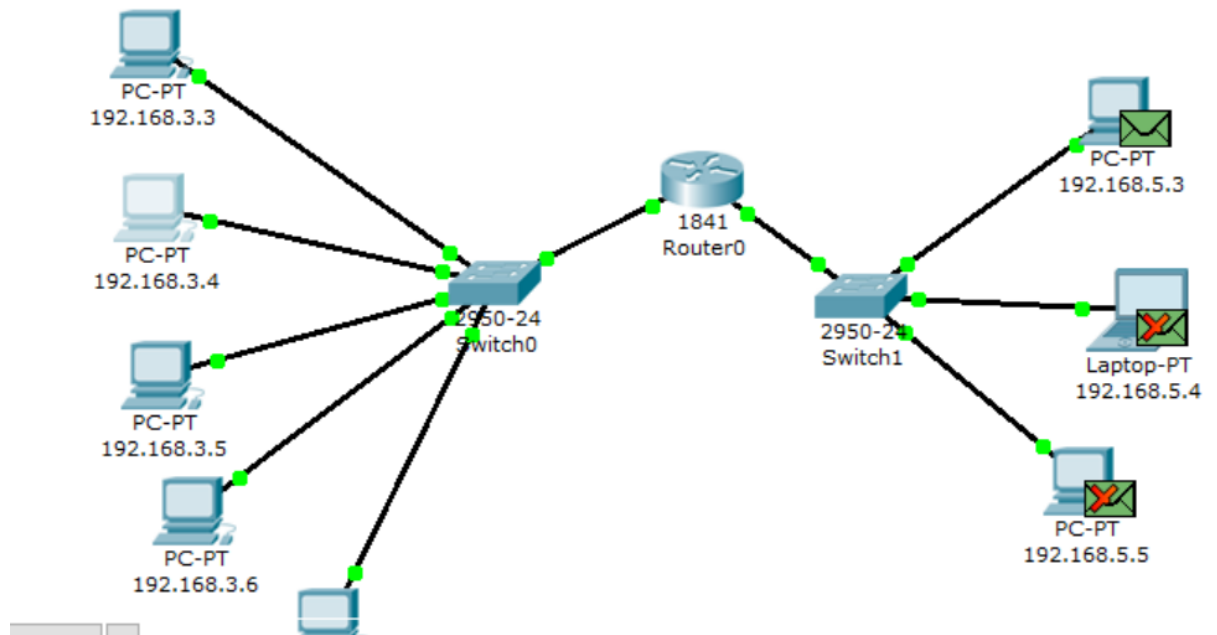
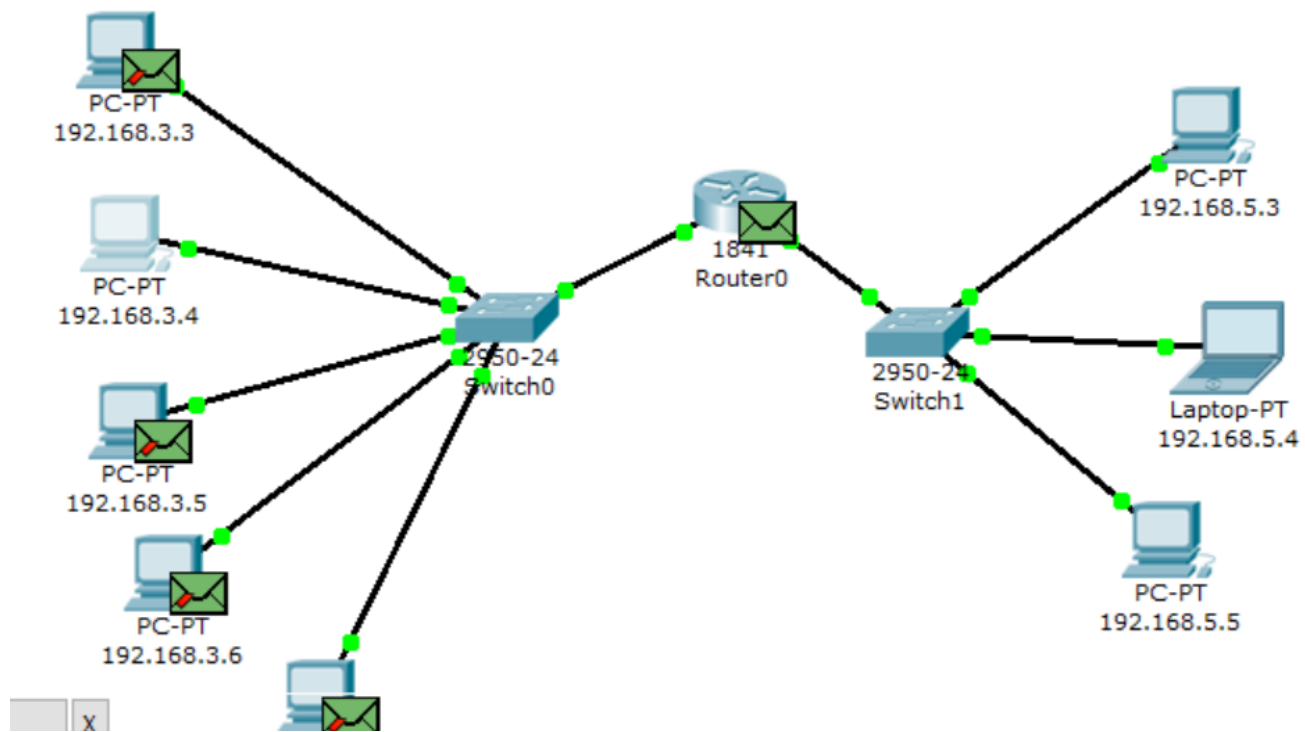
### Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF		SRC MAC: 000C.851D.AAD6	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0	

### ARP

0	8	16	31	Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800		
HLEN: 0x6	PLEN: 0x4		OPCODE: 0x1	
SOURCE MAC: 000C.851D.AAD6 (48 bits)		SOURCE IP (32 bits) ==>		
192.168.3.4				
TARGET MAC: 0000.0000.0000 (48 bits)				
TARGET IP: 192.168.3.1 (32 bits)				

Первым делом отправляется пакет ARP для определения адреса нужного конечного узла. Этот пакет определит маршрутизатор, а потом уже во внешней сети найдет нужный узел.



ARP ответ:

### Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 000C.851D.AAD6		SRC MAC: 0002.167D.6401	
TYPE: 0x806	DATA (VARIABLE LENGTH)			FCS: 0x0	

### ARP

0	8	16	31	Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800		
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2		
SOURCE MAC: 0002.167D.6401 (48 bits)		SOURCE IP (32 bits) ==>		
192.168.3.1				
TARGET MAC: 000C.851D.AAD6 (48 bits)				
TARGET IP: 192.168.3.4 (32 bits)				

Далее ICMP пакет без труда дойдёт до адресата.

Vis.	Time (sec)	Last Device	At Device	Type	Info ^
	6.005	--	192.168.3.4	ICMP	
	6.006	192.168.3.4	Switch0	ICMP	
	6.007	Switch0	Router0	ICMP	
	6.008	Router0	Switch1	ICMP	
	6.009	Switch1	192.168.5.3	ICMP	

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 128		
ID: 0xa			0x0	0x0	
TTL: 127		PRO: 0x1	CHKSUM		
SRC IP: 192.168.5.3					
DST IP: 192.168.3.4					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

## ICMP

0	8	16	31	Bits
TYPE: 0x0		CODE: 0x0	CHECKSUM	
ID: 0x5		SEQ NUMBER: 17		

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.3

Pinging 192.168.5.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127
Reply from 192.168.5.3: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Результат команды `ping` получился таким, так как первый ICMP запрос был уничтожен роутером, который не смог отправить до нужного узла, он не знал адрес конечного узла. Проследим маршрут через `tracert`:

```
PC>tracert 192.168.5.3

Tracing route to 192.168.5.3 over a maximum of 30 hops:

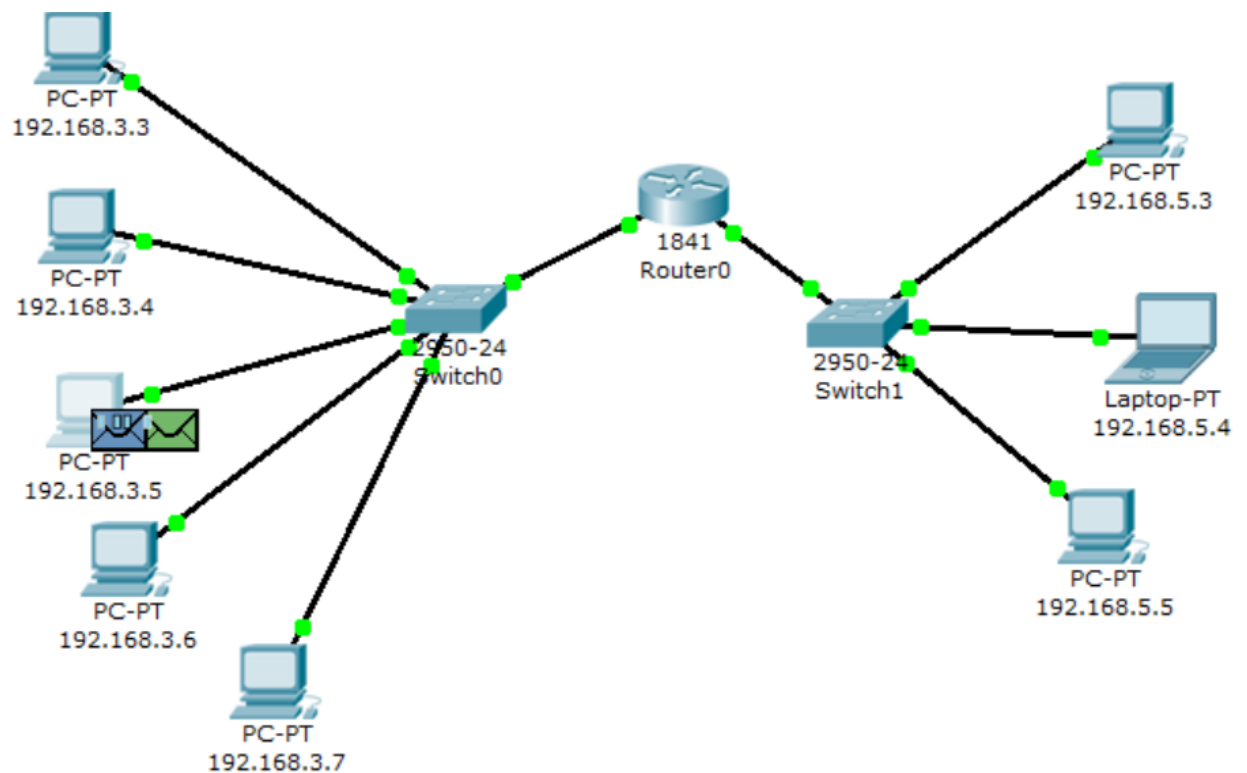
  1    4 ms    4 ms    4 ms    192.168.3.1
  2    8 ms    8 ms    8 ms    192.168.5.3

Trace complete.
```

Результат предсказуемый, так как мы имеем дело лишь с двумя сетями, которые связаны маршрутизатором.

- Источник: 192.168.3.5 Приемник: 192.168.3.4

Такой запрос происходит в пределах одной сети.



ARP запрос:

### Ethernet II

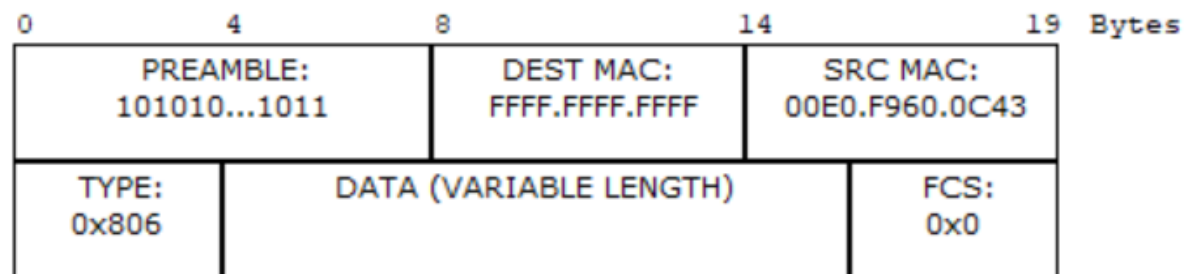
0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: FFFF.FFFF.FFFF		SRC MAC: 00E0.F960.0C43	
TYPE: 0x806		DATA (VARIABLE LENGTH)			FCS: 0x0

### ARP

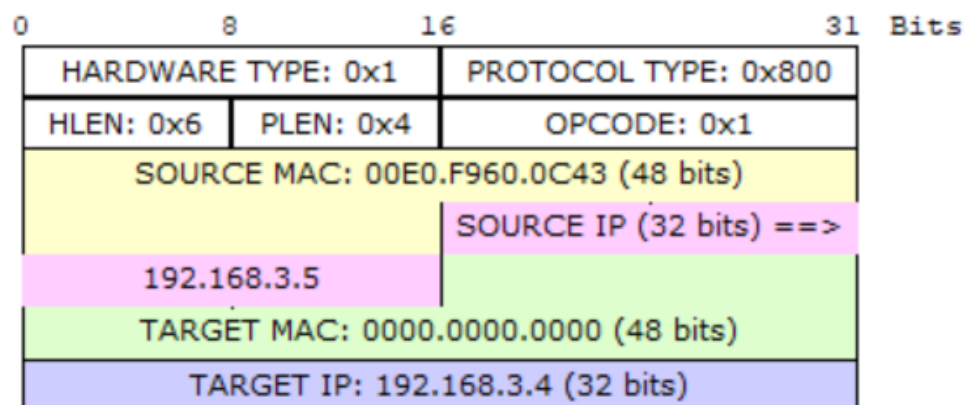
0	8	16	31	Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800		
HLEN: 0x6		PLEN: 0x4	OPCODE: 0x1	
SOURCE MAC: 00E0.F960.0C43 (48 bits)			SOURCE IP (32 bits) ==>	
192.168.3.5				
TARGET MAC: 0000.0000.0000 (48 bits)				
TARGET IP: 192.168.3.5 (32 bits)				

## PDU Formats

### Ethernet II



### ARP



Все также формируется ARP запрос для определения адреса.

ARP ответ:

### Ethernet II

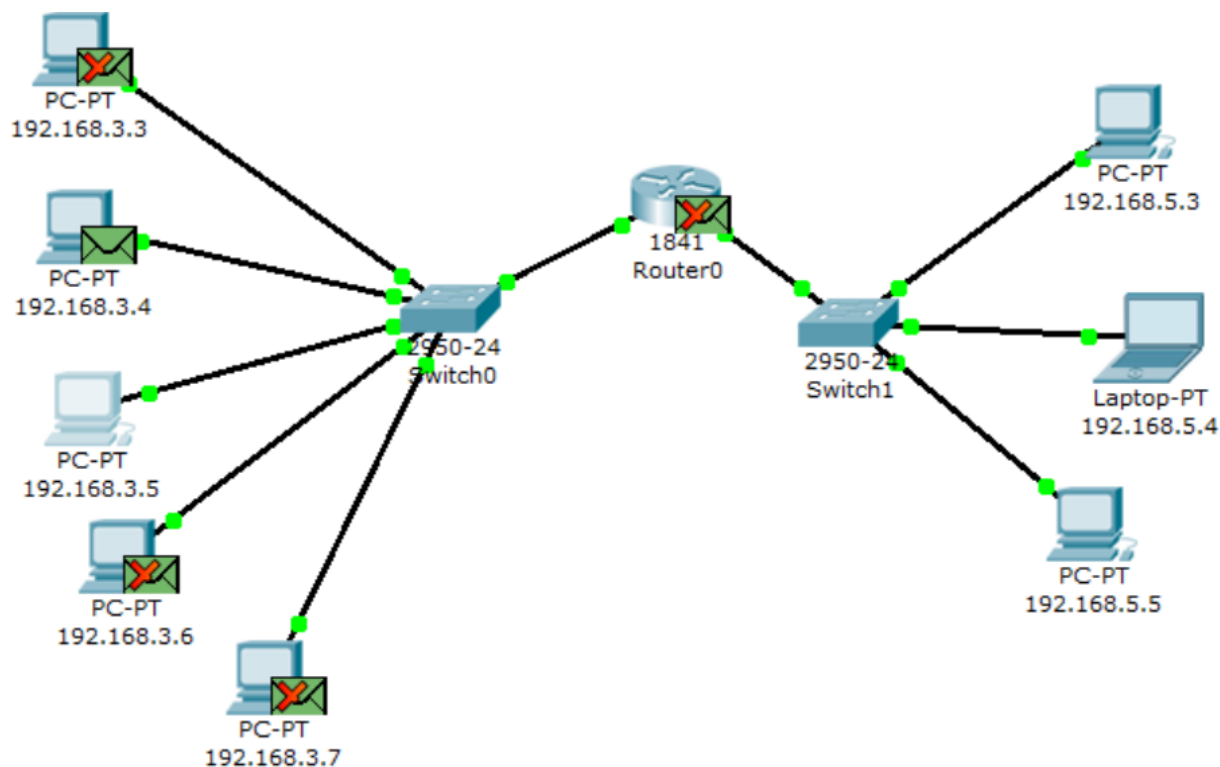
0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00E0.F960.0C43		SRC MAC: 000C.851D.AAD6	
TYPE: 0x806		DATA (VARIABLE LENGTH)			FCS: 0x0

### ARP

0	8	16	31	Bits
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800		
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x2		
SOURCE MAC: 000C.851D.AAD6 (48 bits)		SOURCE IP (32 bits) ==>		
192.168.3.4				
TARGET MAC: 00E0.F960.0C43 (48 bits)				
TARGET IP: 192.168.3.5 (32 bits)				



После ARP ответа последует ICMP запрос:



Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	--	192.168.3.5	ICMP	
	0.005	192.168.3.5	Switch0	ICMP	
	0.006	Switch0	192.168.3.4	ICMP	
	0.007	192.168.3.4	Switch0	ICMP	
	0.008	Switch0	192.168.3.5	ICMP	

ICMP ответ:

### IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 128		
ID: 0x18			0x0	0x0	
TTL: 128		PRO: 0x1	CHKSUM		
SRC IP: 192.168.3.4					
DST IP: 192.168.3.5					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

### ICMP

0	8	16	31 Bits
TYPE: 0x0		CODE: 0x0	CHECKSUM
ID: 0x4			SEQ NUMBER: 8

```
PC>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=8ms TTL=128
Reply from 192.168.3.4: bytes=32 time=4ms TTL=128
Reply from 192.168.3.4: bytes=32 time=4ms TTL=128
Reply from 192.168.3.4: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 8ms, Average = 5ms
```

Поскольку этот запрос происходил в пределах одной сети, то никакие потери, связанные с маршрутизатором, не произошли.

Отследим маршрут:

```
PC>tracert 192.168.3.4

Tracing route to 192.168.3.4 over a maximum of 30 hops:

  1    4 ms    4 ms    4 ms    192.168.3.4

Trace complete.
```

И как мы видим, из пути у нас есть только конечный узел.

#### **Вывод:**

ARP протоколы служат для определения MAC адреса по заданному IP адресу, что позволяет определить нужные маршруты для последующих протоколов таких как ICMP. Принцип построения маршрута зависит от нахождения узла, локальная сети или же внешняя, связанная маршрутизаторам, что может породить некоторые потери, прежде чем сформировать таблицы ARP запросов, которые в свою очередь ускоряют запросы по повторным адресам.

Таким образом, благодаря таким протоколам, сети с разными топологиями, могут эффективно находить необходимые узлы и оптимизировать повторные запросы к ним.