

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования



НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №3

Вариант 17

по дисциплине

«Сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

(подпись)

Гай В. Е.

(фамилия, и.,о.)

СТУДЕНТ:

(подпись)

Сухоруков В.А.

(фамилия, и.,о.)

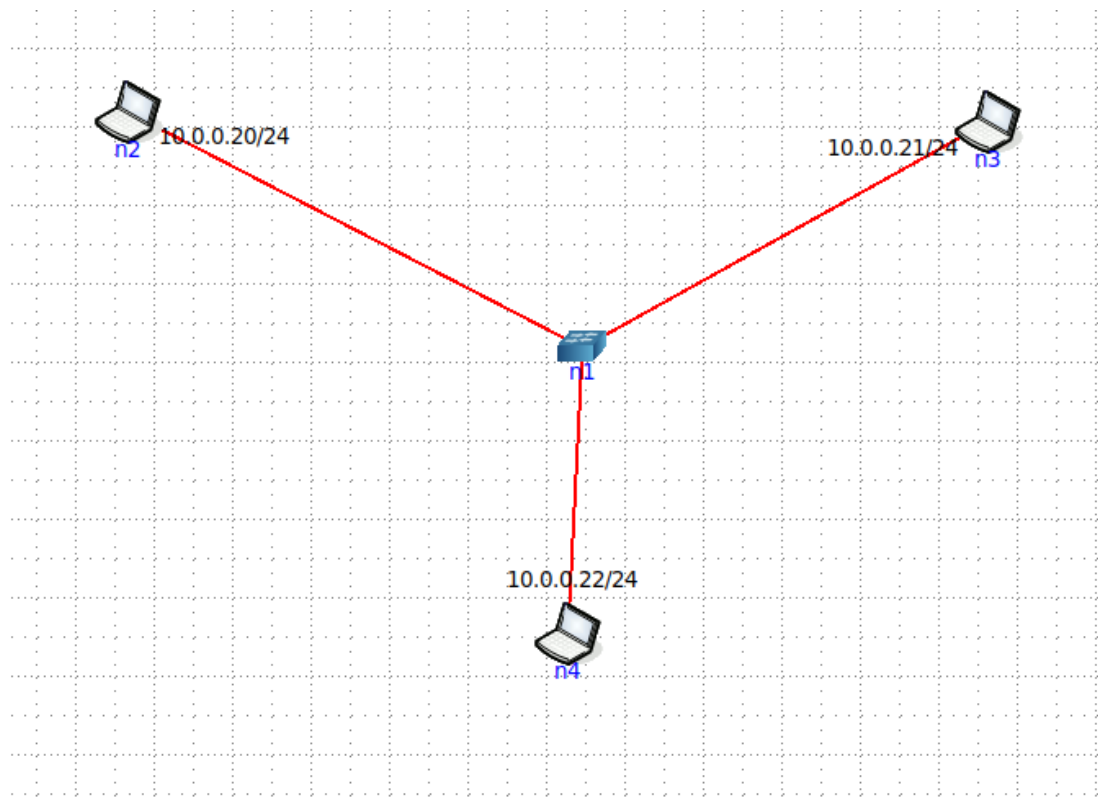
19-В-2

(шифр группы)

Работа защищена «__» _____

С оценкой _____

Схема сети



Примеры использования программ

Создание ARP запроса с помощью PackETH

PACKETH - ethernet packet generator (на n2)

File Help

Builder Gen-b Gen-s Pcap Load Save Default Default Interface Send Stop

Link layer

☒ ver II

☐ 802.3

☐ 802.1q

MAC Header

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

Source 00:00:00:aa:00:00 Select

Ethertype 0x 0806 ARP

802.1q VLAN fields

☐ QinQ 0x8100 0x 0000

Tag ID 0x 8100

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 00:00:00:aa:00:00 Select source IP&mac

Sender IP 10.0.0.20

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

Target IP 10.0.0.21

Обнаружение запроса с помощью Wireshark

The image shows the Wireshark interface capturing traffic from veth2.0.fo. The packet list shows two ARP packets. The selected packet (No. 2) is an ARP request from 00:00:00:aa:00:01 to 00:00:00:aa:00:00. The packet details pane shows the Ethernet II header, IPv4 header, and the ARP request structure. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	00:00:00:aa:00:00	Broadcast	ARP	60	Who has 10.0.0.21? Tell 10.0.0.20
2	0.000020859	00:00:00:aa:00:01	00:00:00:aa:00:00	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: 00:00:00:aa:00:00 (00:00:00:aa:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: 00:00:00:aa:00:00 (00:00:00:aa:00:00)
Sender IP address: 10.0.0.20
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 10.0.0.21

0000 ff ff ff ff ff ff 00 00 00 aa 00 00 08 06 00 01
0010 08 00 06 04 00 01 00 00 00 aa 00 00 0a 00 00 14
0020 00 00 00 00 00 00 0a 00 00 15 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Target MAC address (arp.dst.hw_mac), 6 bytes

Packets: 2 · Displayed: 2 (100.0%) Profile: Default

Вывод таблицы Mac адресов командой arp

The image shows a terminal window titled "Терминал" with the output of the 'arp' command. The output displays a table of IP addresses, hardware types, hardware addresses, flags, masks, and interfaces.

```
Файл Правка Вид Поиск Терминал Справка
root@n3:/tmp/pycore.45377/n3.conf# arp
Адрес HW-тип HW-адрес Флаги Маска Интерфейс
10.0.0.20 ether 00:00:00:aa:00:00 C eth0
root@n3:/tmp/pycore.45377/n3.conf#
```

Исследование протокола ARP на безопасность

Установление соединения между узлами n2 и n3 с помощью netcat

```
root@n2:/tmp/pycore.45377/n2.conf# nc -lp 9000
```

```
root@n3:/tmp/pycore.45377/n3.conf# nc 10.0.0.20 9000
```

Capturing from veth3.0.f0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression... +						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.20	TCP	66	33228 → 9000 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSv
2	0.000056837	10.0.0.20	10.0.0.21	TCP	66	9000 → 33228 [FIN, ACK] Seq=1 Ack=2 Win=510 Len=0 TSv
3	0.000063940	10.0.0.21	10.0.0.20	TCP	66	33228 → 9000 [ACK] Seq=2 Ack=2 Win=502 Len=0 TSval=23
4	5.020924031	00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
5	5.020880860	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.20? Tell 10.0.0.21
6	5.020932958	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
7	5.020936304	00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	42	10.0.0.20 is at 00:00:00:aa:00:00

Передача пакета с n2 на n3

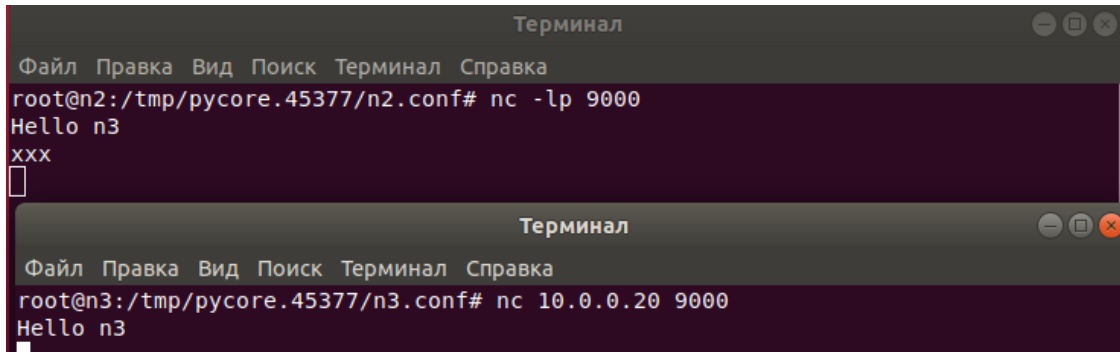
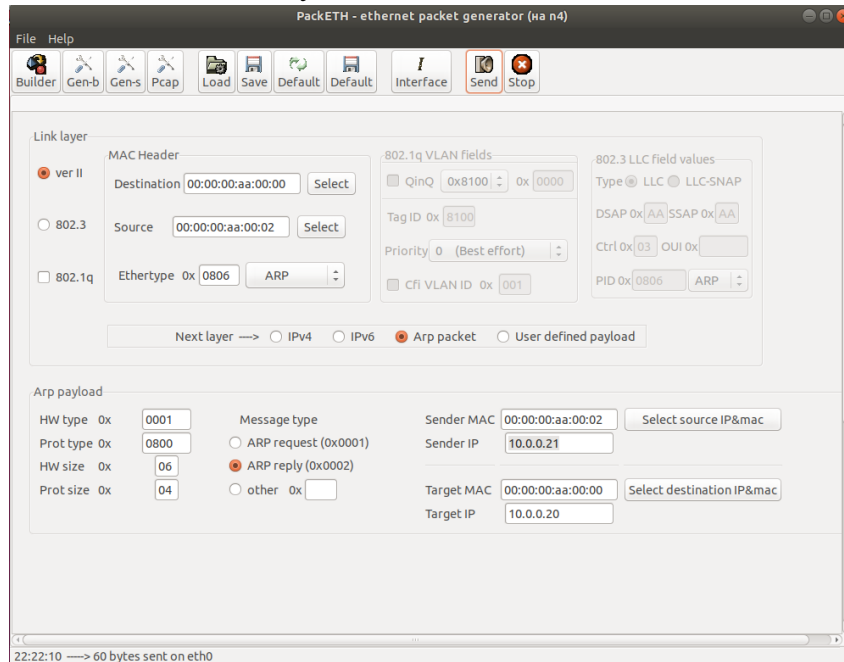
```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.45377/n2.conf# nc -lp 9000
Hello n3

Терминал
Файл Правка Вид Поиск Терминал Справка
root@n3:/tmp/pycore.45377/n3.conf# nc 10.0.0.20 9000
Hello n3
```

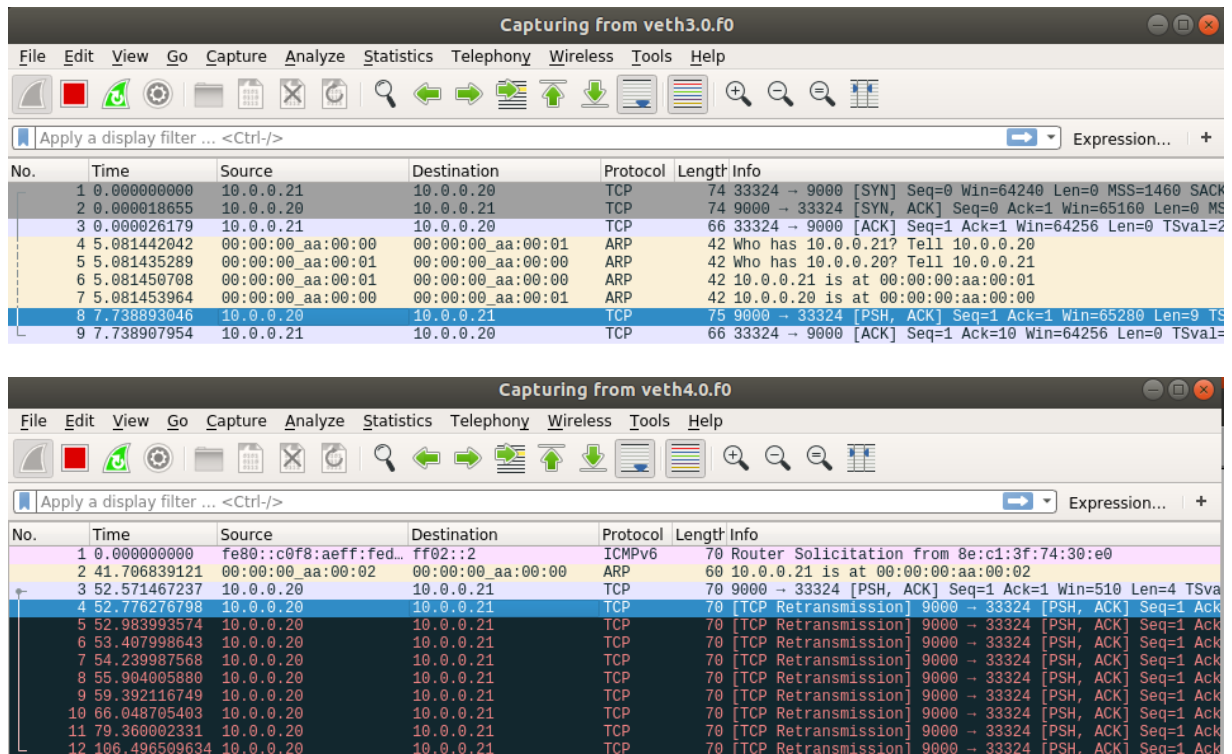
17	191.926397157	10.0.0.20	10.0.0.21	TCP	75	9000 → 33272 [PSH, ACK] Seq=10 Ack=1 Win=65280 Len=9 T
18	191.926406374	10.0.0.21	10.0.0.20	TCP	66	33272 → 9000 [ACK] Seq=1 Ack=19 Win=64256 Len=0 TSval=

0000	00 00 00 aa 00 01 00 00	00 aa 00 00 08 00 45 00E.
0010	00 3d 6a 8e 40 00 40 06	bc 04 0a 00 00 14 0a 00	..=j.@.@.....
0020	00 15 23 28 81 f8 b0 7a	4b 15 71 15 a2 cd 80 18	..#(...z K.q....
0030	01 fe 4f b0 00 00 01 01	08 0a 7e 67 95 37 8c 5a	..0.....~g.7.Z
0040	20 23 48 65 6c 6c 6f 20	6e 33 0a	#Hello n3.

Захват пакета узлом n4 с помощью PackETH



Узел n3 не получает сообщения «xxx», его перехватывает n4.



Ответа на TCP протокол не поступает, поэтому n2 генерирует ARP запрос, который получает n3 и соединение между ними восстанавливается.

Wireshark capture from veth4.0.f0. The capture shows a series of TCP retransmissions from n2 to n3 on port 9000, followed by an ARP request from n2 to n3 and a broadcast ARP request. The interface is set to 'veth4.0.f0'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::c0f8:aef:fed...	ff02::2	ICMPv6	70	Router Solicitation from 8e:c1:3f:74:30:e0
2	41.706839121	00:00:00_aa:00:02	00:00:00_aa:00:00	ARP	60	10.0.0.21 is at 00:00:00:aa:00:02
3	52.571467237	10.0.0.20	10.0.0.21	TCP	70	9000 → 33324 [PSH, ACK] Seq=1 Ack=1 Win=510 Len=4 TSva
4	52.776276798	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
5	52.983993574	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
6	53.407998643	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
7	54.239987568	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
8	55.904005880	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
9	59.392116749	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
10	66.048705403	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
11	79.360002331	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
12	106.496509634	10.0.0.20	10.0.0.21	TCP	70	[TCP Retransmission] 9000 → 33324 [PSH, ACK] Seq=1 Ack
13	111.616017556	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
14	112.640570273	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
15	113.664049092	00:00:00_aa:00:00	00:00:00_aa:00:02	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
16	159.744027144	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20

Wireshark capture from veth3.0.f0. The capture shows a series of TCP retransmissions from n2 to n3 on port 9000, followed by an ARP request from n2 to n3 and a broadcast ARP request. The interface is set to 'veth3.0.f0'.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.21	10.0.0.20	TCP	74	33324 → 9000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
2	0.000018655	10.0.0.20	10.0.0.21	TCP	74	9000 → 33324 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MS
3	0.000026179	10.0.0.21	10.0.0.20	TCP	66	33324 → 9000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2
4	5.081442042	00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
5	5.081435289	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	Who has 10.0.0.20? Tell 10.0.0.21
6	5.081450708	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
7	5.081453964	00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	42	10.0.0.20 is at 00:00:00:aa:00:00
8	7.738893046	10.0.0.20	10.0.0.21	TCP	75	9000 → 33324 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=9 TS
9	7.738907954	10.0.0.21	10.0.0.20	TCP	66	33324 → 9000 [ACK] Seq=1 Ack=10 Win=64256 Len=0 TSval=
10	132.824603254	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
11	132.824614685	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01
12	132.824624664	10.0.0.20	10.0.0.21	TCP	70	9000 → 33324 [PSH, ACK] Seq=10 Ack=1 Win=65280 Len=4 T
13	132.824632078	10.0.0.21	10.0.0.20	TCP	66	33324 → 9000 [ACK] Seq=1 Ack=14 Win=64256 Len=0 TSval=

Terminal window showing the execution of the nc command on n2. The command is `nc -lp 9000`. The output is `Hello n3` and `xxx`.

```
root@n2:/tmp/pycore.45377/n2.conf# nc -lp 9000
Hello n3
xxx
```

Terminal window showing the execution of the nc command on n3. The command is `nc 10.0.0.20 9000`. The output is `Hello n3` and `xxx`.

```
root@n3:/tmp/pycore.45377/n3.conf# nc 10.0.0.20 9000
Hello n3
xxx
```