#### 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 № 2

по дисциплине

## Сети и телекоммуникации

(наименование дисциплины)

РУКОВОДИТЕЛЬ:	
(подпись)	<u>Гай В.Е.</u> (фамилия, и.,о.)
СТУДЕНТ:	
(подпись)	<u>Рыжков Н. Д</u> (фамилия, и.,о.)
	<u>17-AC</u> (шифр группы)
Работа защищена « »	
С оценкой	

## Цель:

- Получить практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом A и кадра ARP-ответа хостом B хосту A. Получение базовых навыков по работе с генераторами пакетов PackETH.
- Получить практические навыки в вычислении контрольной суммы заголовка IP-пакета.

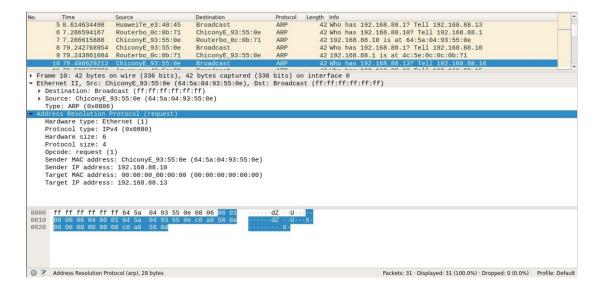
## Ход работы

#### Часть 1

1) Подготовить и записать в 16-теричном виде пример кадра для широковещательной передачи ARP-запроса хостом A и кадра ARP-ответа хостом B хосту A. В кадре ARPответа поля для MAC-адреса хоста B не заполнять. (Хост A - это ПК, за которым работает бригада студентов. IP-адрес хоста B выбирается студентом по схеме ЛВС лаб.521). IP-адрес хоста A можно узнать с помощью команд ifconfig и ip addr show.

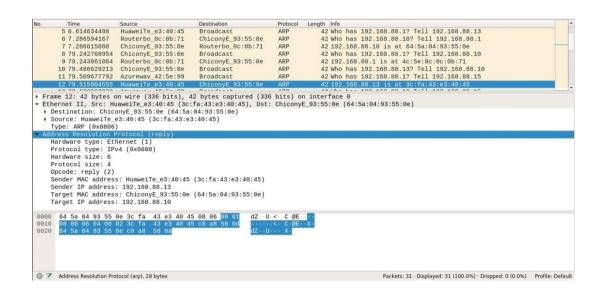
#### Кадр широковещательной передачи ARP-запроса хостом A хосту В

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Destination MAC						,	Source	MAC	1		ETHER	RTYPE	HTYPE		
ff	ff	ff	ff	ff	ff	64	5a	04	93	55	0e	08	06	00	01
PTYPE	E H	LEN	PLEN	1	OP		,	Source	MAC	1			Sour	ce IP	
				C	ODE										
08 0	00	06	04	00	01	64	5a	04	93	55	0e	c0	a8	58	0a
	Des	tinatio	n MAC			Destination IP									
00 (	00	00	00	00	00	c0		a8	58		0d				



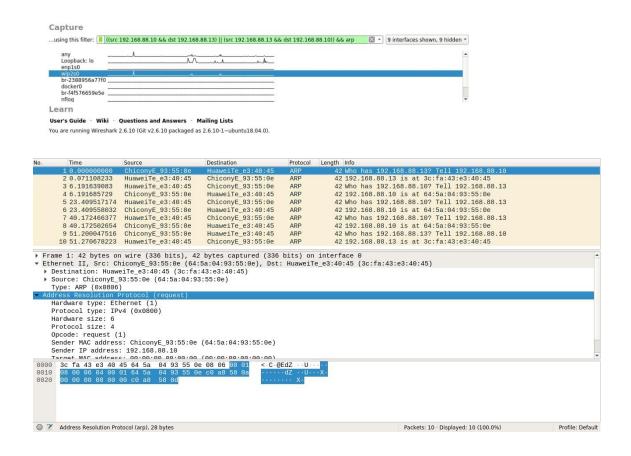
#### Кадр широковещательной передачи ARP-ответа хостом В хосту А

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Destination MAC						Source MAC						R TYPE	HTYPE		
64	5a	04	93	55	0e							08	06	00	01
PTYPE	H	LEN	PLE		OP		,	Source	MAC						
				C	ODE										
08 0	00	06	04	00	02							c0	a8	58	0d
Destination MAC					Destination IP										
64	5a (	04	93	55	0e	c0		a8	58		0a				



2) Начать захват пакетов при помощи любого из изученных анализаторов протоколов. Захват проводить по фильтру (IP-адреса источника и получателя, протокол ARP; для tcpdump дополнительно указать размер пакета 1500 байт, а также флаг отображения пакета (включая заголовок кадра Ethernet) в 16-теричном и ASCII виде).

```
PING 192.168.88.13 (192.168.88.13) 56(84) bytes of data.
  bytes from 192.168.88.13: icmp_seq=1 ttl=64 time=243 ms
bytes from 192.168.88.13: icmp_seq=2 ttl=64 time=19.5 m
bytes from 192.168.88.13: icmp_seq=3 ttl=64 time=43.6 m
                                                   ttl=64 time=19.5 ms
64
                                                                          ms
   bytes from 192.168.88.13: icmp_seq=4 ttl=64 time=65.2 ms
64
   bytes from 192.168.88.13:
bytes from 192.168.88.13:
                                    icmp_seq=5
icmp_seq=6
                                                    ttl=64
                                                             time=84.8 ms
64
                                                   ttl=64
                                                             time=110 ms
   bytes from 192.168.88.13:
64
                                     icmp_seq=7
                                                   ttl=64
                                                            time=29.0 ms
64
   bytes
           from
                  192.168.88.13:
                                     icmp_seq=8
                                                   ttl=64
                                                             time=51.9
                                                                          ms
   bytes from 192.168.88.13:
                                     icmp_seq=9 ttl=64 time=75.9
                                                                         ms
                                     icmp_seq=10 ttl=64 time=201 ms
   bytes from 192.168.88.13:
           from
                  192.168.88.13:
                                     icmp_seq=11
                                                     ttl=64 time=19.6 ms
```

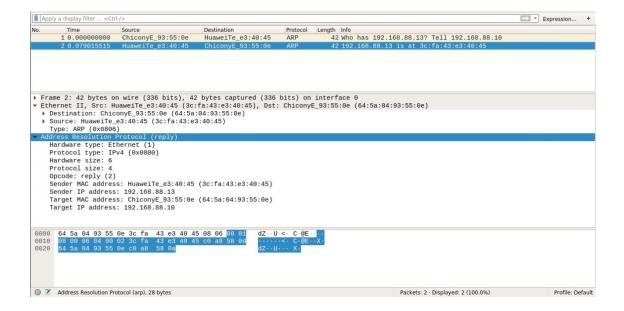


3) Сформировать кадр ARP-запроса с помощью утилиты packit и отправить его в сеть. Команду сохранить для отчета.

Команда:

sudo packit -m inject -t ARP -c 1 -A 1 -y 192.168.88.13 -Y 3c:fa:43:e3:40:45 -x 192.168.88.10 -X 64:5A:04:93:55:0E -E 3c:fa:43:e3:40:45 -i wlp2s0

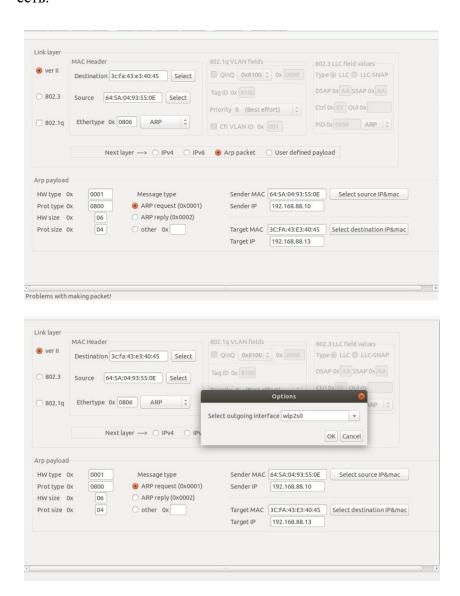
4) Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.



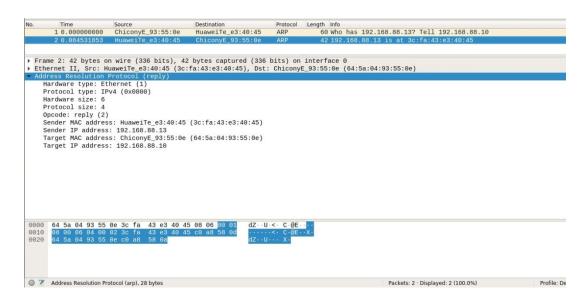
5) Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.

Полученный ARP-ответ совпадает с ARP-ответом из 1 пункта.

6) Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть.



7) Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета.



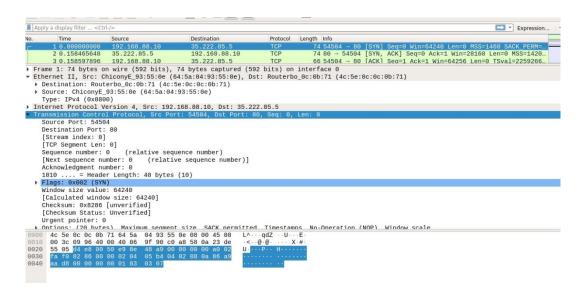
8) Сравнить полученный ARP-ответ с подготовленным в первом пункте примером.

Полученный ARP-ответ совпадает с ARP-ответом из 1 пункта.

#### Часть 2

#### Ход работы:

#### 1) Захваченный пакет



2) Согласно материалам из рекомендованных источников "разбить" заданный кадр на поля.

					Заголо	вок Е	(ther	netOrta,	др <b>Ю</b> 5	b4	04	. (	02	08	0a	86	9a	aa	d8 II	9 00	00	00	00		
МАС получателя МАС						МАС отправителяТСР ТҮРЕ					VERSI IHL Differen			erentia ervice											
											OPT	IONS	S			Code Point									
4c	5e	0c	0c	0b		71	64	5a	04	93	55	0e	08	00	)	45					00				
				N	o-Opera	ition											Wir	idow s	cale						
											I	Р													
					01									03				03				07			
	OTA		IDE	NTIFI	CATI	FL	AGS	5	TTL		ROT	<u> </u>		EAD					S	OURC	Έ				
Ll	ENGT			ON								OCOL				ECK!									
00		3c	09	)	96	40		00	40		06		9f		9	00	c0		a8		58	0:	a		
			IP													TCP									
			11													101									
DH	ESTIN	ATIO	N	SI	RC POR	Т		DE	ST PC	RT		SEGMENT					Acknowledgment				HLEN(1010),				
													NUMBER				NUMBER				FLAGS				
23	de	55	05	d4		e8		00		50		e9	8e	48	a9	00	00	00	00	)	a0		02		
	TCP																								
WI	NDO	СН	ECK	UR	GENT									-	OPT	IONS									
WS	SIZE	SU	JM	PO	INTER																				
fa	f0	82	86	00	00	]	Max	Segm	ent Si	ze	S	ACK						Time	stamps	S					
							Permitted																		

3) Рассчитать контрольную сумму заголовка IP-пакета. Вписать результат в соответствующее поле на бланке задания. Привести процесс расчета.

Контрольная сумма заголовка передаваемого пакета IPv4 рассчитывается по следующему алгоритму:

1. Заголовок разбивается на слова Wi по 16 бит(2 байта). При необходимости последнее слово заголовка дополняется нулями справа (биты заполнения), чтобы «выровнять» длину заголовка в битах кратно 16.

W1	450016
W2	$003c_{16}$
W3	0996 <sub>16</sub>
W4	$4000_{16}$
W5	4006 <sub>16</sub>
W6	$0000_{16}$
W7	c0a8 <sub>16</sub>
W8	580a <sub>16</sub>
W9	23de <sub>16</sub>
W10	5505 <sub>16</sub>

2.Значение поля контрольной суммы, которому соответствует слово W6, принимается равным нулю:

$$W6 = (0000)_{16}$$

3. Полученные 16-битные слова Wi поэлементно суммируются между собой, как двоичные числа с переносом в старшие разряды:

$$4500_{16} + 003c_{16} = 453C_{16}$$

$$453C_{16} + 0996_{16} = 4ED2_{16}$$

$$4ED2_{16} + 4000_{16} = 8ED2_{16}$$

$$8ED2_{16} + 4006_{16} = CED8_{16}$$

$$CED8_{16} + C0A8_{16} = 18F80_{16}$$

$$18F80_{16} + 580A_{16} = 1E78A_{16}$$

$$1E78A_{16} + 23DE_{16} = 20B68_{16}$$

$$20B68_{16} + 5505_{16} = 2606D_{16}$$

$$Ws = 2606D_{16}$$

4. В том случае, если результат сложения Ws в двоичном представлении превышает по длине 16 бит, он разбивается на два 16-битных слова, которые складываются

между собой. Эту процедуру называют «круговым переносом», т. е, переполнение старшего разряда переносится в младший.

$$Ws = 0002_{16} + 606D_{16} = 606F_{16}$$

5. Находится двоичное поразрядное дополнение результата сложения, которое и записывается в поле контрольной суммы:

$$CS_{IP} = 9F90_{16}$$

Контрольная сумма совпала с полученной контрольной суммой из пакета.

Проверка контрольной суммы при приеме IP-пакета производится по аналогичному алгоритму, отличаясь только тем, что в расчете участвует и контрольная сумма принятого IP-пакета. Если итоговое поразрядное двоичное дополнение полученной суммы равно 0, т. е. (()<sub>16</sub>0000), то это говорит о корректности контрольной суммы.

$$4500_{16} + 003c_{16} + 0996_{16} + 4000_{16} + 4006_{16} + 9F90_{16} + C0A8_{16} + 580A_{16} + 23DE_{16} + 5505_{16} = 2FFFD_{16}$$

Разбиваем результат сложения на 2(т.к он превышает 16 бит)

$$0002_{16}$$
 +FFFD<sub>16</sub>=FFFF<sub>16</sub>

Находим поразрядное дополнение

Вычисленная контрольная сумма 9F90<sub>16</sub> корректна.

4) Рассчитать контрольную сумму ТСР-сегмента. Вписать результат в соответствующее поле на бланке задания.

Src IP: c0 a8 58 0a Dst IP: 23 de 55 05 Zero: 00 (const) Proto: 06

TCP\_Len: 0040

TCP\_Len скадывается из: длина TCP Header, длина доп. опций, длина полезных данных.

Считаем сумму псевдозаголовка COA8 + 580A + 23DE + 5505 + 0000 + 0600 + 0040 = 197D5

Считаем сумму ТСР-заголовка с зануленной суммой

W1	D4E8	W11	0204
W2	0050	W12	05B4
W3	E98E	W13	0402
W4	48A9	W14	080A
W5	0000	W15	86A9
W6	0000	W16	AAD8
W7	A002	W17	0000
W8	FA FO	W18	0000
W9	0000	W19	0103
W10	0000	W20	0307
Σ	4EBB0		

4EBB0+ 197D5 =68385

0006 + 8385=838B

Находим двоичное поразрядное дополнение:

 $838B_{16} = 1000\ 0011\ 1000\ 0101_2$ 

CS<sub>TCP</sub>=7C74<sub>16</sub>

Проверка:

C0A8+580A+23DE+5505+0000+0600+0040+ D4E8+0050+E98E+48A9+0000+0000+A002+FAF0+7C74+0000+0204+05B4+0402+080A+86A9+AAD8+0000+0000+0103+0307=6FFF9
0006+FFF9=FFFF<sub>16</sub>

Находим поразрядное дополнение

FFFF<sub>16</sub> FFFF<sub>16</sub>=0000<sub>16</sub>

#### Выводы

В ходе лабораторной работы были получены практические навыки в составлении кадра для широковещательной передачи ARP-запроса хостом A и кадра ARP-ответа хостом B хосту A, получены базовые навыки по работе с генераторами пакетов PackETH и packit, получены практические навыки в вычислении контрольных суммы заголовка IP-пакета и TCP сегмента.