

PC 1

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private 66:68:00	Broadcast	ARP	64	Who has 10.10.0.2? Tell 10.10.0.1
2	0.000211	Private 66:68:01	Private 66:68:00	ARP	64	10.10.0.2 is at 00:50:79:66:68:01

Мультикастовый адрес

LG бит. адрес локально назначен

MAC получателя

MAC отправителя

Наполнение

Контрольная сумма

Тип оборудования

Тип протокола

Тип операции

MAC (выше) и IP (ниже) адреса отправителя

MAC (выше) и IP (ниже) адреса получателя

ARP запрос от PC1 к PC2

arp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private 66:68:00	Broadcast	ARP	64	Who has 10.10.0.2? Tell 10.10.0.1
2	0.000211	Private 66:68:01	Private 66:68:00	ARP	64	10.10.0.2 is at 00:50:79:66:68:01

Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface --, id 0

Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)

Destination: Private_66:68:00 (00:50:79:66:68:00)

Source: Private_66:68:01 (00:50:79:66:68:01)

Type: ARP (0x0806)

Stream index: 1

Padding: 00000000000000000000000000000000

Frame check sequence: 0x00000000 [unverified]

FCS Status: Unverified

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)

Sender IP address: 10.10.0.2

Target MAC address: Private_66:68:00 (00:50:79:66:68:00)

Target IP address: 10.10.0.1

Тип оборудования

Тип протокола

Тип операции (ответ)

MAC и IP получателя

MAC и IP отправителя

ARP ответ от PC2 к PC1

PC 2

[illegible]

ARP запрос от PC1 к PC2

```
arp
No. Time Source Destination Protocol Length Info
1 0.000000 Private_66:68:00 Broadcast ARP 64 Who has 10.10.0.2? Tell 10.10.0.1
2 0.000173 Private_66:68:01 Private_66:68:00 ARP 64 10.10.0.2 is at 00:50:79:66:68:01

Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
  Destination: Private_66:68:00 (00:50:79:66:68:00)
  Source: Private_66:68:01 (00:50:79:66:68:01)
  Type: ARP (0x8006)
    [Stream index: 1]
    Padding: 00000000000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
  Sender IP address: 10.10.0.2
  Target MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Target IP address: 10.10.0.1
```

ARP ответ от PC2 к PC1

PC1 Router

No.	Time	Source	Destination	Protocol	Length	Info
2	0.523027	cc:01:25:fb:00:00	Broadcast	ARP	60	Gratuitous ARP for 10.10.0.1 (Reply)
5	25.162395	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc3e8, seq=1/256, ttl=64 (no response found!)
6	27.162395	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc3e8, seq=2/512, ttl=64 (no response found!)
7	27.174537	cc:01:25:fb:00:00	Broadcast	ARP	60	Who has 10.10.0.15? Tell 10.10.0.1
8	27.174603	Private_66:68:03	cc:01:25:fb:00:00	ARP	60	10.10.0.15 is at 00:50:79:66:68:03
9	29.586399	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc7e8, seq=1/256, ttl=64 (reply in 10)
10	29.597811	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc7e8, seq=1/256, ttl=63 (request in 9)
11	30.597983	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc8e8, seq=2/512, ttl=64 (reply in 12)
12	30.613480	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc8e8, seq=2/512, ttl=63 (request in 11)
13	31.613982	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9e8, seq=3/768, ttl=64 (reply in 14)
14	31.629018	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9e8, seq=3/768, ttl=63 (request in 13)
15	32.629083	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcae8, seq=4/1024, ttl=64 (reply in 15)
16	32.645411	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcae8, seq=4/1024, ttl=63 (request in 15)
17	33.645875	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcbe8, seq=5/1280, ttl=64 (reply in 18)
18	33.660849	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcbe8, seq=5/1280, ttl=63 (request in 17)

ARP запрос от PC1 до PC2. Отправлен на маршрутизатор

No.	Time	Source	Destination	Protocol	Length	Info
2	0.523827	cc:01:25:fb:00:00	Broadcast	ARP	60	Gratuitous ARP for 10.10.0.1 (Reply)
5	25.162395	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc3e8, seq=1/256, ttl=64 (no response found!)
6	27.162995	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc5e8, seq=2/512, ttl=64 (no response found!)
7	27.174537	cc:01:25:fb:00:00	Broadcast	ARP	60	Who has 10.10.0.1? Tell 10.10.0.1
8	27.174603	Private_66:68:03	cc:01:25:fb:00:00	ARP	60	10.10.0.15 is at 00:50:79:66:68:03
9	29.586399	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc7e8, seq=1/256, ttl=64 (reply in 10)
10	29.597911	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc7e8, seq=1/256, ttl=63 (request in 9)
11	30.597983	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc8e8, seq=2/512, ttl=64 (reply in 12)
12	30.613480	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc8e8, seq=2/512, ttl=63 (request in 11)
13	31.613982	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9e8, seq=3/768, ttl=64 (reply in 14)
14	31.614018	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9e8, seq=3/768, ttl=63 (request in 13)
15	32.629883	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcae8, seq=4/1024, ttl=64 (reply in 16)
16	32.645411	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcae8, seq=4/1024, ttl=63 (request in 15)
17	33.645875	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcbc8, seq=5/1280, ttl=64 (reply in 18)
18	33.660849	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcbc8, seq=5/1280, ttl=63 (request in 17)

Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0

- Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: cc:01:25:fb:00:00 (cc:01:25:fb:00:00)
 - Destination: cc:01:25:fb:00:00 (cc:01:25:fb:00:00)
 - Source: Private_66:68:03 (00:50:79:66:68:03)
 - Type: ARP (0x0806)
 - [Stream offset: 3]
 - Padding: 00
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IPv4 (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (2)
 - Sender MAC address: Private_66:68:03 (00:50:79:66:68:03)
 - Sender IP address: 10.10.0.15
 - Target MAC address: cc:01:25:fb:00:00 (cc:01:25:fb:00:00)
 - Target IP address: 10.10.0.1

```

0000 cc 01 25 fb 00 00 50 79 66 68 03 00 06 00 01   ...P yfh...
0010 08 00 06 04 00 02 00 50 79 65 68 03 0a 0a 0f   ...P yfh...
0020 cc 01 25 fb 00 0a 0a 00 01 00 00 00 00 00 00   ...%.....
0030 00 00 00 00 00 00 00 00 00 00 00 00           ....

```

ARP ответ от PC2 к PC1. Пришел с маршрутизатора

PC2 Router

No.	Time	Source	Destination	Protocol	Length	Info
2	6.134360	cc:01:25:fb:00:10	Broadcast	ARP	60	who has 10.10.1.15? Tell 10.10.1.1
3	6.134447	Private_66:68:01	cc:01:25:fb:00:10	ARP	60	10.10.1.15 is at 00:50:79:66:68:01
4	6.125520	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc5e8, seq=2/512, ttl=63 (reply in 5)
5	6.125614	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc5e8, seq=2/512, ttl=64 (request in 4)
6	10.548026	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc7e8, seq=1/256, ttl=63 (reply in 7)
7	10.548900	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc7e8, seq=1/256, ttl=64 (request in 6)
8	11.564405	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc8e8, seq=2/512, ttl=63 (reply in 9)
9	11.564563	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc8e8, seq=2/512, ttl=64 (request in 8)
10	12.580006	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9e8, seq=3/768, ttl=63 (reply in 11)
11	12.580143	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9e8, seq=3/768, ttl=64 (request in 10)
12	13.596423	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcae8, seq=4/1024, ttl=63 (reply in 13)
13	13.596513	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcae8, seq=4/1024, ttl=64 (request in 12)
14	14.611884	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcbc8, seq=5/1280, ttl=63 (reply in 15)
15	14.611993	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcbc8, seq=5/1280, ttl=64 (request in 14)

ARP запрос от PC1 до PC2. Пришел с маршрутизатора

arp icmp						
No.	Time	Source	Destination	Protocol	Length Info	
2	6.134360	cc:01:25:fb:00:10	Broadcast	ARP	60	Who has 10.10.1.15? Tell 10.10.1.1
3	6.134447	Private_66:68:01	cc:01:25:fb:00:10	ARP	60	10.10.1.15 is at 00:50:79:66:68:01
4	8.125529	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc5e8, seq=2/512, ttl=63 (reply in 5)
5	8.125514	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc5e8, seq=2/512, ttl=64 (request in 4)
6	10.548826	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc7e8, seq=1/256, ttl=63 (reply in 7)
7	10.548900	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc7e8, seq=1/256, ttl=64 (request in 6)
8	11.564465	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcde8, seq=2/512, ttl=63 (reply in 9)
9	11.564563	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcde8, seq=2/512, ttl=64 (request in 8)
10	12.500000	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9e8, seq=3/768, ttl=63 (reply in 11)
11	12.500143	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9e8, seq=3/768, ttl=64 (request in 10)
12	13.596423	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9ae8, seq=4/1024, ttl=63 (reply in 13)
13	13.596513	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9ae8, seq=4/1024, ttl=64 (request in 12)
14	14.611804	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcbe8, seq=5/1280, ttl=63 (reply in 15)
15	14.611993	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcbe8, seq=5/1280, ttl=64 (request in 14)
<pre> * Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface --, id 0 * Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: cc:01:25:fb:00:10 (cc:01:25:fb:00:10) * Destination: cc:01:25:fb:00:10 (cc:01:25:fb:00:10) * Source: Private_66:68:01 (00:50:79:66:68:01) Type: ARP (0x0006) [Stream index: 2] Padding: 00 * Address Resolution Protocol (reply) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0000) Hardware size: 6 Protocol size: 4 Opcode: reply (2) Sender MAC address: Private_66:68:01 (00:50:79:66:68:01) Sender IP address: 10.10.1.15 Target MAC address: cc:01:25:fb:00:10 (cc:01:25:fb:00:10) Target IP address: 10.10.1.1 </pre>						
				0000	cc 01 25 fb 00 10 00 50	79 66 68 01 00 00 01
				0010	00 00 06 04 00 02 00 50	79 66 68 01 0a 0a 0f
				0020	cc 01 25 fb 00 10 0a 0a	01 01 00 00 00 00 00
				0030	00 00 00 00 00 00 00 00	00 00 00 00

ARP ответ от PC2 к PC1. Отправлен на маршрутизатор

Анализ ICMP заголовка

arp || icmp

No.	Time	Source	Destination	Protocol	Length	Info
2	0.523027	cc:01:25:fb:00:00	Broadcast	ARP	60	Gratuitous ARP for 10.10.0.1 (Reply)
5	25.162395	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc3e8, seq=1/256, ttl=64 (no response found!)
6	27.162995	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc5e8, seq=2/512, ttl=64 (no response found!)
7	27.174537	cc:01:25:fb:00:00	Broadcast	ARP	60	Who has 10.10.0.15? Tell 10.10.0.1
8	27.174603	Private 66:68:03	cc:01:25:fb:00:00	ARP	60	10.10.0.15 is at 00:50:79:66:68:03
9	29.586399	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc7e8, seq=1/256, ttl=64 (reply in 10)
10	29.597611	10.10.0.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc7e8, seq=1/256, ttl=63 (request in 9)
11	30.597083	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc8e8, seq=2/512, ttl=64 (reply in 12)
12	30.613480	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc8e8, seq=2/512, ttl=63 (request in 11)
13	31.613982	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xc9e8, seq=3/768, ttl=64 (reply in 14)
14	31.629018	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xc9e8, seq=3/768, ttl=63 (request in 13)
15	32.629083	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcae8, seq=4/1024, ttl=64 (reply in 16)
16	32.645411	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcae8, seq=4/1024, ttl=63 (request in 15)
17	33.645875	10.10.0.15	10.10.1.15	ICMP	98	Echo (ping) request id=0xcbe8, seq=5/1280, ttl=64 (reply in 18)
18	33.658049	10.10.1.15	10.10.0.15	ICMP	98	Echo (ping) reply id=0xcbe8, seq=5/1280, ttl=63 (request in 17)

Frame 9: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

Ethernet II, Src: Private 66:68:03 (00:50:79:66:68:03), Dst: cc:01:25:fb:00:00 (cc:01:25:fb:00:00)

Internet Protocol Version 4, Src: 10.10.0.15, Dst: 10.10.1.15

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total length: 64

Identification: 0xe8c7 (59591)

0000 = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: ICMP (1)

Header Checksum: 0x7cb0 [validation disabled]

[Header checksum status: Unverified]

Source Address: 10.10.0.15

Destination Address: 10.10.1.15

[Stream index: 0]

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x5822 [correct]

[Checksum Status: Good]

Identifier (BE): 51176 (0xc7e8)

Identifier (LE): 59591 (0xe8c7)

Sequence Number (BE): 1 (0x0001)

Sequence Number (LE): 256 (0x0100)

[0xc7e8000100000000]

Data (56 bytes)

0000 cc 01 25 fb 00 00 00 50 79 66 68 03 00 00 45 00 --%...p yfh...E-

0010 00 54 e8 c7 00 00 40 01 7c b0 0a 0a 00 0f 0a 0a -T...@ [.....

0020 01 0f 00 00 58 22 c7 e5 00 01 00 09 0a 00 0c 0d --X".....

0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d

0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d --!"\$%&'()*+,-

0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789:;<=

0060 3e 3f >?