

МИНОБРАЗОВАНИЯ 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:

(подпись)

Гай В. Е.
(фамилия, и.,о.)

СТУДЕНТ:

(подпись)

Пигасин Д. А.
(фамилия, и.,о.)

18-АС
(шифр группы)

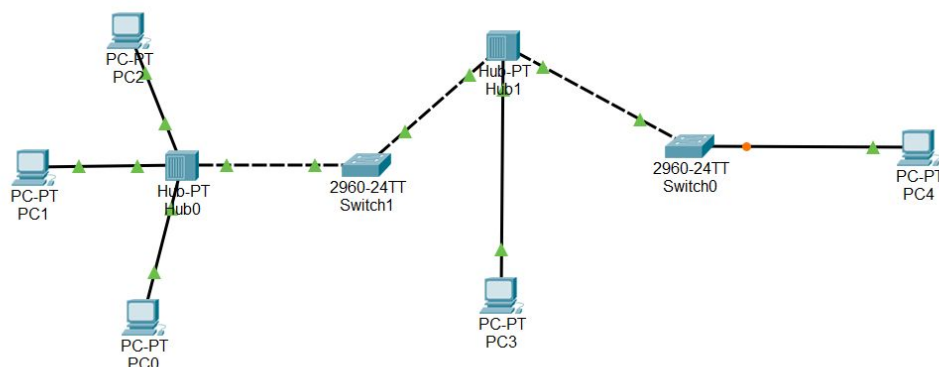
Работа защищена «__» _____

С оценкой _____

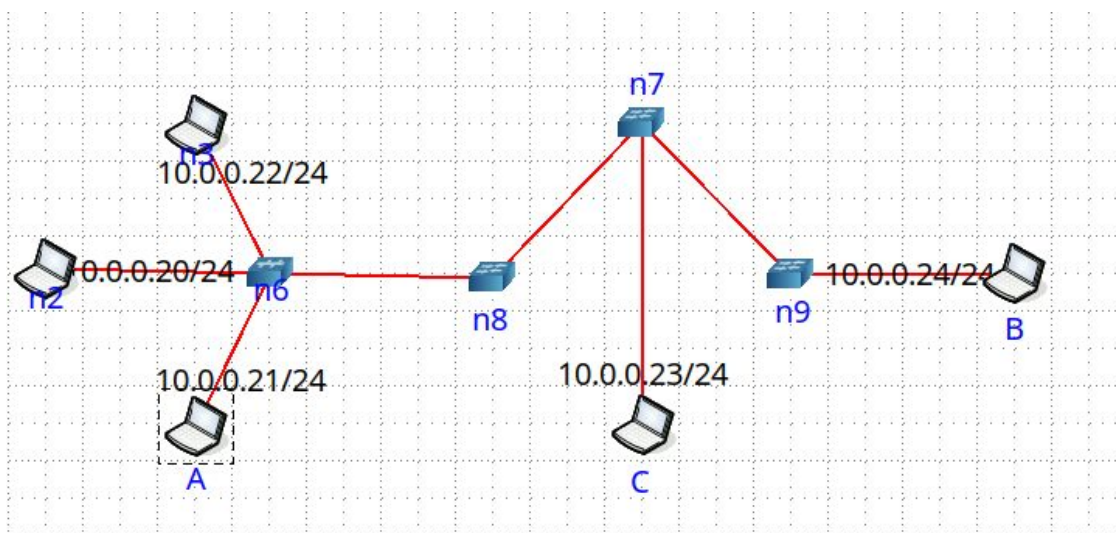
Задание

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 А, чтобы узнать MAC адрес связанный с 10.0.0.24

Link layer

☒ ver II

MAC Header

Destination ff:ff:ff:ff:ff:ff Select

Source 00:00:aa:00:01 Select

Ethertype 0x 0806 ARP

802.1q VLAN fields

☐ QinQ 0x8100 0x 0000

Tag ID 0x 81C

Priority 0 (Best effort)

☐ Cfi VLAN ID 0x 001

802.3 LLC field values

Type ☒ LLC ☐ LLC-SNAP

DSAP 0x AA SSAP 0x AA

Ctrl 0x 03 OUI 0x

PID 0x 0806 ARP

Next layer ----> ☐ IPv4 ☐ IPv6 ☒ Arp packet ☐ User defined payload

Arp payload

HW type 0x 0001 Message type ☒ ARP request (0x0001) ☐ ARP reply (0x0002) ☐ other 0x

Prot type 0x 0800

HW size 0x 06

Prot size 0x 04

Sender MAC 00:00:aa:00:01 Select source IP&mac

Sender IP 10.0.0.21

Target MAC 00:00:00:00:00 Select destination IP&mac

Target IP 10.0.0.24

Компьютер А

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 В

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 С

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 ARP reply от В к А идет уже напрямую, компьютер С его не видит.

Запускаем чат между А и В (netcat)

Компьютер А

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

Компьютер В

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

Компьютер А

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 В

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 С

No.	Time	Source	Destination	Protocol	Length	Info

Реализация атаки ARP-spoofing

Отправляем ARP reply, в котором указан ip компьютера В и MAC адрес компьютера С на компьютер А.

Link layer

ver II

802.3

802.1q

MAC Header

Destination 00:00:aa:00:01 Select

Source 00:00:aa:00:04 Select

Ethertype 0x 0806 ARP

802.1q VLAN fields

QinQ

0x8100

0x 0000

Tag ID

0x 810

Priority

0 (Best effort)

Cfi VLAN ID

0x 001

802.3 LLC field values

Type LLC LLC-SNAP

DSAP 0x AA

SSAP 0x AA

Ctrl 0x 03

OUI 0x

PID 0x 0806

ARP

Next layer ---->

IPv4

IPv6

Arp packet

User defined payload

Arp payload

HW type 0x 0001

Prot type 0x 0800

HW size 0x 06

Prot size 0x 04

Message type

ARP request (0x0001)

ARP reply (0x0002)

other 0x

Sender MAC 00:00:aa:00:04 Select source IP&mac

Sender IP 10.0.0.24

Target MAC 00:00:aa:00:01 Select destination IP&mac

Target IP 10.0.0.21

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 А 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 А

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

Компьютер В

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

Компьютер А

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 В

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 С (перехваченное сообщение)

No.	Time	Source	Destination	Protocol	Length	Info
1	8.078394133	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
2	8.285479780	10.0.0.21	10.0.0.24	S101	74	9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=8 TSval=41289...
3	8.493765183	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
4	8.921634960	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
5	8.921634960	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
6	9.753520133	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
7	11.417491457	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
8	14.745540790	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
9	21.401637261	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
10	34.713650688	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
11	61.081764932	10.0.0.21	10.0.0.24	TCP	74	[TCP Retransmission] 9000 → 58466 [PSH, ACK] Seq=1 Ack=1 Win=...
12	66.201523236	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
13	67.225644291	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
14	68.249647297	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
15	114.333469762	00:00:00_aa:00:01	Broadcast	ARP	42	who has 10.0.0.24? Tell 10.0.0.21
▶ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface veth4.0.9c, id 0						
▶ Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:04 (00:00:00:aa:00:04)						
▶ Internet Protocol Version 4, Src: 10.0.0.21, Dst: 10.0.0.24						
▶ Transmission Control Protocol, Src Port: 9000, Dst Port: 58466, Seq: 1, Ack: 1, Len: 8						
▼ Data (8 bytes)						
Data: 6e6f74466f72430a						
[Length: 8]						
0000	00 00 00 aa 00 04 00 00	00 aa 00 01 08 00 45 00E.			
0010	00 3c f8 17 40 00 40 06	2e 78 0a 00 00 15 0a 00	.<.@.X.....			
0020	00 18 23 28 e4 62 ad 99	fa 86 0b 5f 5e af 80 18	#(.b.....^...			
0030	01 fe ce ef 00 00 01 01	08 0a f6 1a 38 b7 d4 e58...			
0040	de ee 6e 6f 74 46 6f 72	43 0a	notFor C			

Компьютер А, 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 А формирует широковещательный пакет, В отвечает, после чего соединение восстанавливается и сообщение приходит.

Компьютер А

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

Компьютер В

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