Address Resolution Protocol

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

Работа ARP

Хост отправляет широковещательный (broadcast) запрос:
“ Какой MAC-адрес имеет 10.109.11.67? Ответьте на 10.109.11.32 - 8A:5F:3C:23:45:13 ”

Хост, у которого IP-адрес 10.109.11.67 отвечает:
“ Мой IP+MAC 10.109.11.67 – 8A:5F:3C:23:45:56 ответ отправляю на 8A:5F:3C:23:45:13 ”

Broadcast довольно затратные (время/ресурс).

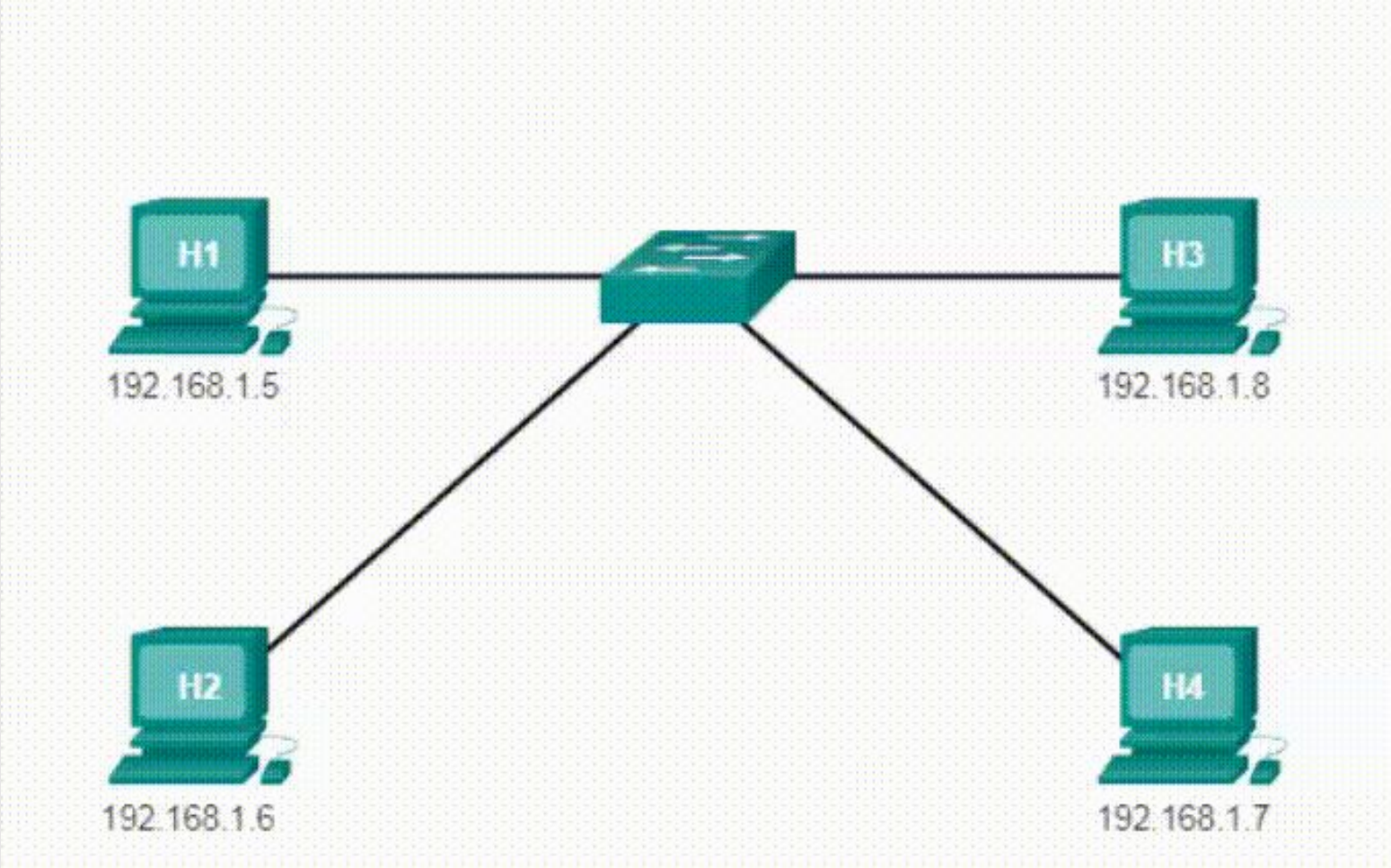
ARP ответы кэшируются (ARP-cache).

Хост обновляет кэш-таблицу, если получает ARP-broadcast.

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

Визуальная работа ARP

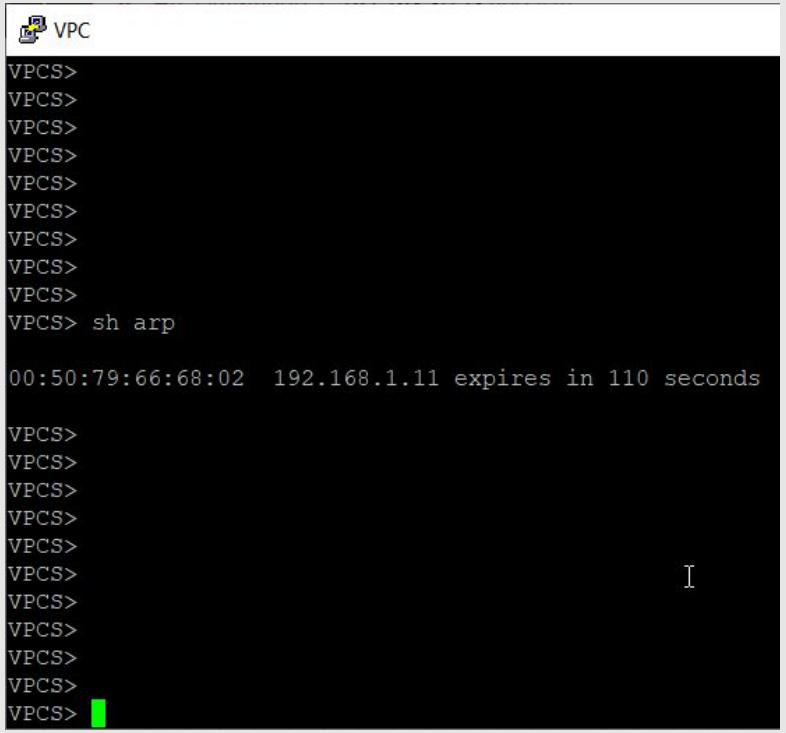


- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

ARP таблица

Протокол имеет ARP-таблицу, в которой хранятся пары адресов (IP == MAC) с целью уменьшения количества посылаемых запросов, следовательно, экономии трафика и ресурсов.



Слева – IP-адреса, справа – MAC-адреса.

ARP таблица

Пример vpc

Пример на ubuntu

```
coolzi@Terentev: ~
File  Edit  View  Search  Terminal  Help
coolzi@Terentev  ~  arp -a                                  ✔  6797  17:02:22
? (10.226.255.69) at 00:24:97:dd:53:d2 [ether] on enp2s0
? (10.226.255.233) at 00:24:97:dd:6a:9e [ether] on enp2s0
? (192.168.10.16) at 14:dd:a9:e6:33:20 [ether] on enp3s0
? (192.168.11.29) at 00:19:17:00:00:01 [ether] on enp3s0
? (192.168.10.105) at b4:b5:2f:61:83:0c [ether] on enp3s0
? (192.168.11.19) at 00:19:17:91:72:d6 [ether] on enp3s0
? (192.168.10.37) at 38:d5:47:1a:18:f3 [ether] on enp3s0
? (10.226.255.71) at 2c:54:2d:f5:fb:20 [ether] on enp2s0
? (192.168.10.36) at ac:22:0b:4f:57:f3 [ether] on enp3s0
? (192.168.10.247) at 00:19:17:91:7b:4b [ether] on enp3s0
? (10.226.255.249) at c8:9c:1d:68:20:3f [ether] on enp2s0
? (10.226.255.244) at 70:81:05:b6:5a:7f [ether] on enp2s0
? (192.168.10.197) at 64:d1:54:99:37:e4 [ether] on enp3s0
? (192.168.11.237) at 00:1a:4a:16:01:78 [ether] on enp3s0
? (10.226.255.12) at e4:c7:22:1b:1f:82 [ether] on enp2s0
? (10.226.255.231) at 00:24:97:dd:6a:23 [ether] on enp2s0
? (192.168.10.219) at 14:1f:ba:eb:c0:1a [ether] on enp3s0
? (10.226.255.63) at e4:c7:22:2f:4a:30 [ether] on enp2s0
? (192.168.11.38) at 40:a8:f0:26:01:dc [ether] on enp3s0
? (10.226.255.245) at 70:ca:9b:8e:35:bf [ether] on enp2s0
? (192.168.11.78) at 8c:1c:da:87:c4:69 [ether] on enp3s0
? (10.226.255.251) at cc:b2:55:8a:b6:60 [ether] on enp2s0
? (10.226.255.19) at a4:4c:11:35:0f:a0 [ether] on enp2s0
```

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

Структура пакета

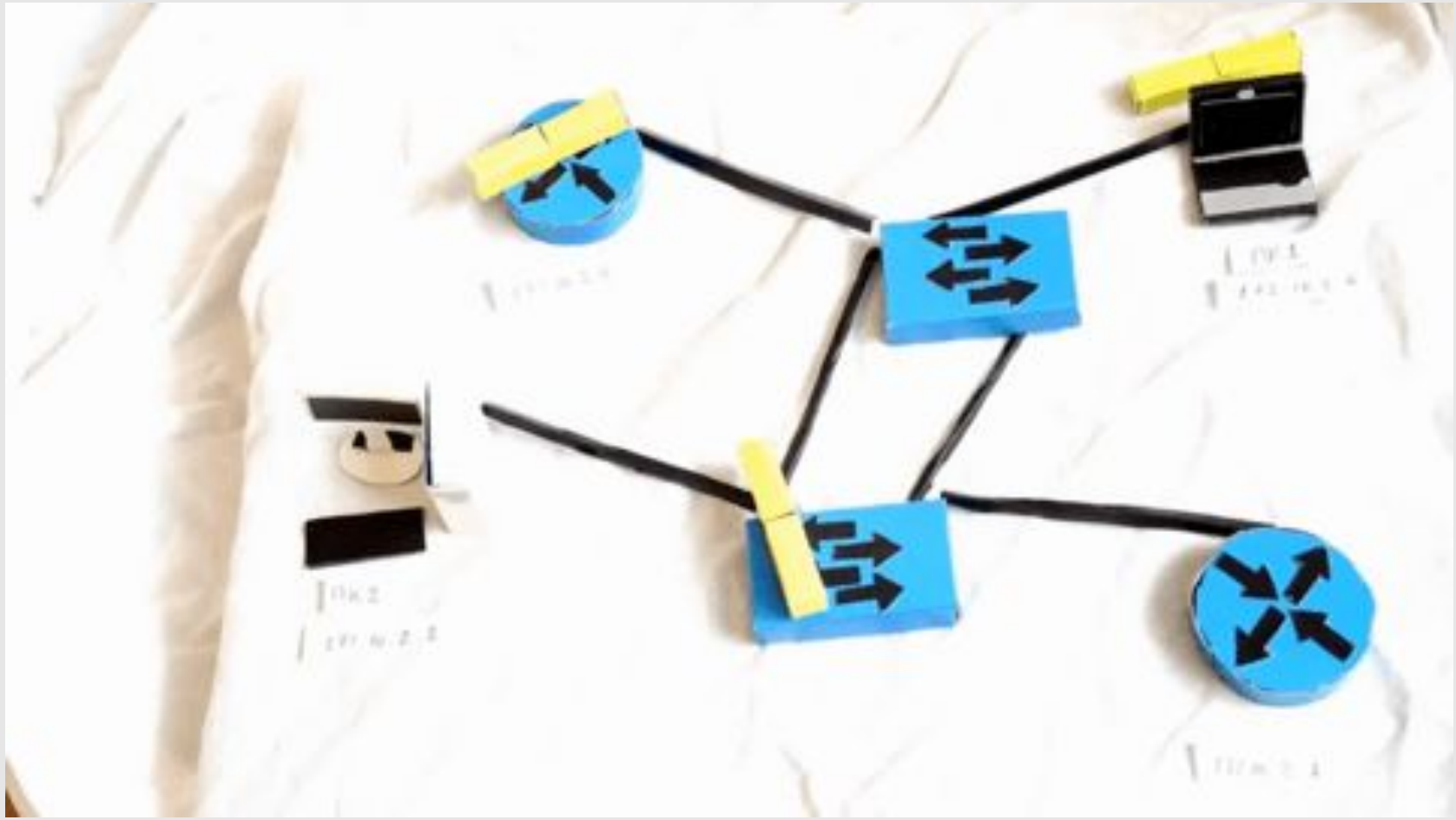
Ниже показана структура пакета, используемого в запросах и ответах ARP.
В сетях Ethernet в этих пакетах используется EtherType 0x0806, и запросы рассылаются на широковещательный MAC-адрес — FF:FF:FF:FF:FF:FF.

+	Bits 0 — 7	8 — 15	16 — 31
0	Hardware type (HTYPE) // Канальный протокол.		Protocol type (PTYPE) // Код сетевого протокола.
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER) // Q/A == 0x0001/2
64	Sender hardware address (SHA) // MAC отправителя.		
?	Sender protocol address (SPA) // IP отправителя.		
?	Target hardware address (THA) // MAC получателя.		
?	Target protocol address (TPA) // IP получателя.		

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

BROADCAST STORM



- ARP

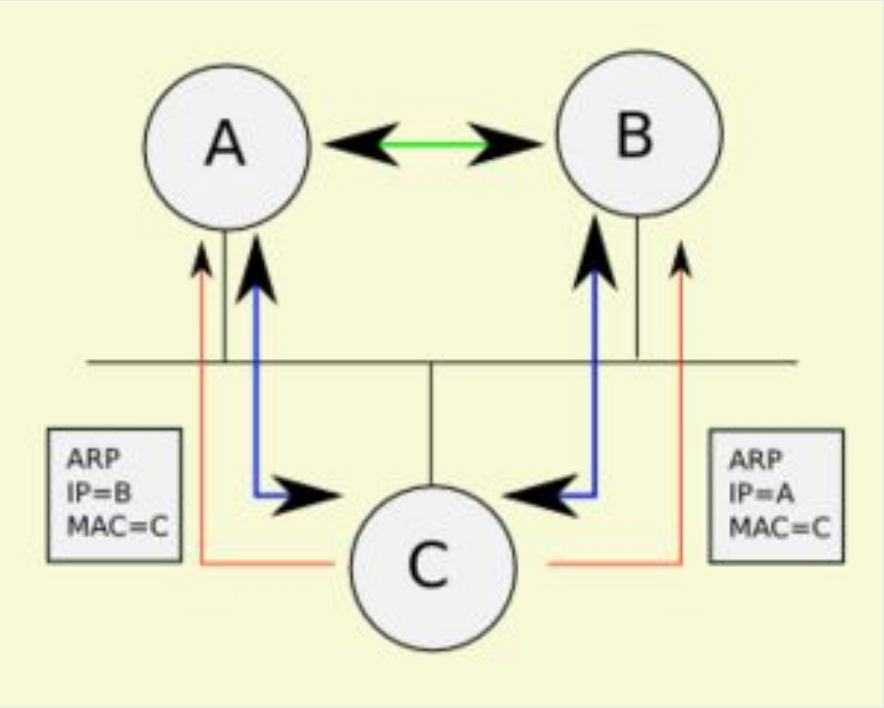
1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

ARP-spoofing

Протокол ARP является абсолютно незащищённым. У него нет способов проверки подлинности запросов, так и ответов.

В ходе выполнения ARP-spoofing'а компьютер **C**, выполняющий атаку, отправляет ARP-ответы (без получения запросов)

После того как атака выполнена, когда компьютер *A* хочет передать пакет компьютеру **B**, он находит в ARP-таблице запись и определяет из неё MAC-адрес получателя (она соответствует компьютеру *C*). Отправленный по этому MAC-адресу пакет приходит компьютеру *C* вместо получателя. Компьютер *C* затем ретранслирует пакет тому, кому он действительно адресован — т. е. компьютеру *B*.



Атака на A и B

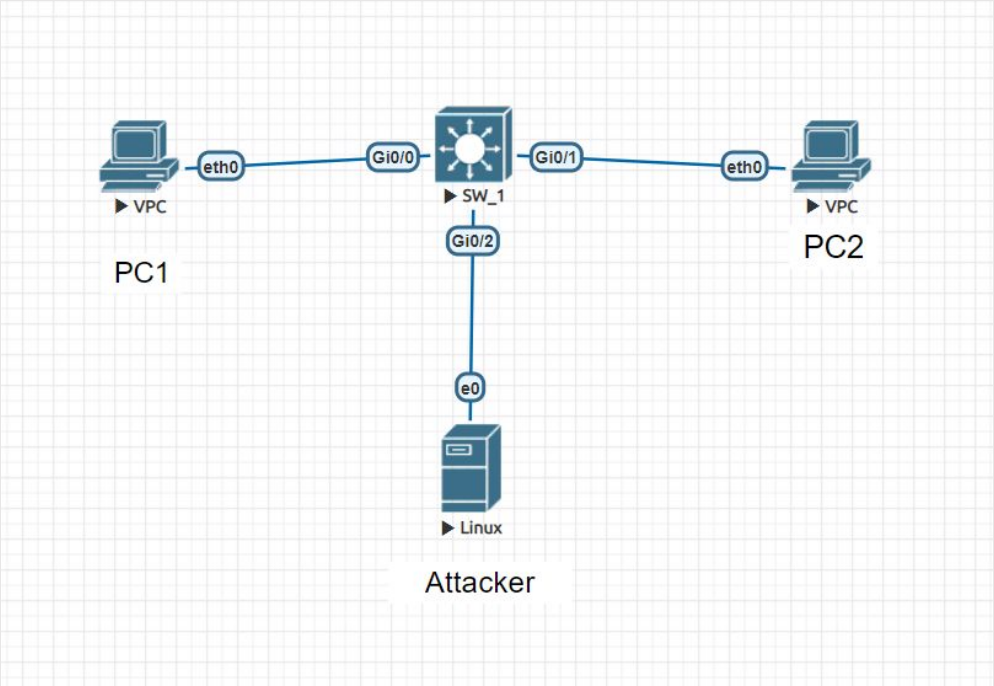
ARP-spoofing

Обмен данными между A и B

До ARP-spoofing'а

После ARP-spoofing'а

ARP-spoofing



IP	MAC	HOSTNAME
192.168.1.10	00:50:79:66:68:03	PC1
192.168.1.11	00:50:79:66:68:02	PC2
192.168.1.50	00:50:00:00:06:00	Attacker

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp

No.	Time	Source	Destination	Protocol	Length	Info
169	288.209183	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.1.10? Tel…
170	288.209245	Private_66:68:03	Private_66:68:02	ARP	64	192.168.1.10 is at 00:50:…

```
> Frame 169: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
> Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Private_66:68:02 (00:50:79:66:68:02)
    Sender IP address: 192.168.1.11
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.1.10
```

Target MAC address (arp.dst.hw_mac), 6 байты | Пакеты: 207 · Показаны: 2 (1.0%) | Профиль: Default

```
arp table is empty

VPCS> ping 192.168.1.10

84 bytes from 192.168.1.10 icmp_seq=1 ttl=64 time=5.026 ms
^C
VPCS> arp

00:50:79:66:68:03  192.168.1.10 expires in 107 seconds

VPCS>
```

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp

No.	Time	Source	Destination	Protocol	Length	Info
279	480.090095	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.1.10? Tel…
280	480.097909	Private_66:68:03	Private_66:68:02	ARP	64	192.168.1.10 is at 00:50:…

```
> Frame 280: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
> Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
v 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: 192.168.1.10
    Target MAC address: Private_66:68:02 (00:50:79:66:68:02)
    Target IP address: 192.168.1.11
```

Target MAC address (arp.dst.hw_mac), 6 байты | Пакеты: 317 · Показаны: 2 (0.6%) | Профиль: Default

```
VPCS>
VPCS>
VPCS> sh arp

arp table is empty

VPCS> arp

00:50:79:66:68:02  192.168.1.11 expires in 105 seconds

VPCS>
```

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp | Выражение...

No.	Time	Source	Destination	Protocol	Length	Info
169	288.209183	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.1.10? Tel…
170	288.209245	Private_66:68:03	Private_66:68:02	ARP	64	192.168.1.10 is at 00:50:…

```
> Frame 170: 64 bytes on wire (512 bits), 64 bytes captured (5
> Ethernet II, Src: Private_66:68:03 (00:50:79:66:68:03), Dst:
v 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: 192.168.1.10
    Target MAC address: Private_66:68:02 (00:50:79:66:68:02)
    Target IP address: 192.168.1.11
```

Target MAC address (arp.dst.hw_mac), 6 байты

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp | Выражение...

No.	Time	Source	Destination	Protocol	Length	Info
279	480.090095	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.1.10? Tel…
280	480.097909	Private_66:68:03	Private_66:68:02	ARP	64	192.168.1.10 is at 00:50:…

```
s), 64 bytes captured (512 bits) on interface 0
00:50:79:66:68:03), Dst: Private_66:68:02 (00:50:79:66:68:02)
:03 (00:50:79:66:68:03)
:02 (00:50:79:66:68:02)
```

Пакеты: 485 · Показаны: 2 (0.4%) | Профиль: Default

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония

arp | Выражение...

No.	Time	Source	Destination	Protocol	Length	Info
112	188.220016	Private_66:68:02	Broadcast	ARP	64	Who

```
> Frame 112: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interfac
> Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: Broadcast (ff:ff:ff
> Address Resolution Protocol (request)
```

wireshark_-_20190712093207_a01684.pcapng | Пакеты: 314 · Показаны: 1 (0.3%) | Профиль: Default

9 ARP-spoofing

Слайд 9 из 10 | английский (США) | Заметки | Примечания | 89%

*-

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp — Выражение...

No.	Time	Source	Destination	Protocol	Length	Info
1131	1467.482762	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1137	1477.492083	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1138	1477.495943	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1139	1477.503112	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1140	1477.506940	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1148	1487.511810	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1149	1487.514551	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1150	1487.523278	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1151	1487.526013	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1157	1497.533572	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1158	1497.536149	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1159	1497.543578	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1160	1497.546338	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…

```
> Frame 1160: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: NexoComm_00:06:00 (00:50:00:00:06:00), Dst: Private_66:68:02 (00:50:79:66:68:02)
> [Duplicate IP address detected for 192.168.1.10 (00:50:00:00:06:00) - also in use by 00:50:79:66:68:03
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: NexoComm_00:06:00 (00:50:00:00:06:00)
    Sender IP address: 192.168.1.10
    Target MAC address: Private_66:68:02 (00:50:79:66:68:02)
    Target IP address: 192.168.1.11
```

Sender MAC address (arp.src.hw_mac), 6 байты | Пакеты: 1332 · Показаны: 332 (24.9%) | Профиль: Default

```
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
VPCS> arp

00:50:00:00:06:00  192.168.1.10 expires in 112 seconds
00:50:00:00:06:00  192.168.1.11 expires in 112 seconds

VPCS>
```

*-

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

arp — Выражение...

No.	Time	Source	Destination	Protocol	Length	Info
1412	1829.724572	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1418	1839.732601	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1419	1839.735375	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1420	1839.743538	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1421	1839.746120	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1427	1849.753899	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1428	1849.756527	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1429	1849.763538	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1430	1849.766226	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1437	1859.773631	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…
1438	1859.776326	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1439	1859.783109	NexoComm_00:06:00	Private_66:68:03	ARP	60	192.168.1.11 is at 00:5…
1440	1859.785656	NexoComm_00:06:00	Private_66:68:02	ARP	60	192.168.1.10 is at 00:5…

```
> Frame 1361: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: NexoComm_00:06:00 (00:50:00:00:06:00), Dst: Private_66:68:03 (00:50:79:66:68:03)
> [Duplicate IP address detected for 192.168.1.11 (00:50:00:00:06:00) - also in use by 00:50:79:66:68:02
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: NexoComm_00:06:00 (00:50:00:00:06:00)
    Sender IP address: 192.168.1.11
    Target MAC address: Private_66:68:03 (00:50:79:66:68:03)
    Target IP address: 192.168.1.10
```

Sender MAC address (arp.src.hw_mac), 6 байты | Пакеты: 1444 · Показаны: 332 (23.0%) | Профиль: Default

```
VPCS>
VPCS>
VPCS>
VPCS>
VPCS>
VPCS> arp

00:50:00:00:06:00  192.168.1.11 expires in 111 seconds
00:50:00:00:06:00  192.168.1.10 expires in 111 seconds

VPCS>
```

519	683.697760	192.168.1.10	192.168.1.11	ICMP	98	Echo (ping) reply id=0x88f3, seq=3/768, ttl=64

```
> Frame 519: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: NexoComm_00:06:00 (00:50:00:00:06:00), Dst: Private_66:68:02 (00:50:79:66:68:02)
> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.11
> Internet Control Message Protocol
```

- ARP

1. Описание протокола
2. Для чего это нужно
3. Механизм работы
    1. Алгоритм
    2. Графически
    3. ARP таблица
    4. Структура пакета
4. Недостатки
    1. Петля
    2. ARP-spoofing
5. Proxy ARP

PROXY ARP

Механизм позволяющий объединить две не связанные на L2 сети в одну. Хосты находящиеся в этих сетях, могут использовать адреса из одной подсети и обмениваться трафиком между собой без использования роутера.

-Хост A отправляет данные хосту B. Так как, на хосте A IP-add 10.0.1.10/8, то он считает, что B с IP-add 10.0.2.10/8, находится с ним в одной сети.

-При включенном Proxy ARP, маршрутизатор отвечает на запрос своим MAC.

У хоста A, создается соответствие 10.0.2.10 - MAC f0/0.

У хоста B, создается соответствие 10.0.1.10 - MAC f0/1.

-Роутер получает пакет, смотрит на IP-адрес получателя и отправляет пакет ему. Так как его ARP-таблица не изменилась.

-Теперь хосты могут обмениваться данными.