МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

ОТЧЕТ

по лабораторной работе №3

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

_____ _____Гай В. Е._____

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

_____ ___Пигасин Д. А.___

(подпись) (фамилия, и.,о.)

_____18-АС_____

(шифр группы)

Работа защищена «___» _____

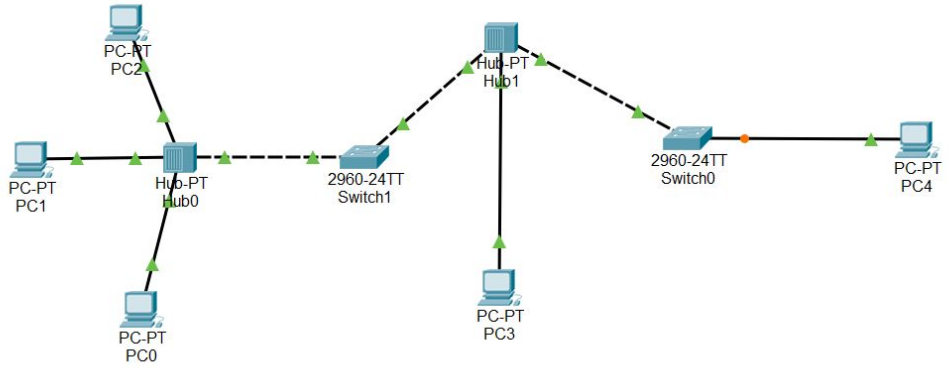
С оценкой _____

Нижний Новгород 2020

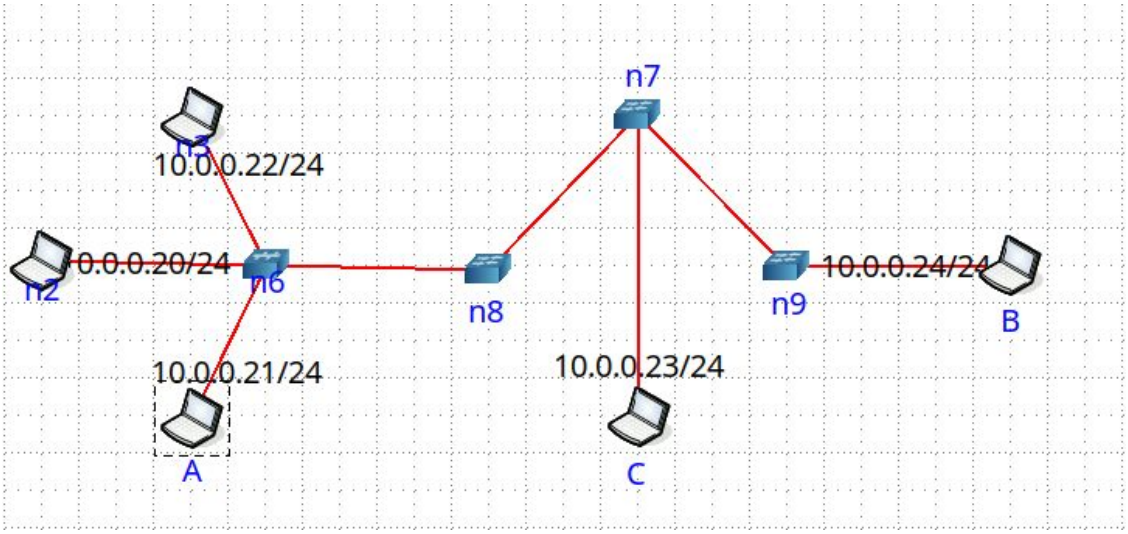
Задание

Знакомство с особенностями работы ARP протокола на примере атаки ARP-spoofing.

Вариант 2 (лаб 1)

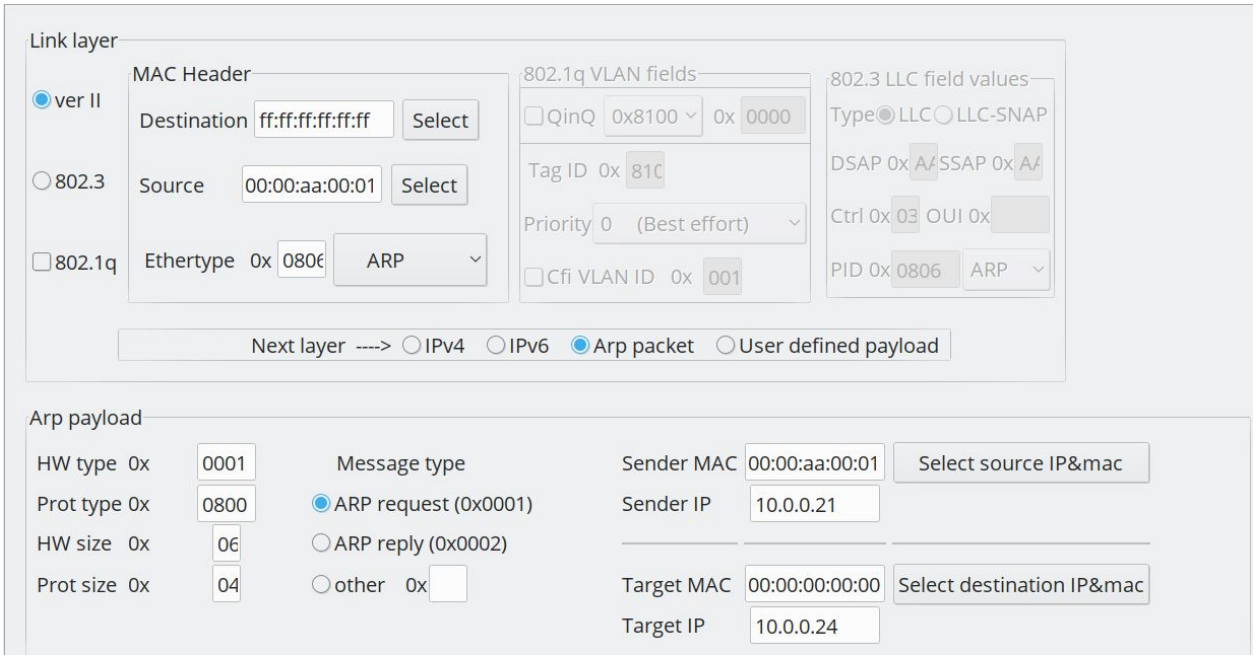


Собранная схема



ARP request (packeth)

Отправляем широковещательный ARP запрос с компьютера A, чтобы узнать MAC адрес связанный с 10.0.0.24



Компьютер A

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00_aa:00:01	Broadcast	ARP	60	Who has 10.0.0.24? Tell 10.0.0.21
2	0.000123883	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03

Компьютер B

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00_aa:00:01	Broadcast	ARP	60	Who has 10.0.0.24? Tell 10.0.0.21
2	0.000028067	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03

Компьютер C

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00_aa:00:01	Broadcast	ARP	60	Who has 10.0.0.24? Tell 10.0.0.21

Так как APR reply от B к A идет уже напрямую, компьютер C его не видит.

Запускаем чат между A и B (netcat)

Компьютер A

```
root@A:/tmp/pycore.44487/A.conf# netcat -lp 9000
hi
root
toor
```

Компьютер B

```
root@B:/tmp/pycore.44487/B.conf# netcat 10.0.0.21 9000
hi
root
toor
```

Компьютер A

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.24	TCP	69	9000 → 56274 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=3 TSval=18605…
2	0.000102106	10.0.0.24	10.0.0.21	TCP	66	56274 → 9000 [ACK] Seq=1 Ack=4 Win=502 Len=0 TSval=3510069739…
3	5.203377364	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
4	5.203477211	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
5	5.203496231	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
6	5.203523538	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
7	152.941519268	10.0.0.24	10.0.0.21	S101	71	56274 → 9000 [PSH, ACK] Seq=1 Ack=4 Win=502 Len=5 TSval=35102…
8	152.941564615	10.0.0.21	10.0.0.24	TCP	66	9000 → 56274 [ACK] Seq=4 Ack=6 Win=510 Len=0 TSval=1860680367…
9	158.035510489	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
10	158.035603966	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
11	158.035626609	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
12	158.035643263	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
13	189.269342321	10.0.0.21	10.0.0.24	S101	71	9000 → 56274 [PSH, ACK] Seq=4 Ack=6 Win=510 Len=5 TSval=18607…
14	189.269451763	10.0.0.24	10.0.0.21	TCP	66	56274 → 9000 [ACK] Seq=6 Ack=9 Win=502 Len=0 TSval=3510259009…

Компьютер B

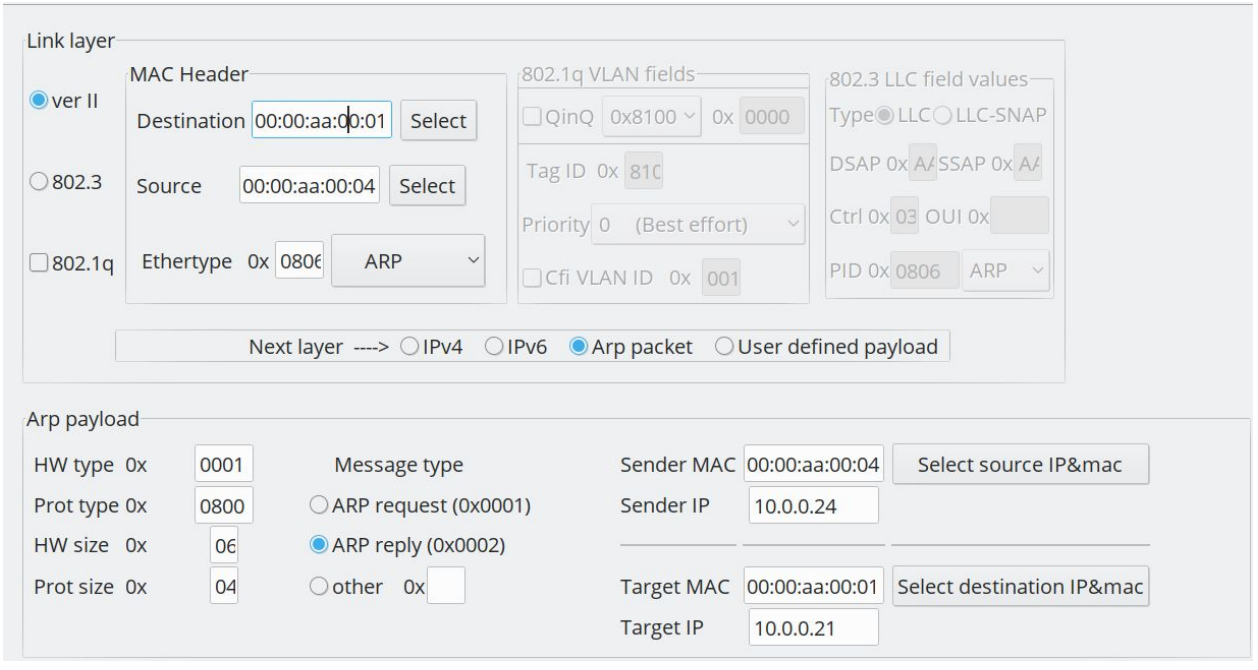
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.24	TCP	69	9000 → 56274 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=3 TSval=18605…
2	0.000044208	10.0.0.24	10.0.0.21	TCP	66	56274 → 9000 [ACK] Seq=1 Ack=4 Win=502 Len=0 TSval=3510069739…
3	5.203313182	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
4	5.203438253	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
5	5.203461257	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
6	5.203476341	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
7	152.941433320	10.0.0.24	10.0.0.21	S101	71	56274 → 9000 [PSH, ACK] Seq=1 Ack=4 Win=502 Len=5 TSval=35102…
8	152.941540036	10.0.0.21	10.0.0.24	TCP	66	9000 → 56274 [ACK] Seq=4 Ack=6 Win=510 Len=0 TSval=1860680367…
9	158.035486287	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
10	158.035555732	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
11	158.035576423	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
12	158.035603027	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
13	189.269345376	10.0.0.21	10.0.0.24	S101	71	9000 → 56274 [PSH, ACK] Seq=4 Ack=6 Win=510 Len=5 TSval=18607…
14	189.269388838	10.0.0.24	10.0.0.21	TCP	66	56274 → 9000 [ACK] Seq=6 Ack=9 Win=502 Len=0 TSval=3510259009…

Компьютер C

No.	Time	Source	Destination	Protocol	Length	Info

Реализация атаки ARP-spoofing

Отправляем ARP reply, в котором указан ip компьютера B и MAC адрес компьютера C на компьютер A.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00_aa:00:04	00:00:00_aa:00:01	ARP	60	10.0.0.24 is at 00:00:00:aa:00:04

ARP таблица компьютера A до и после отправки пакета

```
root@A:/tmp/pycore.44487/A.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.24                ether   00:00:00:aa:00:03   C                     eth0
root@A:/tmp/pycore.44487/A.conf# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
10.0.0.24                ether   00:00:00:aa:00:04   C                     eth0
root@A:/tmp/pycore.44487/A.conf#
```

Отправляем еще одно сообщение

Компьютер A

```
root@A:/tmp/pycore.46377/A.conf# netcat -lp 9000
hi
root
toor
notForC
```

Компьютер B

```
root@B:/tmp/pycore.46377/B.conf# netcat 10.0.0.21 9000
hi
root
toor
```

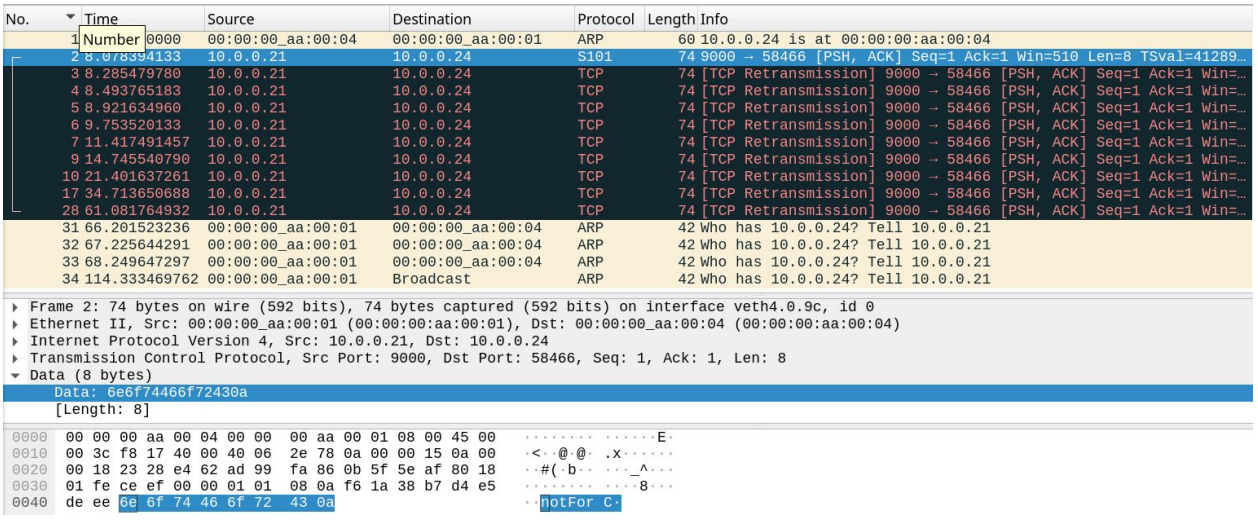
Компьютер A

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.24	TCP	69	9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=3 TSval=41288…
2	0.000122037	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=1 Ack=4 Win=502 Len=0 TSval=3571823033…
3	4.662280968	10.0.0.24	10.0.0.21	S101	71	58466 → 9000 [PSH, ACK] Seq=1 Ack=4 Win=502 Len=5 TSval=35718…
4	4.662320314	10.0.0.21	10.0.0.24	TCP	66	9000 → 58466 [ACK] Seq=4 Ack=6 Win=510 Len=0 TSval=4128892715…
5	5.069089132	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
6	5.069100245	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
7	11.573662157	10.0.0.21	10.0.0.24	S101	71	9000 → 58466 [PSH, ACK] Seq=4 Ack=6 Win=510 Len=5 TSval=41288…
8	11.573712994	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=6 Ack=9 Win=502 Len=0 TSval=3571834606…
9	17.459616478	00:00:00_aa:00:04	00:00:00_aa:00:01	ARP	60	10.0.0.24 is at 00:00:00:aa:00:04
10	25.537935736	10.0.0.21	10.0.0.24	S101	74	9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=510 Len=8 TSval=41289…
11	25.744964932	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
12	25.953270372	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
13	26.381160143	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
14	27.213057438	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
15	28.877024159	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
16	32.205031728	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
17	38.861149800	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
24	52.173168885	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
35	78.541296027	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
38	83.661013202	00:00:00_aa:00:01	00:00:00_aa:00:04	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
39	84.685166795	00:00:00_aa:00:01	00:00:00_aa:00:04	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
40	85.709158167	00:00:00_aa:00:01	00:00:00_aa:00:04	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
42	131.793007386	00:00:00_aa:00:01	Broadcast	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
43	131.793067420	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
44	131.793070878	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=…
45	131.793092681	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=6 Ack=17 Win=502 Len=0 TSval=357195482…
46	136.909231521	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
47	136.909253449	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01

Компьютер B

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.24	TCP	69	9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=3 TSval=41288…
2	0.000055660	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=1 Ack=4 Win=502 Len=0 TSval=3571823033…
3	4.662199446	10.0.0.24	10.0.0.21	S101	71	58466 → 9000 [PSH, ACK] Seq=1 Ack=4 Win=502 Len=5 TSval=35718…
4	4.662297187	10.0.0.21	10.0.0.24	TCP	66	9000 → 58466 [ACK] Seq=4 Ack=6 Win=510 Len=0 TSval=4128892715…
5	5.069013238	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
6	5.069060986	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
7	11.573642014	10.0.0.21	10.0.0.24	S101	71	9000 → 58466 [PSH, ACK] Seq=4 Ack=6 Win=510 Len=5 TSval=41288…
8	11.573660790	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=6 Ack=9 Win=502 Len=0 TSval=3571834606…
28	131.793010210	00:00:00_aa:00:01	Broadcast	ARP	42	Who has 10.0.0.24? Tell 10.0.0.21
29	131.793016653	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	10.0.0.24 is at 00:00:00:aa:00:03
30	131.793032907	10.0.0.21	10.0.0.24	S101	74	9000 → 58466 [PSH, ACK] Seq=9 Ack=6 Win=510 Len=8 TSval=41290…
31	131.793040186	10.0.0.24	10.0.0.21	TCP	66	58466 → 9000 [ACK] Seq=6 Ack=17 Win=502 Len=0 TSval=357195482…
32	136.909117537	00:00:00_aa:00:03	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.24
33	136.909221841	00:00:00_aa:00:01	00:00:00_aa:00:03	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01

Компьютер C (перехваченное сообщение)



Компьютер A, не получив подтверждения о доставки сообщения, начинает отправлять ARP запросы для уточнения физического адреса связанного с сетевым 10.0.0.24. Сначала он отправляет их опираясь на свою ARP таблицу с неверными данными. Не получив ответа A формирует широковещательный пакет, B отвечает, после чего соединение восстанавливается и сообщение приходит.

Компьютер A

```
root@A:/tmp/pycore.46377/A.conf# netcat -lp 9000
hi
root
toor
notForC
```

Компьютер B

```
root@B:/tmp/pycore.46377/B.conf# netcat 10.0.0.21 9000
hi
root
toor
notForC
```