СЛЁРМ

Поиск соседей в рамках канала в IPv4 и в IPv6

Спикер:
Роман Козлов

ПОИСК СОСЕДЕЙ В РАМКАХ КАНАЛА

- ARP
- NDP
- ICMP и ICMPv6

ARP

Спикер:
Роман Козлов

ARP

01

Address Resolution Protocol

02

ARP объединяет IP-адрес клиента (Layer3) с MAC-адресом (Layer2)ARP

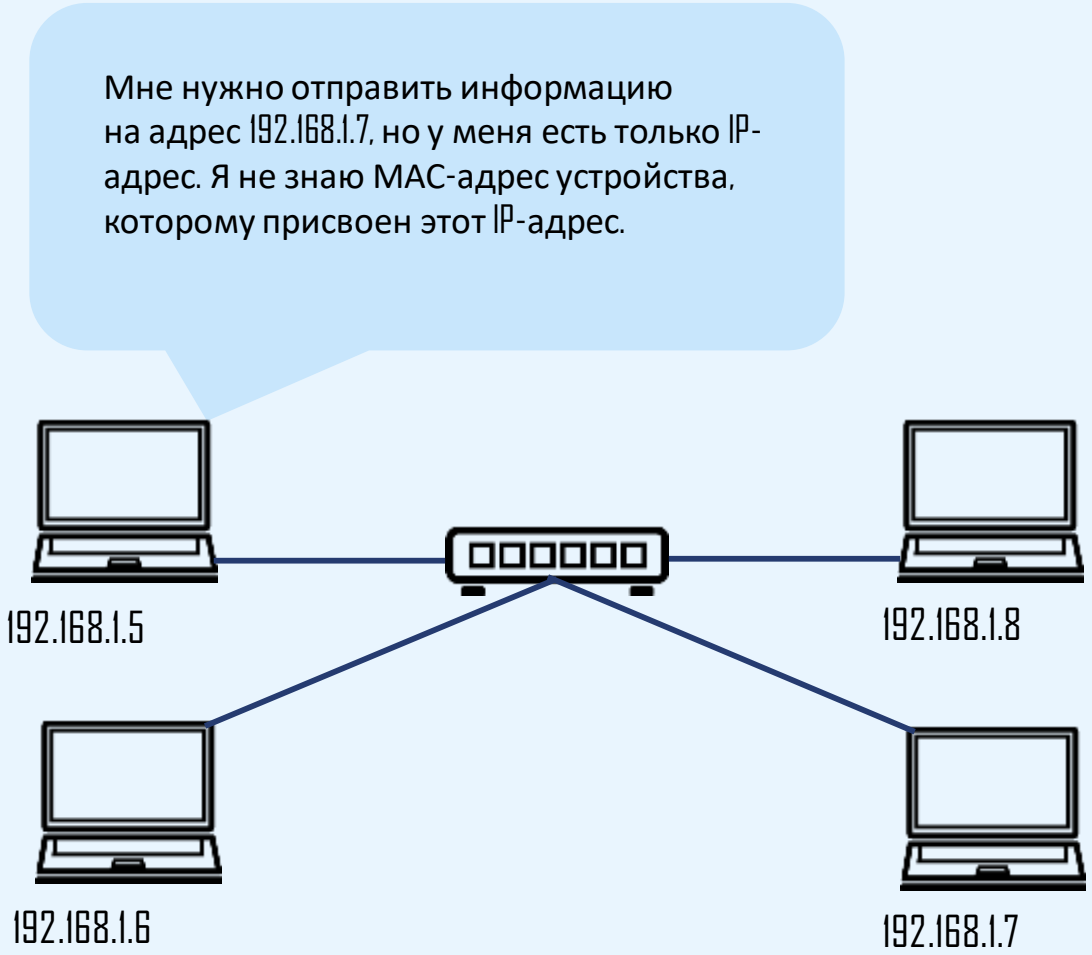
03

Работает динамически

04

Можно также настроить вручную

ARP



Если адрес сети (**network address**) адреса назначения (**dst address**) равна адресу сети (**network address**) источника (**src address**), посылай *широковещательный запрос*

ARP В ЛОКАЛЬНОЙ СЕТИ

Если адрес сети (**network address**) адреса назначения (**dst address**) равна адресу сети (**network address**) источника (**src address**), посылай *широковещательный запрос* для получения mac-адреса назначения (**dst mac-address**)

192.0.2.254/24 = **192.0.2**.1/24 => широковещательный запрос ”кто есть 192.0.2.1”

ARP запрос

50:00:01:02:00:01 (SRC MAC) > ff:ff:ff:ff:ff:ff (DST MAC), ethertype ARP (0x0806): Ethernet (len 6), IPv4 (len 4), Request who-has 192.0.2.254 tell 192.0.2.1

ARP ответ

50:00:00:01:00:00 (SRC MAC) > 50:00:01:02:00:01 (DST MAC), ethertype ARP (0x0806): Ethernet (len 6), IPv4 (len 4), Reply 192.0.2.254 is-at 50:00:00:01:00:00

ARP С УДАЛЕННОЙ СЕТЬЮ

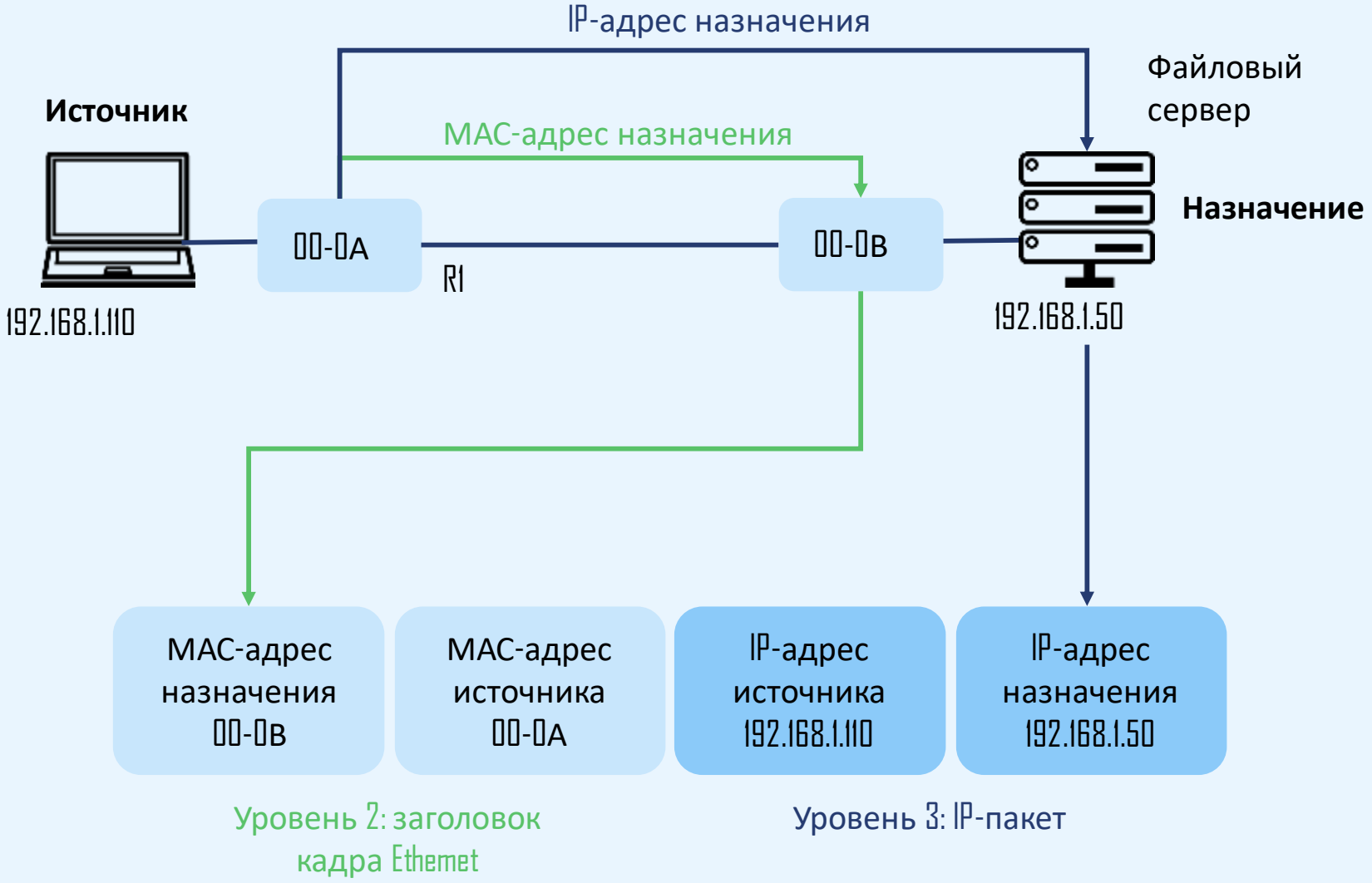
Если адрес сети (**network address**) адреса назначения (**dst address**) не равен на адресу сети (**network address**) адреса источника (**src address**), то мы *отправляем пакеты нашему шлюзу* – то есть подставляем в заголовки кадров MAC-адрес нашего шлюза

192.0.2.254/24 != **192.0.0**.254/24 => отправляем пакеты шлюзу 192.0.2.1

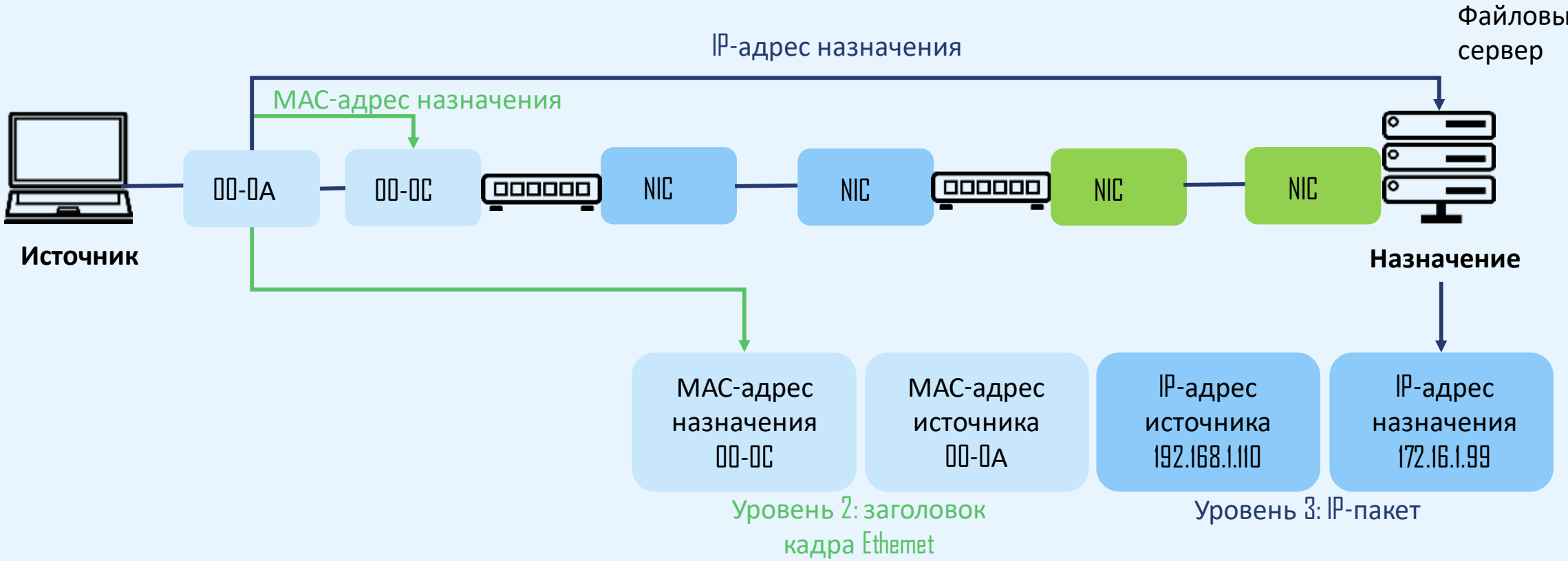
Если не знаем MAC-адрес шлюза

192.0.2.254/24 = **192.0.2**.1/24 => широковещательный ARP запрос ”кто есть 192.0.2.1”

ARP


IP-адрес назначения
Файловый сервер
Источник
MAC-адрес назначения
00-0A
R1
00-0B
Назначение
192.168.1.110
192.168.1.50
MAC-адрес назначения 00-0B
MAC-адрес источника 00-0A
IP-адрес источника 192.168.1.110
IP-адрес назначения 192.168.1.50
Уровень 2: заголовок кадра Ethernet
Уровень 3: IP-пакет

ARP



С удаленной сетью фактически нет ARP запросов и ответов.
Кадры отправляются на MAC-адреса нашего шлюза.
Если мы не знаем MAC-адрес шлюза –
то тогда посылается ARP-запрос на IP-адрес шлюза.

ARParp –n и ip -4 neighbor

Просмотр ARP таблиц и цепочек
arp –n

```
root@ubuntu22-server:~# arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
8.8.4.4                          (incomplete)                              ens5
192.0.2.2                        (incomplete)                              ens3
192.0.2.1                ether   50:00:01:02:00:01   C                     ens3
8.8.8.8                          (incomplete)                              ens5
```

Просмотр ARP таблиц и цепочек
ip -4 neighbor

```
root@ubuntu22-server:~# ip -4 neighbor
8.8.4.4 dev ens5  FAILED
192.0.2.2 dev ens3  FAILED
192.0.2.1 dev ens3 lladdr 50:00:01:02:00:01 REACHABLE
8.8.8.8 dev ens5  FAILED
```

ip -4 neighbor добавление

ip -4 neighbour add 192.0.2.1 lladdr 50:00:01:02:00:01 dev ens3

ip -4 neighbour change 192.0.2.1 lladdr 50:00:01:02:00:01 dev ens3

```
root@ubuntu22-server:~# ip -4 n
192.0.2.4 dev ens3 lladdr 50:00:01:02:00:32 PERMANENT
8.8.4.4 dev ens5  INCOMPLETE
192.0.2.2 dev ens3  FAILED
192.0.2.1 dev ens3 lladdr 50:00:01:02:00:01 PERMANENT
8.8.8.8 dev ens5  FAILED
```

arping

```
root@ubuntu22-server:~# arping 192.0.2.1
ARPING 192.0.2.1
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=0 time=3.765 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=1 time=1.904 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=2 time=4.274 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=3 time=2.187 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=4 time=1.501 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=5 time=2.161 msec
^C
```

arping

arping — утилита для обнаружения хостов в компьютерной сети

Функционирует аналогично утилите ping, но, в отличие от неё, посылает/получает не ICMP-запросы/ответы, а ARP-запросы/ответы

-I — наименование сетевого интерфейса, через который будут отправлены ARP-пакеты

```
root@ubuntu22-server:~# arping 192.0.2.1 -i ens3
ARPING 192.0.2.1
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=0 time=1.599 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=1 time=1.613 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=2 time=1.810 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=3 time=1.944 msec
60 bytes from 50:00:01:02:00:01 (192.0.2.1): index=4 time=2.000 msec
^C
--- 192.0.2.1 statistics ---
```

arpscan

Arp-scan утилита командной строки которая посылает arp запросы получает arp ответы от устройств

Подходит для поиска устройств в локальной сети

apt install arp-scan

arp-scan --interface=eth0 localnet

arp-scan --interface=eth0 192.168.0.0/24

```
root@ubuntu22-server:~# arp-scan --interface=ens3 192.0.2.0/24
Interface: ens3, type: EN10MB, MAC: 50:00:00:01:00:00, IPv4: 192.0.2.254
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.0.2.1       50:00:01:02:00:01       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.026 seconds (126.36 hosts/sec). 1 responded
```

NDP

Спикер:
Роман Козлов

NDP - Neighbor Discovery Protocol

01

Замена для ARP в IPv4

02

Использует ICMPv6
и мультикаст

03

Обнаруживает другие
устройства на линке

04

Отслеживает доступность

NDP - Neighbor Discovery Protocol

NDP использует 5 различных типов ICMPv6 пакетов:

- Тип 133 – Router solicitation – запрос маршрутизатора
- Тип 134 – Router advertisement – анонс маршрутизатора
- Тип 135 – Neighbor solicitation – запрос соседей
- Тип 136 – Neighbor advertisement – анонс от соседей
- Тип 137 – Redirect – переадресация

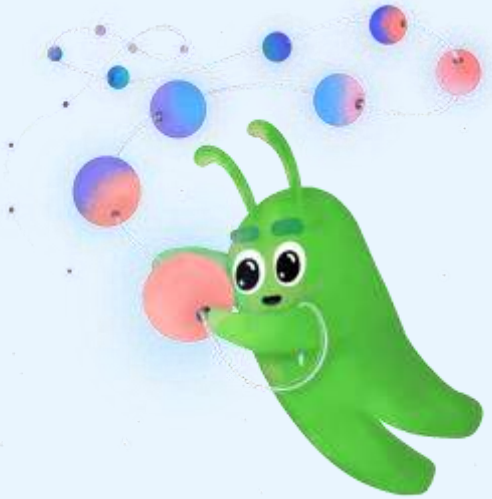
NDP - Neighbor Discovery Protocol

Neighbor Discovery использует несколько различных специальных mulicast адресов, включая:

- Link-local scope address для всех узлов – FF02::1 (multicast)
- Link-local scope address to для всех маршрутизаторов – FF02::2 (multicast)
- И другие, больше информации в https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

```
root@ubuntu22-server:~# ping ff02::1%ens3
PING ff02::1%ens3(ff02::1%ens3) 56 data bytes
64 bytes from fe80::5200:ff:fe01:0%ens3: icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from fe80::5200:1ff:fe02:1%ens3: icmp_seq=1 ttl=64 time=3.22 ms
64 bytes from fe80::5200:ff:fe01:0%ens3: icmp_seq=2 ttl=64 time=0.083 ms
64 bytes from fe80::5200:1ff:fe02:1%ens3: icmp_seq=2 ttl=64 time=2.49 ms
64 bytes from fe80::5200:ff:fe01:0%ens3: icmp_seq=3 ttl=64 time=0.072 ms
64 bytes from fe80::5200:1ff:fe02:1%ens3: icmp_seq=3 ttl=64 time=2.59 ms
```

ICMPV6



ICMPv6 является неотъемлемой частью IPv6:

- Используется для сообщения об ошибках, возникающих при обработке пакетов, и для выполнения других функций, таких как диагностика

- Существует 2 типа сообщений ICMPv6 – ошибки (error - типы 0-127) и информация (information типы 128-255)

Neighbor Solicitation

- Узлы выполняют разрешение адресов путем многоадресной рассылки (multicast) **Neighbor Solicitation**, который просит целевой узел вернуть свой адрес канального уровня (MAC)

- Чтобы убедиться, что сосед все еще доступен

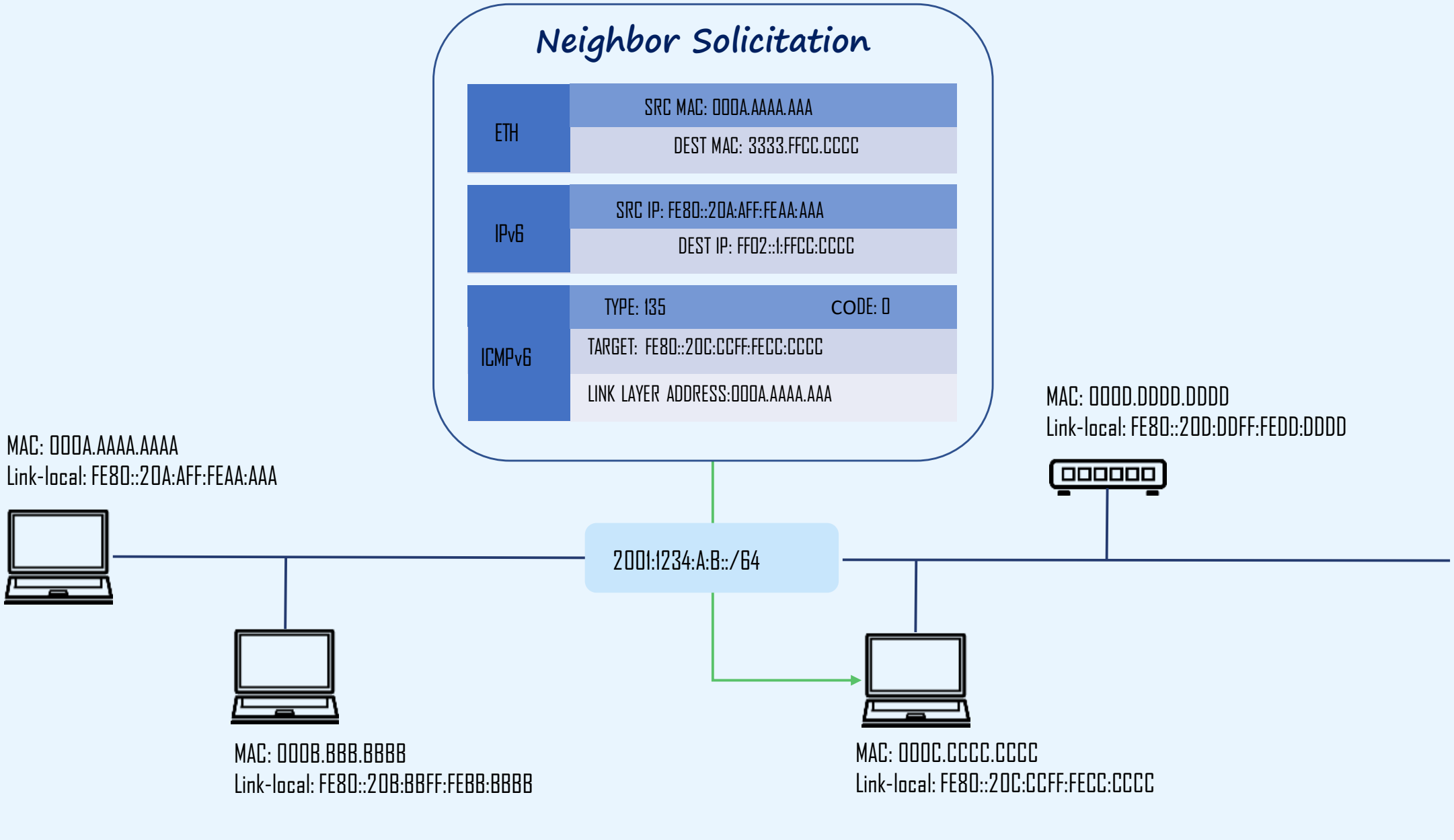
- Целевой узел возвращает свой адрес канального уровня (MAC) в одноадресном сообщении (unicast) **Neighbor Advertisement**

Neighbor Solicitation

- Одной пары пакетов запрос-ответ достаточно для обоих, чтобы разрешить адреса канального уровня (MAC) друг друга

- Neighbor Solicitation также используется для Duplicate Address Detection (DAD - обнаружение дублирующихся адресов)

Neighbor Solicitation



Neighbor Solicitation

Source:

- адрес, назначенный на интерфейсе, с которого отправляется сообщение, или (в процесса DAD) unspecified address

Destination:

- solicited-node multicast address или
- целевой адрес

```
root@ubuntu22-server:~# tcpdump -i ens3 -p ip6 -n -e
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:45:26.883305 50:00:00:01:00:00 > 33:33:ff:00:00:00, ethertype IPv6 (0x86dd), length 86: fe80::5200:ff:fe01:0 > ff02::1:ff00:0: ICMP6, neighbor solicitation, who has 2a05:4800:4:f200::, len
10:45:26.886265 50:00:01:02:00:01 > 50:00:00:01:00:00, ethertype IPv6 (0x86dd), length 86: 2a05:4800:4:f200:: > fe80::5200:ff:fe01:0: ICMP6, neighbor advertisement, tgt is 2a05:4800:4:f200::,
10:45:27.426069 50:00:00:01:00:00 > 50:00:00:01:00:00, ethertype IPv6 (0x86dd), length 86: fe80::5200:ff:fe01:0 > fe80::5200:ff:fe01:0: ICMP6, neighbor advertisement, tgt is 2a05:4800:4:f200:
10:45:32.482068 50:00:00:01:00:00 > 50:00:00:01:00:00, ethertype IPv6 (0x86dd), length 86: fe80::5200:ff:fe01:0 > fe80::5200:ff:fe01:0: ICMP6, neighbor solicitation, who has fe80::5200:ff:fe0
10:45:33.506083 50:00:00:01:00:00 > 50:00:00:01:00:00, ethertype IPv6 (0x86dd), length 86: fe80::5200:ff:fe01:0 > fe80::5200:ff:fe01:0: ICMP6, neighbor solicitation, who has fe80::5200:ff:fe0
10:45:34.530046 50:00:00:01:00:00 > 50:00:00:01:00:00, ethertype IPv6 (0x86dd), length 86: fe80::5200:ff:fe01:0 > fe80::5200:ff:fe01:0: ICMP6, neighbor solicitation, who has fe80::5200:ff:fe0

6 packets captured
```

Solicited-node multicast

- **Solicited-node multicast** адрес вычисляется из unicast и anycast адресов хоста.
  У всех адресов одинаковый префикс FF02::1:FF00:0/104. К указанному префиксу добавляются 24 low-order бита адреса (unicast или anycast), в результате solicited-node multicast адрес может быть в диапазоне от FF02:0:0:0:0:1:FF00:0000 до FF02:0:0:0:0:1:FFFF:FFFF
- Хост должен вычислить и присоединиться (на соответствующем интерфейсе) ко всем solicited-node multicast адресам, полученных из всех unicast и anycast адресов, которые настроены на интерфейсах хоста (вручную или автоматически)
- Solicited-node multicast адреса используются протоколом обнаружения соседей – Neighbor Discovery (ND или NDP)

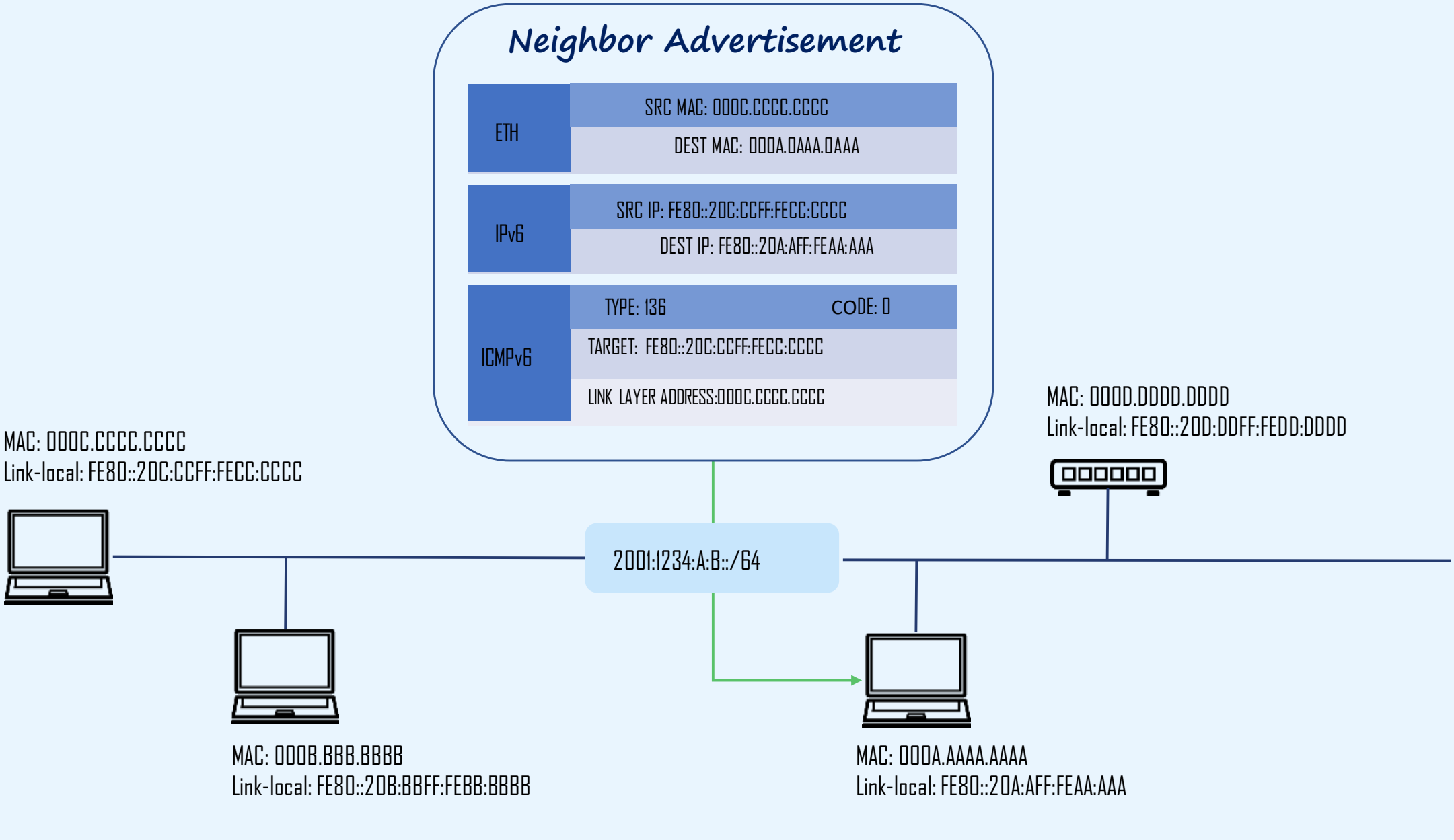
```
root@ubuntu22-server:~# ndisc6 -1 2a05:4800:4:f200:: ens3
Soliciting 2a05:4800:4:f200:: (2a05:4800:4:f200::) on ens3...
Target link-layer address: 50:00:01:02:00:01
 from 2a05:4800:4:f200::
```

Neighbor Advertisement

- Ответ на сообщение Neighbor Solicitation
- node также может отправить unsolicited (без запроса) Neighbor Advertisements для быстрого распространения новой информации (unreliably)
- Например, для анонсирования изменения link-layer адреса (MAC)

```
root@ubuntu22-server:~# ndisc6 -1 2a05:4800:4:f200:: ens3
Soliciting 2a05:4800:4:f200:: (2a05:4800:4:f200::) on ens3...
Target link-layer address: 50:00:01:02:00:01
 from 2a05:4800:4:f200::
```

Neighbor Advertisement



Neighbor Advertisement

Source:

- адрес, назначенный на интерфейсе, с которого отправляется сообщение

Destination:

- Source Address отправителя Neighbor Solicitation

Или

- all-nodes multicast address

```
root@ubuntu22-server:~# ndisc6 -1 2a05:4800:4:f200:: ens3
Soliciting 2a05:4800:4:f200:: (2a05:4800:4:f200::) on ens3...
Target link-layer address: 50:00:01:02:00:01
 from 2a05:4800:4:f200::
```

ICMP и ICMPv6

Спикер:
Роман Козлов

ICMPv4

01

Internet Control Message Protocol RFC 792 950

02

Является неотъемлемой частью IP и обязателен при реализации стека TCP/IP

03

Используется для передачи сообщений об ошибках и других исключительных ситуациях

04

Протокол IP инкапсулирует соответствующее ICMP-сообщение с новым заголовком IP 1

ICMPv6

01

Неотъемлемая часть IPv6 RFC 4443

02

Использует ICMPv6 и мультикаст

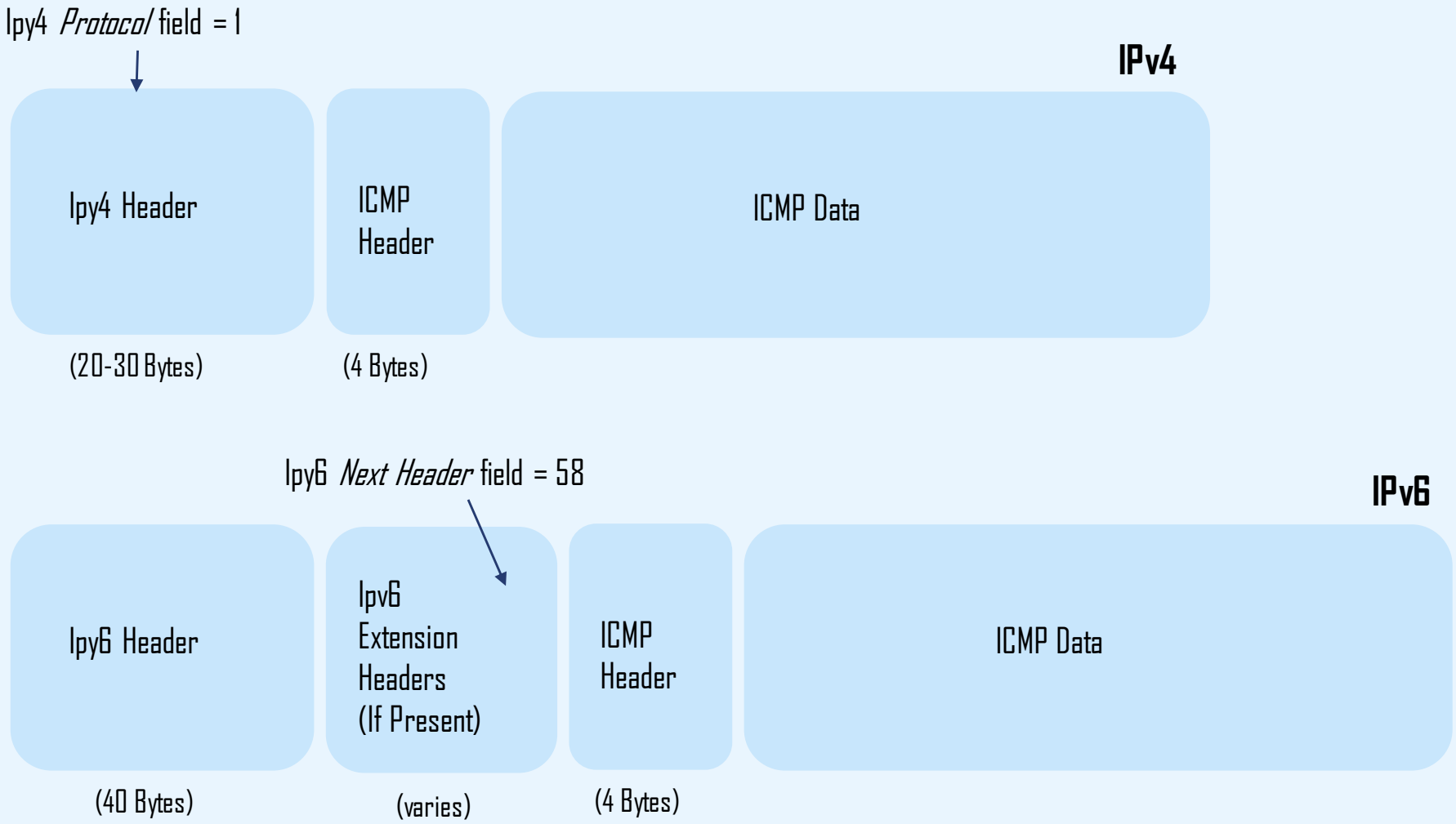
03

Сообщения об ошибках 0-127
и информационные сообщения
128-255

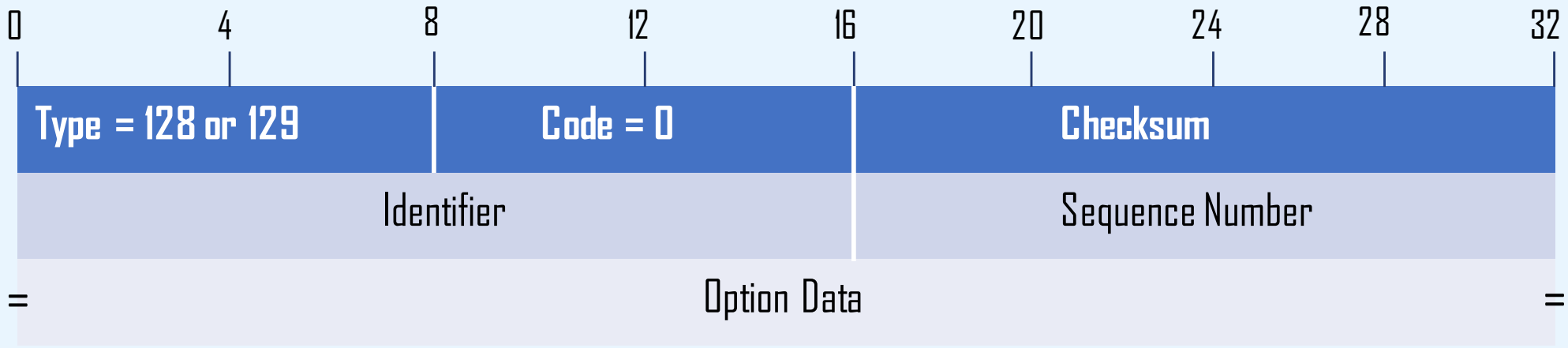
04

ICMPv6-сообщения инкапсулированы в пакеты IPv6 с полем Next Header, установленным в 58

ICMPv4 ICMPv6



ICMPv6


0
4
8
12
16
20
24
28
32
Type = 128 or 129
Code = 0
Checksum
Identifier
Sequence Number
Option Data