



# Технологии коммутации и маршрутизации современных сетей Ethernet

Базовый сертификационный курс



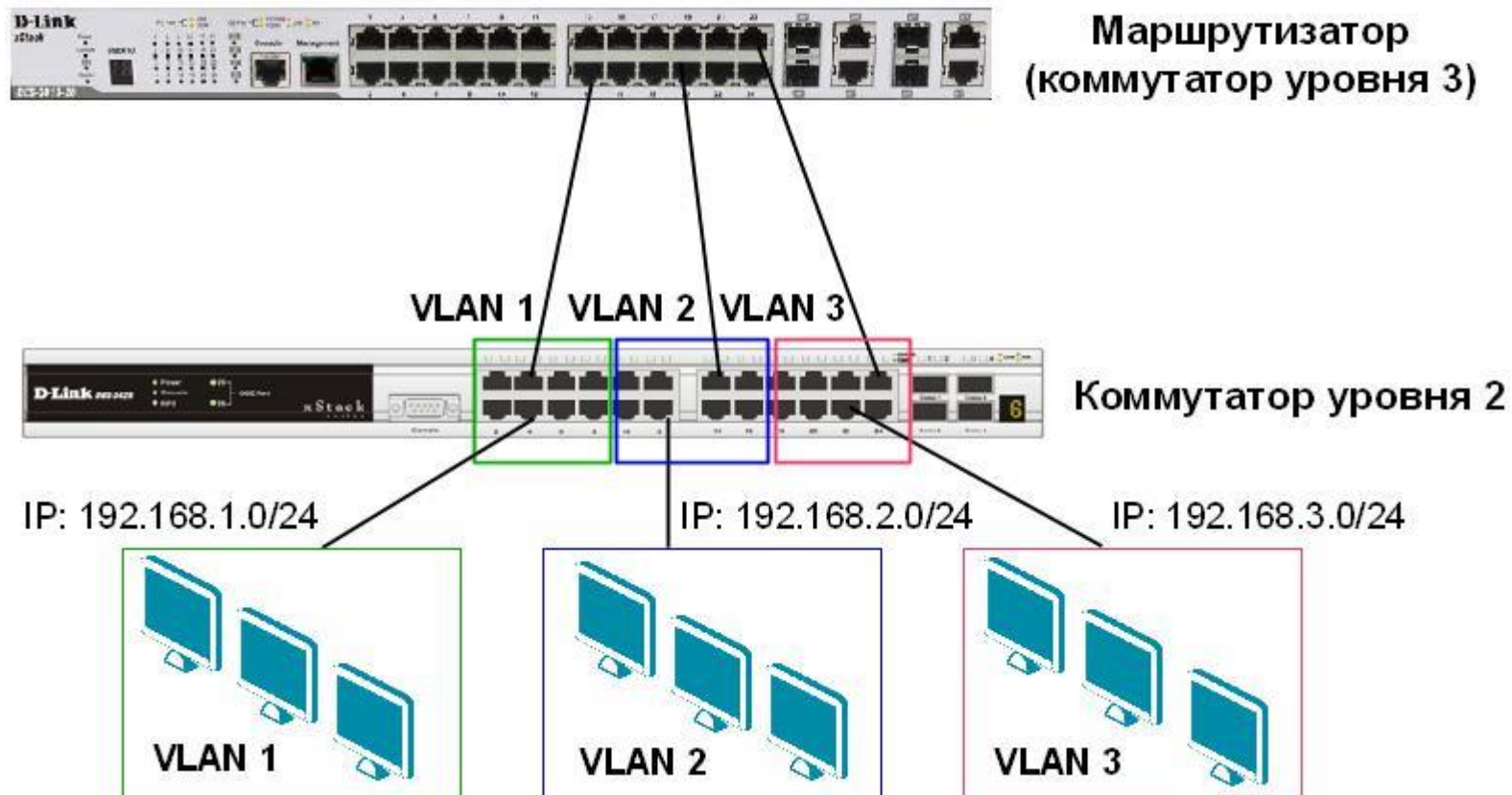
# **Введение в маршрутизацию**

## **Введение в маршрутизацию**

- Сетевой уровень
- Обзор IPv4-адресации сетевого уровня
- Формирование IPv4-подсетей
- Бесклассовая IPv4-адресация
- Способы настройки IPv4-адреса
- Протокол IPv6
- Типы IPv6 адресов
- Формирование идентификатора интерфейса
- Способы настройки IPv6-адреса
- Планирование подсетей IPv6
- Протокол NDP
- Маршрутизация

## Сетевой уровень

- ❑ При построении сетей передачи данных возникает задача организации связи между различными сетями или подсетями, образующими составную сеть. Эта задача решается с помощью функций *сетевого уровня (network layer)* модели OSI.



## Сетевой уровень

- ❑ В наиболее распространенном в настоящее время стеке протоколов TCP/IP за обработку данных на сетевом уровне отвечает *протокол IP*, который позволяет доставлять данные в сетях TCP/IP между любыми узлами составной сети и выполняет две основные функции:
  - маршрутизация;
  - адресация узлов (IP-адресация).
  
- ❑ Протокол IP не гарантирует надёжной доставки пакета до адресата, эта функция выполняется протоколами более высокого уровня. Такой тип доставки данных называют *best-effort*.

В настоящее время существует две версии протокола IP:

❖ **IP версии 4 (IPv4):**

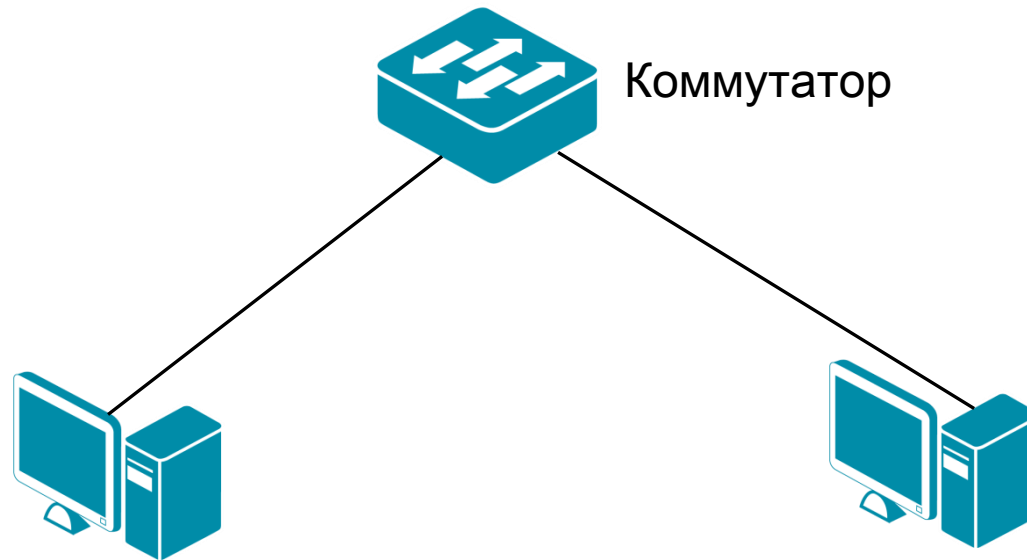
- описан в RFC 791 (сентябрь 1981 года), заменившем RFC 760 (январь 1980 года);
- использует 32-битные адреса, ограничивающие адресное пространство 4 294 967 296 ( $2^{32}$ ) возможными уникальными адресами.

❖ **IP версии 6 (IPv6):**

- описан в серии RFC, начиная с RFC 1883;
- использует 128-битные адреса ( $3,4 \cdot 10^{38}$  уникальных адресов).

## Обзор адресации сетевого уровня

- ❑ Каждое устройство, которое выполняет передачу данных, имеет связанный с ним **физический адрес** (MAC-адрес) на канальном уровне и назначенный ему **логический адрес** (IP-адрес) на сетевом уровне, который иногда называют *адресом третьего уровня*.



ПК 1:

Физический адрес: 11-A0-17-3D-BB-01

Логический адрес: 192.168.1.2

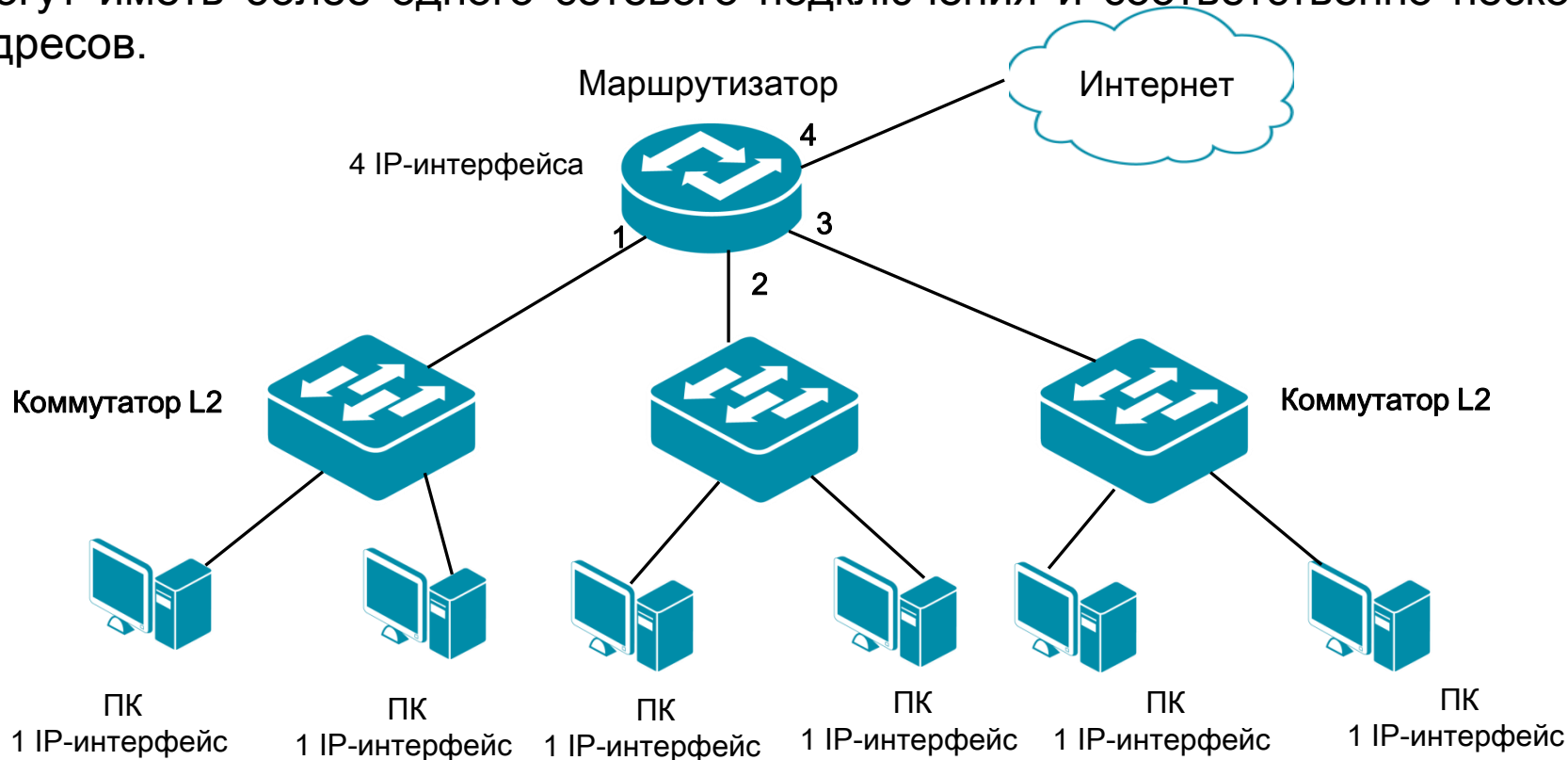
ПК 2:

Физический адрес: 11-A0-17-3D-BB-02

Логический адрес: 192.168.1.11

## Обзор адресации сетевого уровня

- ❑ Для того чтобы устройство могло участвовать в межсетевом взаимодействии с помощью протокола IP, ему должен быть присвоен уникальный IP-адрес, который позволяет однозначно идентифицировать интерфейс между устройством и сетью.
- ❑ IP-адрес не идентифицирует непосредственно устройство.
- ❑ Некоторые устройства, например, маршрутизаторы (коммутаторы 3-го уровня), могут иметь более одного сетевого подключения и соответственно несколько IP-адресов.



## Формат пакета IPv4

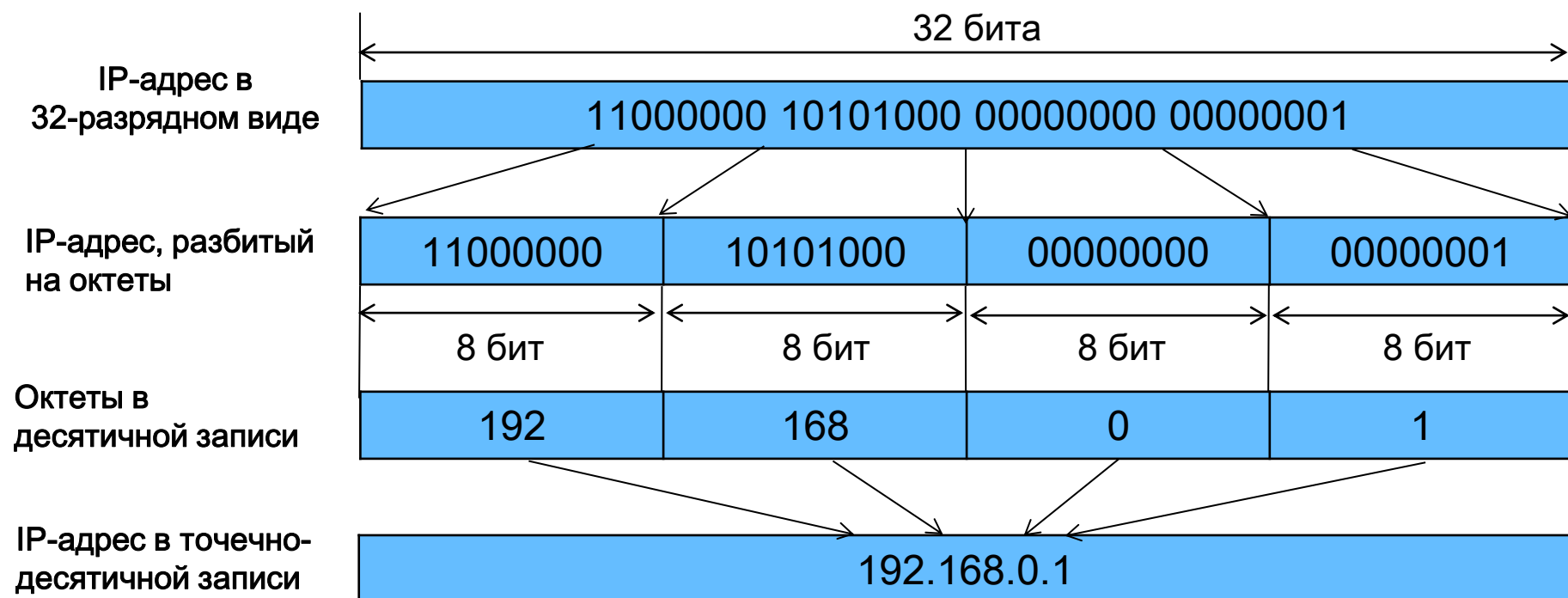
|                               |                          |                     |                            |                             |
|-------------------------------|--------------------------|---------------------|----------------------------|-----------------------------|
| Версия (4 бита)               | Длина заголовка (4 бита) | Тип сервиса (8 бит) | Общая длина (16 бит)       |                             |
| Идентификатор пакета (16 бит) |                          |                     | Флаги (3 бита)             | Смещение фрагмента (13 бит) |
| Время жизни (8 бит)           |                          | Протокол (8 бит)    | Контрольная сумма (16 бит) |                             |
| Адрес источника (32 бита)     |                          |                     |                            |                             |
| Адрес назначения (32 бита)    |                          |                     |                            |                             |
| Опции (необязательное)        |                          |                     |                            |                             |
| Данные                        |                          |                     |                            |                             |

Заголовок  
20 байт

- **Версия** (*Version*) — для IPv4 значение поля равно 4;
- **Длина заголовка** (*IHL, Internet Header Length*) – указывает на начало блока данных в пакете. Обычно значение для этого поля равно 5;
- **Тип сервиса** (*Type of Service*) – указывает приоритет пакета;
- **Общая длина** (*Total Length*) - общая длина пакета с учетом заголовка и поля данных;
- **Идентификатор пакета** (*Identification*) – используется для распознавания пакетов, образованных при фрагментации исходного пакета;
- **Флаги** (*Flags*) – содержит признаки, связанные с фрагментацией пакета;
- **Смещение фрагмента** (*Fragment Offset*) – значение, определяющее позицию фрагмента в потоке данных;
- **Время жизни** (*Time to Live*) – временной интервал, в течение которого пакет может перемещаться по сети маршрутизаторами;
- **Протокол** (*Protocol*) – указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета;
- **Контрольная сумма** (*Header Checksum*) – рассчитывается только по заголовку и позволяют определить целостность пакета;
- **IP-адрес источника** (*Source IP Address*) и **IP-адрес назначения** (*Destination IP Address*) – указывают отправителя и получателя пакета;
- **Опции** (*Options*) – необязательное поле, используется при отладке сети.

## Представление IPv4-адреса

- ❑ Адрес IPv4 представляет собой 32-разрядное (4 байта) двоичное поле. Для удобства восприятия и запоминания этот адрес разделяют на 4 части по 8 бит (октеты), каждый октет переводят в десятичное число и при записи разделяют точками. Это представление адреса называется *десятично-точечной нотацией*.



Преобразование октета из двоичного вида в десятичный:

| Двоичное значение октета | Значение битов октета | Десятичное значение октета |
|--------------------------|-----------------------|----------------------------|
| 00000000                 | 0                     | 0                          |
| 10000000                 | 128                   | 128                        |
| 11000000                 | 128+64                | 192                        |
| 11100000                 | 128+64+32             | 224                        |
| 11110000                 | 128+64+32+16          | 240                        |
| 11111000                 | 128+64+32+16+8        | 248                        |
| 11111100                 | 128+64+32+16+8+4      | 252                        |
| 11111110                 | 128+64+32+16+8+4+2    | 254                        |
| 11111111                 | 128+64+32+16+8+4+2+1  | 255                        |

## Адрес IPv4

- IPv4-адрес структурирован и состоит из двух логических частей:
- **Идентификатор сети** - Network Identifier (Net ID) – определяет конкретную сеть или сегмент сети, в которой находится узел и используется для маршрутизации.
  - **Идентификатор узла** - Host Identifier (Host ID) – используется для уникальной идентификации узла внутри сети или сегмента сети.



## Классовая адресация IPv4

Задача: оптимизация адресов с точки зрения максимально эффективного использования IPv4-адресного пространства.

Решение: использование классовой модели IP-адресации.

- Все пространство IP-адресов делится на 5 классов в зависимости от значения первых четырех бит IPv4-адреса.
- Классам присвоены имена от А до Е.



## Классовая адресация IPv4

- ❑ Согласно классовой модели адресации, существует определенное количество сетей каждого класса и в сети каждого класса может быть адресовано только определенное количество сетевых узлов.

| Класс адреса | Диапазон адресов            | Доступное количество сетей | Доступное количество узлов |
|--------------|-----------------------------|----------------------------|----------------------------|
| Класс А      | 1.0.0.0 – 126.0.0.0         | 126                        | 16 777 214                 |
| Класс В      | 128.0.0.0 – 191.255.0.0     | 16 384                     | 65 532                     |
| Класс С      | 192.0.0.0 – 223.255.255.0   | 2 097 152                  | 254                        |
| Класс D      | 224.0.0.0 – 239.255.255.254 | Multicast                  | -                          |
| Класс E      | 240.0.0.0 – 254.255.255.255 | Зарезервировано            | -                          |

## Частные и публичные адреса IPv4

- ❑ **Публичные (public) IP-адреса** – уникальные адреса, которые не должны повторяться в глобальной сети.
  - ❑ **Частные (private) IP-адреса** – используются в локальных сетях и не маршрутизируются в глобальную сеть.
- 
- Публичные адреса находятся в пределах от 1.0.0.1 до 223.255.255.254 за исключением частных адресов IPv4.
  - Адресное пространство частных IPv4-адресов состоит из 3 блоков:
    - 10.0.0.0 – 10.255.255.255 (класс A);
    - 172.16.0.0 – 172.31.255.255 (класс B);
    - 192.168.0.0 – 192.168.255.255 (класс C).

## Специальные IPv4-адреса

| Идентификатор сети | Идентификатор узла | Описание                                                                                                                                                                                                                            |
|--------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Все «0»            | Все «0»            | 0.0.0.0 – адрес узла, сгенерировавшего пакет. Используется устройством для ссылки на самого себя, если оно не знает свой IPv4-адрес. Используется, например, когда устройство пытается получить IPv4-адрес с помощью протокола DHCP |
| Все «0»            | Идентификатор узла | Узел назначения принадлежит той же сети, что и узел-отправитель, например, 0.0.0.25                                                                                                                                                 |
| Идентификатор сети | Все «0»            | Адрес сети IPv4, например 175.11.0.0                                                                                                                                                                                                |
| Идентификатор сети | Все «1»            | Ограниченный широковещательный адрес (в пределах данной IP-сети), например 192.168.100.255                                                                                                                                          |
| Все «1»            | Все «1»            | 255.255.255.255 – «глобальный» широковещательный адрес                                                                                                                                                                              |
| 127.0.0.0          |                    | Адрес интерфейса обратной петли (loopback), предназначен для тестирования оборудования без реальной отправки пакета                                                                                                                 |

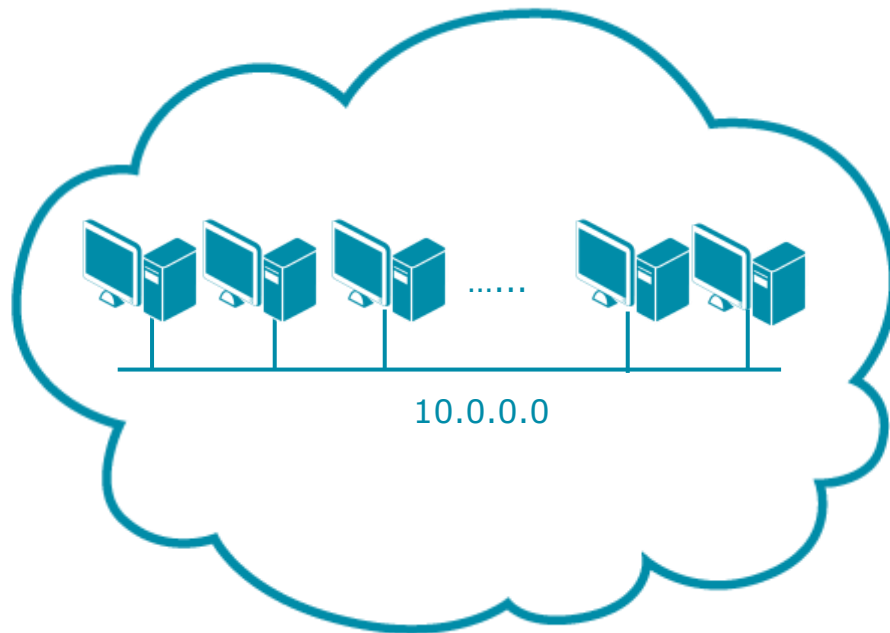
## Формирование подсетей

- ❑ Изначально IPv4-адрес имел два уровня иерархии: идентификатор сети и идентификатор узла.
- ❑ Каждой организации выдавался IPv4-адрес из нужного диапазона (А, В и С) в зависимости от текущего числа компьютеров и его планируемого увеличения.
- ❑ Для более эффективного использования адресного пространства были внесены изменения в существующую классовую систему адресации. В RFC 950 была описана процедура разбиения сетей на подсети, и в структуру IPv4-адреса был добавлен еще один уровень – *подсеть* (subnetwork).

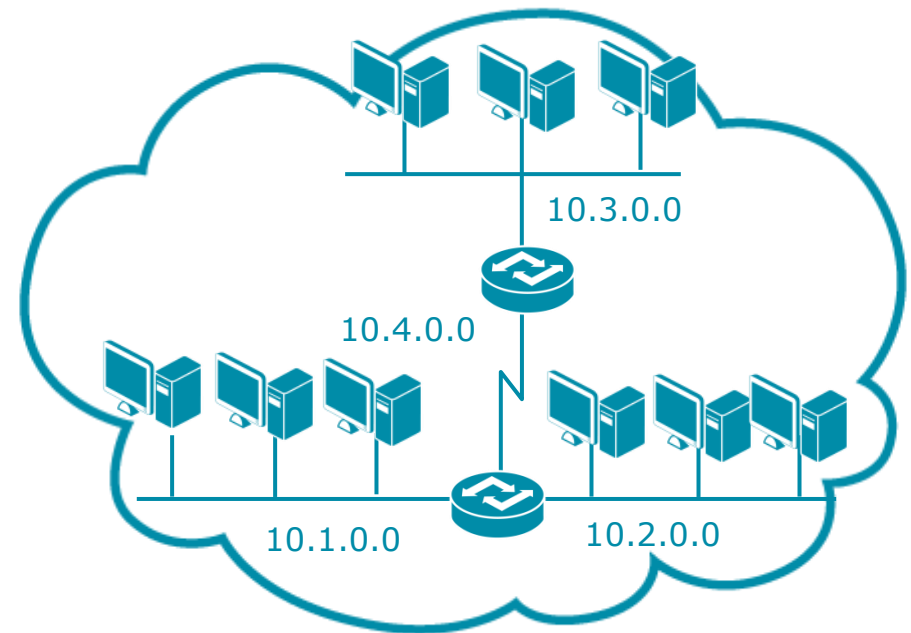


## Формирование подсетей

- ❑ Разбиение одной крупной сети на несколько мелких позволяет:
  - рационально использовать адресное пространство (т.е. выделить для сегмента сети блок адресом не целиком класса А, В или С, а только часть классовой сети);
  - повысить безопасность и управляемость сети (за счет уменьшения размеров сегментов и изоляции трафика сегментов друг от друга).



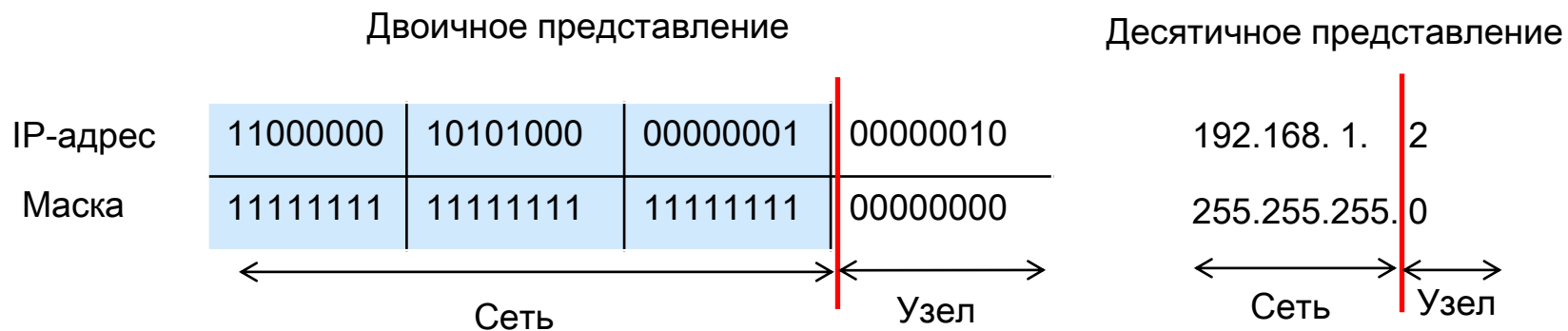
Адресное пространство класса А  
без разбиения на подсети



Адресное пространство класса А  
после разбиения на подсети

## Маска подсети

- ❑ С появлением трехуровневой иерархии IPv4-адреса потребовались дополнительные методы, которые позволяли бы определить, какая часть адреса указывает на идентификатор сети, а какая – на идентификатор узла. Было предложено использовать *маску подсети*.
- ❑ **Маска подсети** (subnet mask) – это 32-битное число, двоичная запись которого содержит единицы в тех разрядах, которые должны определяться как идентификатор сети.
- ❑ Маска подсети записывается в десятично-точечной нотации аналогично IPv4-адресу.



## Маска подсети

- Чтобы получить адрес сети, зная IPv4-адрес и маску подсети, необходимо применить к ним операцию *логическое «И»*. Другими словами, в тех позициях IPv4-адреса, в которых в маске подсети стоят двоичные 1, находится идентификатор сети, а где двоичные 0 – идентификатор узла.

|            |          |          |          |          |                     |
|------------|----------|----------|----------|----------|---------------------|
| IP-адрес   | 11000000 | 10101000 | 00000001 | 00000010 | 192.168. 1. 2       |
| Маска      | 11111111 | 11111111 | 11111111 | 00000000 | &<br>255.255.255. 0 |
| Адрес сети | 11000000 | 10101000 | 00000001 | 00000000 | =<br>192.168.1.0    |

Во избежание проблем с адресацией и маршрутизацией **все компьютеры** стека TCP/IP **в одном сегменте** сети **должны использовать одну и ту же маску подсети**.

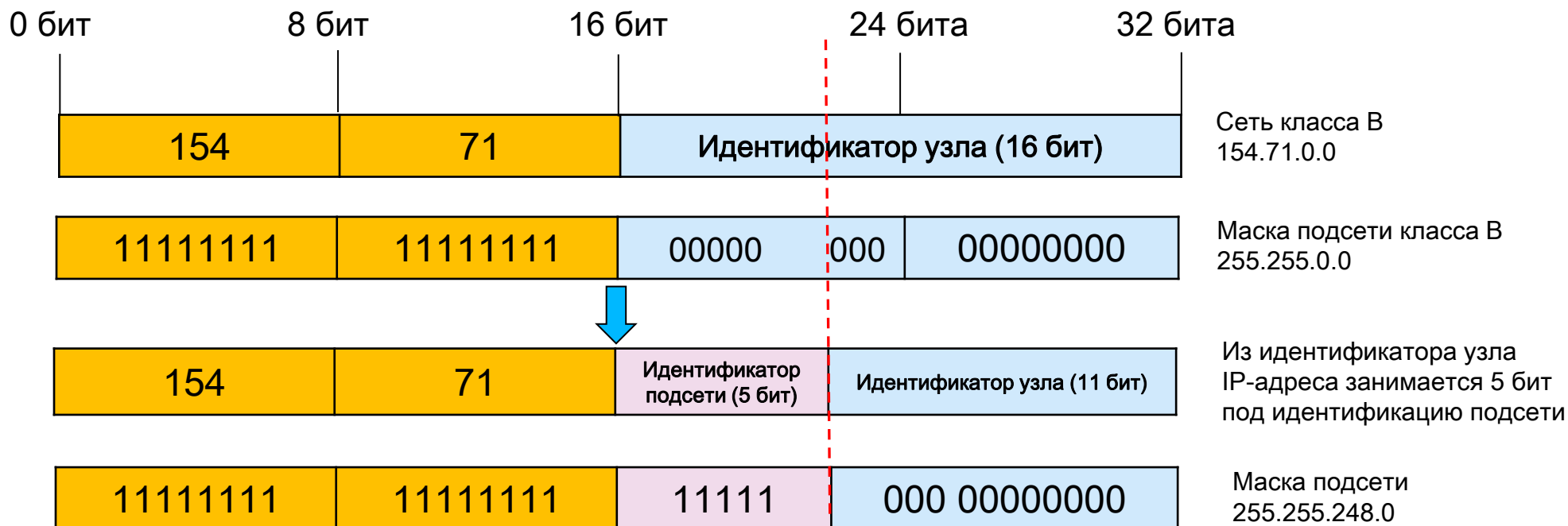
## Маски подсети для стандартных классов сетей

- ❑ Для сетей класса А, В и С определены фиксированные маски подсети, которые жестко определяют количество возможных IPv4-адресов и механизм маршрутизации.

| Класс сети | Маска подсети | Количество бит идентификатора |
|------------|---------------|-------------------------------|
| Класс А    | 255.0.0.0     | 8                             |
| Класс В    | 255.255.0.0   | 16                            |
| Класс С    | 255.255.255.0 | 24                            |

## Планирование подсетей

- ❑ При использовании масок подсети сети можно разделять на меньшие по размеру подсети путем расширения сетевой части адреса и уменьшения узловой части.
- ❑ Для вычисления *количества подсетей* существует формула  $2^s$ , где  $s$  – количество бит, занятых под идентификатор сети из части, отведенной под идентификатор узла.
- ❑ *Количество узлов* в каждой подсети вычисляется по формуле  $2^n - 2$ , где  $n$  – количество бит, оставшихся в части, идентифицирующей узел, а два адреса – адрес подсети и широковещательный адрес – в каждой полученной подсети зарезервированы.



## Пример планирования подсетей

**Задача:** разбить сеть 192.168.1.0 на 20 подсетей по 6 компьютеров в каждой.

**Решение:**

1. Определить, к какому классу относится IPv4-адрес. 192.168.1.0 – это класс C, стандартная маска подсети класса C – 255.255.255.0;
2. Определить количество бит, занимаемых для формирования 20 подсетей. Поскольку найти число, при котором степень 2 будет равна 20 невозможно, выбираем ближайшее большее число  $2^5 = 32$ . Таким образом, количество бит подсети = 5, количество бит для идентификации узлов в подсети = 3.

## Пример планирования подсетей

|          |          |          |          |                                  |
|----------|----------|----------|----------|----------------------------------|
| 11000000 | 10101000 | 00000001 | 00000000 | Сеть класса C<br>192.168.1.0/24  |
| 11111111 | 11111111 | 11111111 | 00000000 |                                  |
| ↓        |          |          |          |                                  |
| 11000000 | 10101000 | 00000001 | 00000000 | Подсеть 1<br>192.168.1.0         |
| 11111111 | 11111111 | 11111111 | 11111000 | Маска подсети<br>255.255.255.248 |
| ↓        |          |          |          |                                  |
| 11000000 | 10101000 | 00000001 | 00001000 | Подсеть 2<br>192.168.1.8         |
| 11111111 | 11111111 | 11111111 | 11111000 | Маска подсети<br>255.255.255.248 |
| ↓        |          |          |          |                                  |
| 11000000 | 10101000 | 00000001 | 00010000 | Подсеть 3<br>192.168.1.16        |
| 11111111 | 11111111 | 11111111 | 11111000 | Маска подсети<br>255.255.255.248 |
| ...      |          |          |          | ...                              |
| 11000000 | 10101000 | 00000001 | 10011000 | Подсеть 20<br>192.168.1.152      |
| 11111111 | 11111111 | 11111111 | 11111000 | Маска подсети<br>255.255.255.248 |

## Бесклассовая адресация

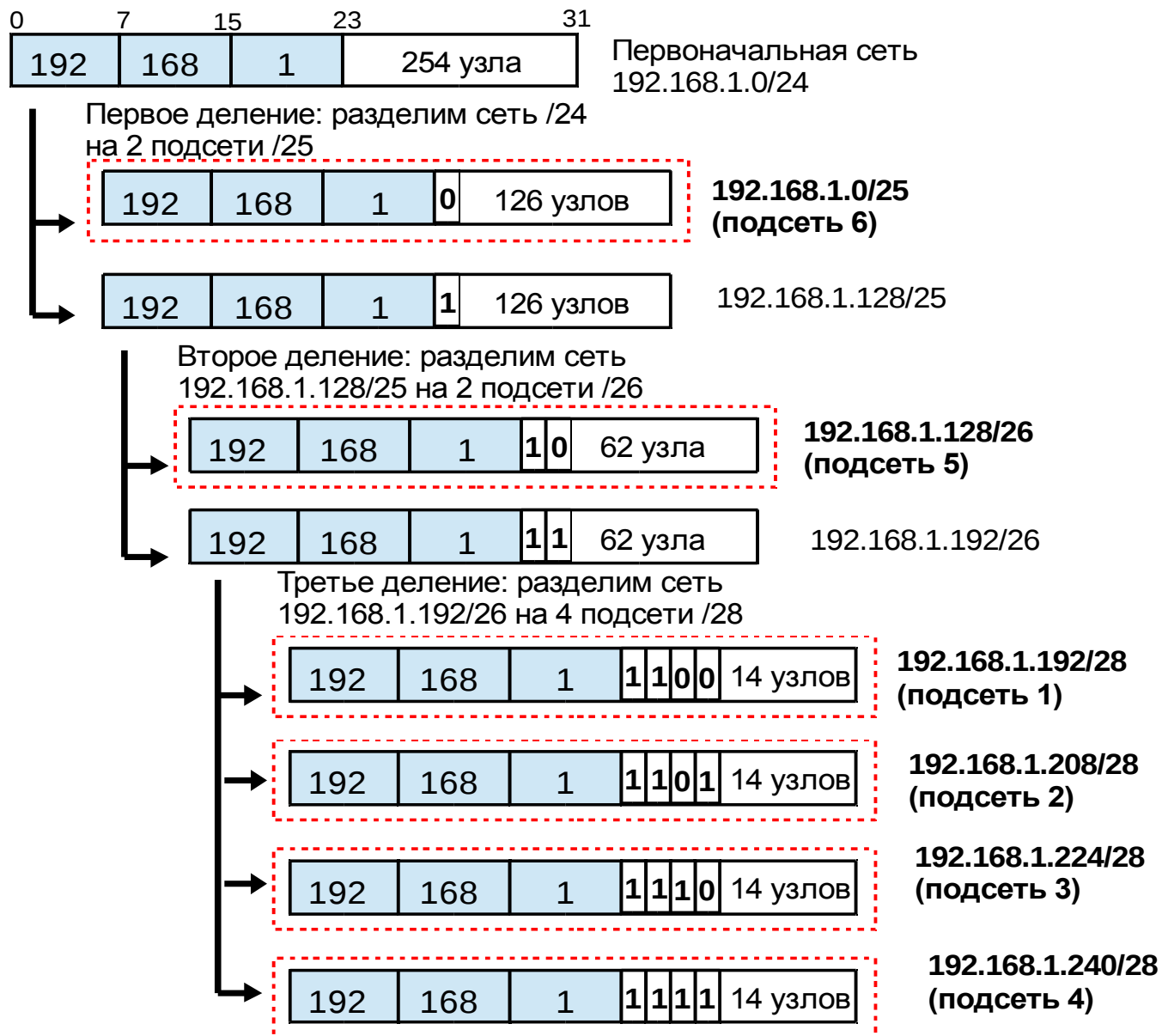
- ❑ Классовая модель адресации оказалась нерациональной с точки зрения эффективного использования адресного пространства.
- ❑ В случае классовой адресации сеть можно разбить только на подсети одинакового размера.
- ❑ В бесклассовой модели IPv4-адресации:
  - отсутствует привязка к классу сети и маске подсети по умолчанию;
  - используется маски подсети переменной длины (Variable Length Subnet Mask, VLSM);
  - использует технологию бесклассовой междоменной маршрутизации (Classless Inter Domain Routing, CIDR).
- ❑ Маска VLSM позволяет разбить сеть на подсети, а потом подсеть разбить еще на подсети с различными масками подсети.
- ❑ Маски подсети являются основой метода бесклассовой маршрутизации и записываются в виде нотации «IP-адрес/длина префикса». Число после символа «/» означает количество единичных разрядов в маске подсети.
- ❑ Например, адрес 192.168.1.8 с маской подсети 255.255.255.248 может быть записан 192.168.1.8/29

## Маски подсети переменной длины

**Задача:** организации выделена сеть класса С 192.168.1.0/24. Требуется разделить ее на 6 подсетей. В подсетях 1, 2, 3 и 4 должно быть 10 узлов, в 5-й подсети – 50, в 6-й подсети – 100.

- ☐ Теоретически для сети 192.168.1.0/24 допустимое количество узлов равно 254, и разбить такую сеть на подсети с требуемым количеством узлов без использования VLSM невозможно.

## Маски подсети переменной длины



## Способы настройки IPv4-адреса

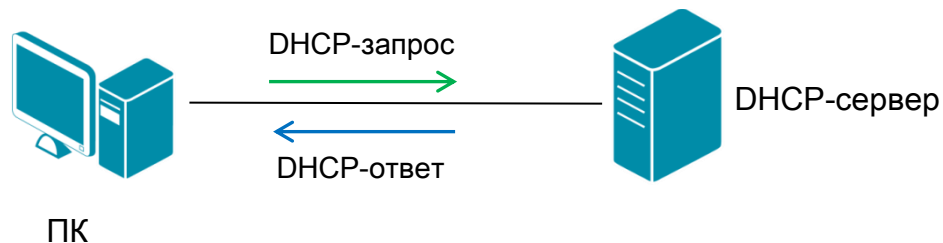
### ❖ Статическая настройка:

- IP-адрес называют статическим (постоянным, неизменяемым), если он назначается пользователем в настройках устройства.
- администратор вручную вводит IP-адрес, маску подсети и адрес шлюза по умолчанию.



### ❖ Динамическая настройка:

- IP-адрес называют динамическим (непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, указанного в сервисе назначавшем IP-адрес (DHCP).

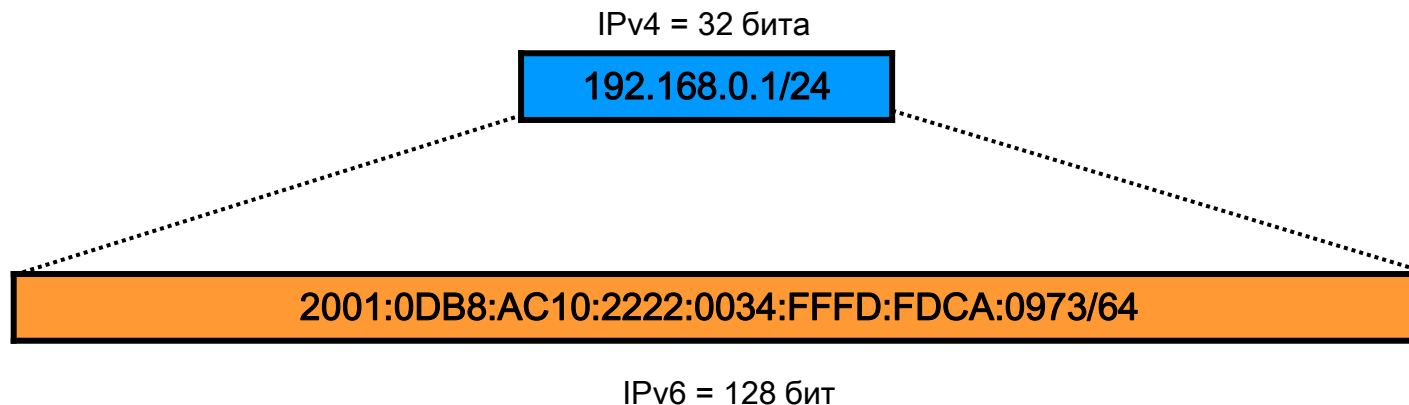


## Протокол IPv6

- ❖ Протокол IPv6 – это новая версия протокола IP, которая разработана в качестве приемника IPv4 и призвана решить проблему исчерпания адресного пространства.

Основным отличием протокола IPv6 от IPv4 является:

- ☐ Больше адресное пространство:
  - размер адреса IPv6 составляет 128 бит;
  - поддерживает  $2^{128}$  (примерно  $3,4 \times 10^{38}$ ) адресов.
- ☐ улучшенные механизмы автоматического назначения адресов узлов;
- ☐ упрощение маршрутизации;
- ☐ улучшенные механизмы обеспечения качества обслуживания (QoS) и безопасности (IPSec);
- ☐ упрощенный заголовок пакета.



## Формат заголовка IPv6

Фиксированный заголовок состоит из 40 байт и имеет следующий формат:

| Версия<br>(4 бита)          | Класс трафика<br>(8 бит) | Метка потока<br>(20 бит)    |                                |
|-----------------------------|--------------------------|-----------------------------|--------------------------------|
| Размер поля данных (16 бит) |                          | Следующий заголовок (8 бит) | Предельное число шагов (8 бит) |
| Адрес источника (128 бит)   |                          |                             |                                |
| Адрес назначения (128 бит)  |                          |                             |                                |

- **Версия (Version)** — для IPv6 значение поля равно 6;
- **Класс трафика (Traffic Class)** – поле приоритета пакета;
- **Метка потока (Flow Label)** – используется отправителем для обозначения последовательности пакетов, которые должны быть подвергнуты определенной обработке маршрутизаторами;
- **Размер поля данных (Payload Length)** - число, указывающее длину поля данных, идущего за заголовком пакета (с учетом расширенного заголовка);
- **Следующий заголовок (Next Header)** – задает тип расширенного заголовка IPv6, который следует за фиксированным;
- **Предельное число шагов (Hop Limit)** – уменьшается на 1 каждым маршрутизатором, через который передается пакет. При значении, равном 0, пакет отбрасывается;
- **Адрес источника (Source Address)** – 128-битный адрес отправителя пакета;
- **Адрес назначения (Destination Address)** – 128-битный адрес получателя пакета.

## Сравнение форматов пакетов IPv4 и IPv6

Заголовок IPv4 (20 байт)

|                               |                                |                           |                            |                                |
|-------------------------------|--------------------------------|---------------------------|----------------------------|--------------------------------|
| Версия<br>(4 бита)            | Длина<br>заголовка (4<br>бита) | Тип<br>сервиса<br>(8 бит) | Общая длина (16 бит)       |                                |
| Идентификатор пакета (16 бит) |                                |                           | Флаги<br>(3 бита)          | Смещение фрагмента<br>(13 бит) |
| Время жизни (8 бит)           |                                | Протокол<br>(8 бит)       | Контрольная сумма (16 бит) |                                |
| Адрес источника (32 бита)     |                                |                           |                            |                                |
| Адрес назначения (32 бита)    |                                |                           |                            |                                |

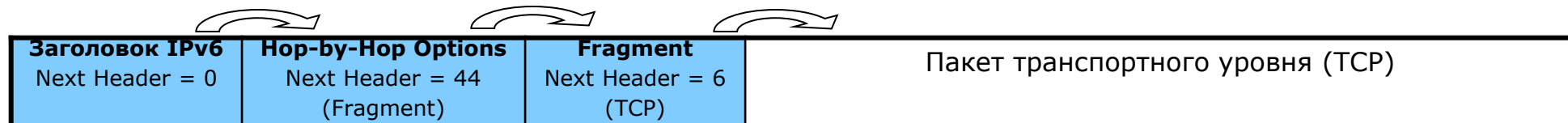
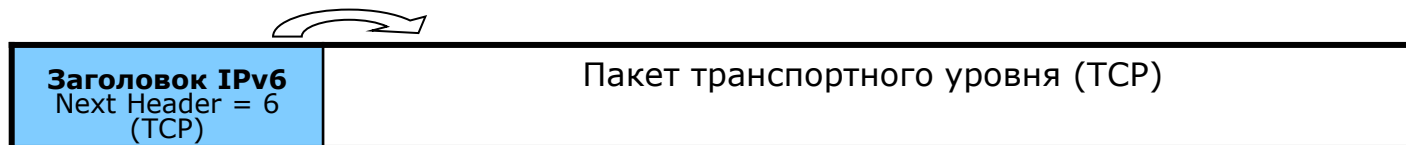
Заголовок IPv6 (40 байт)

|                             |                       |                       |                             |                                |
|-----------------------------|-----------------------|-----------------------|-----------------------------|--------------------------------|
| Версия (4 бита)             | Класс трафика (8 бит) | Метка потока (20 бит) |                             |                                |
| Размер поля данных (16 бит) |                       |                       | Следующий заголовок (8 бит) | Предельное число шагов (8 бит) |
| Адрес источника (128 бит)   |                       |                       |                             |                                |
| Адрес назначения (128 бит)  |                       |                       |                             |                                |

## Расширенные заголовки IPv6

- ❑ Используются для поддержки механизмов безопасности, фрагментации, сетевого управления и расположены между фиксированным заголовком и заголовком протокола более высокого уровня.
- ❑ Пакет IPv6 может содержать 0, 1 или несколько расширенных заголовков, каждый из которых идентифицируется значением поля Next Header предшествующего заголовка.

| Расширенный заголовок                | Тип | Описание                                                                                  |
|--------------------------------------|-----|-------------------------------------------------------------------------------------------|
| Hop-by-Hop Options                   | 0   | Параметры которые должны быть обработаны каждым транзитным узлом                          |
| Routing                              | 43  | Позволяет отправителю определять список узлов, которые пакет должен пройти                |
| Fragment                             | 44  | Содержит информацию по фрагментации пакета                                                |
| Encapsulating Security Payload (ESP) | 50  | Обеспечивает шифрование данных с помощью IPSec                                            |
| Destination Options                  | 60  | Определяет произвольный набор опций, которые должны быть обработаны получателем пакета    |
| Authentication Header (AH)           | 51  | Содержит информацию для проверки подлинности зашифрованных данных при использовании IPSec |



## Представление адреса IPv6

- ❖ Адрес IPv6 имеет длину 128 бит и записывается как восемь групп по четыре шестнадцатеричные цифры, разделенные двоеточием. Например,

2001:0DB8:AC10:FE01:0018:8BFF:FED8:E3E0

- ❑ Существует несколько способов, которые позволяют сократить запись IPv6-адреса:

- нули в начале группы можно заменить одним;
- одна или несколько идущих подряд групп, состоящих из нулей, может быть заменена знаком «::»;

0001:0123:0000:0000:0000:ABCD:0000:0001

0001:0123:0:0:0:ABCD:0:1

1:123::ABCD:0:1

- конечные нули в группе должны присутствовать.

2001:1000:0000:0000:0000:ABCD:0000:0001

2001:1000::ABCD:0:1

## Представление адреса IPv6

- Альтернативной формой записи адреса, которая удобна для использования в смешанной среде с узлами IPv4 и IPv6, является запись вида

`x:x:x:x:x:x:d.d.d.d`

«x» – шестнадцатеричное значение 6 первых групп адреса, «d» – десятичное значение 4 последних групп адреса (стандартное представление адреса IPv4).

`0:0:0:0:0:0:13.1.68.3` или `::13.1.68`

`0:0:0:0:0:FFFF:129.144.52.38` или `::FFFF:129.144.52.38`

## Структура адреса IPv6

IPv6-адрес состоит из двух логических частей:

- ❖ **Префикс (Prefix)** – первые 64 бита адреса – часть адреса, отведенная под идентификатор сети/подсети (аналог идентификатора сети в IPv4). Представление префикса идентификатора для сети и подсети IPv6 аналогично записи префикса адреса IPv4 в нотации CIDR. Префикс адреса IPv6 записывается в виде

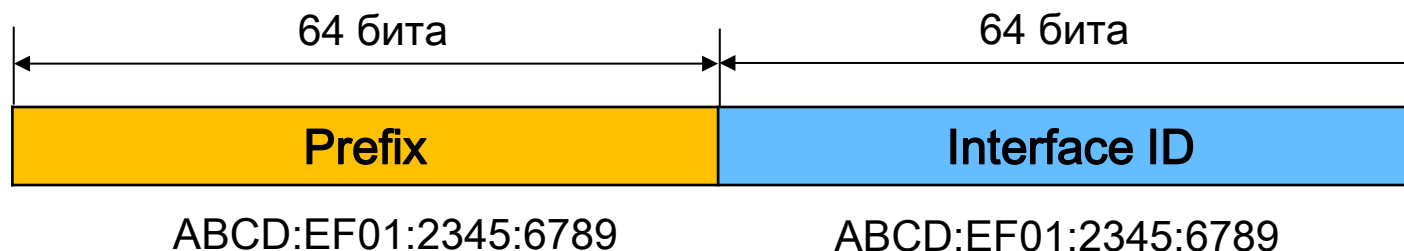
адрес IPv6/длина префикса

Пример:

21DA:D3::/48 – префикс сети

21DA:D3:0:2F3B::/64 – префикс подсети

- ❖ **Идентификатор интерфейса (Interface ID)** – последние 64 бита IPv6-адреса, используемые для идентификации интерфейса в сегменте сети (аналог идентификатора узла в IPv4). Он должен быть уникальным внутри сети/подсети.



## Типы IPv6-адресов

Адресное пространство протокола IPv6 разделено на три типа адресов:

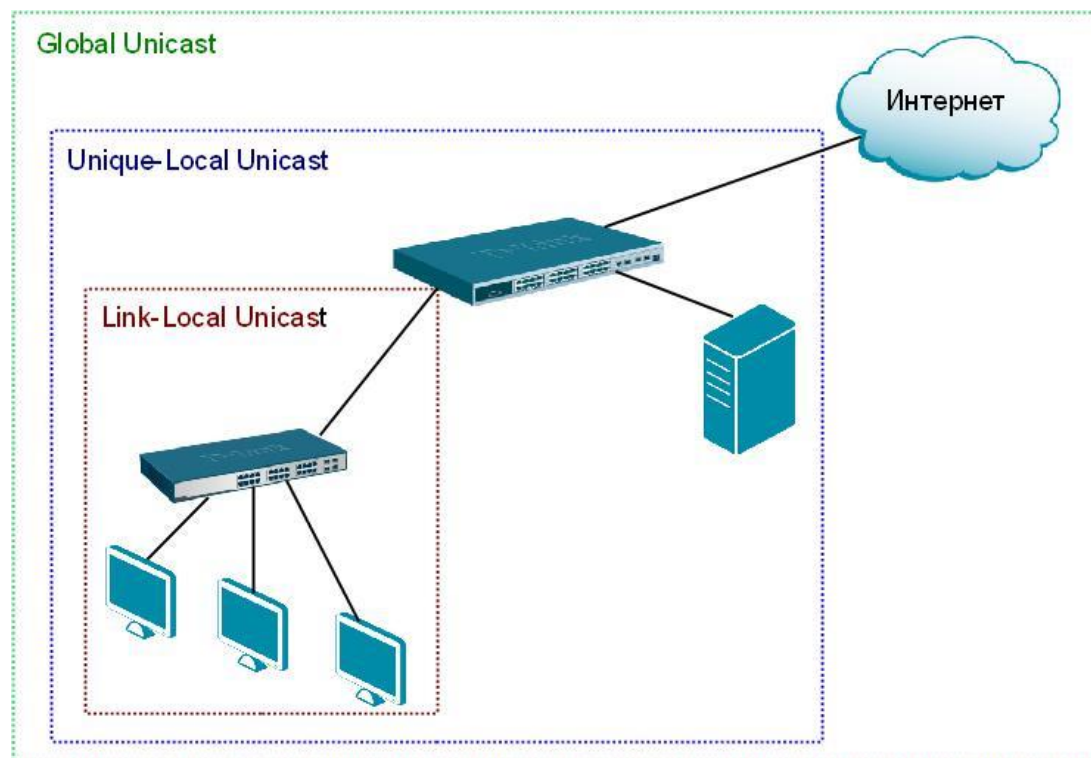
- ❖ **Индивидуальные адреса** (unicast) идентифицируют один интерфейс устройства. Пакеты, отправленные на этот адрес, доставляются только на этот интерфейс;
- ❖ **Групповые адреса** (multicast) идентифицируют группу адресов. Пакеты, посылаемые на этот адрес, доставляются всем интерфейсам – участникам группы;
- ❖ **Альтернативные адреса** (anycast) позволяют адресовать группу интерфейсов (обычно принадлежащих разным узлам). Однако в отличие от групповых адресов, пакеты, передаваемые на альтернативный адрес, доставляются на один из интерфейсов (обычно «ближайший» интерфейс, согласно метрике маршрутизации), определяемых этим адресом.
- *Широковещательные адреса* (broadcast), которые используются в IPv4, в IPv6 отсутствуют, что способствует уменьшению сетевого трафика и снижению нагрузки на большинство систем. Широковещательные адреса заменены групповыми.

## Индивидуальные IPv6-адреса

Существует несколько типов индивидуальных IPv6-адресов:

- ❖ Global Unicast;
- ❖ Unique-Local Unicast;
- ❖ Link-Local Unicast.

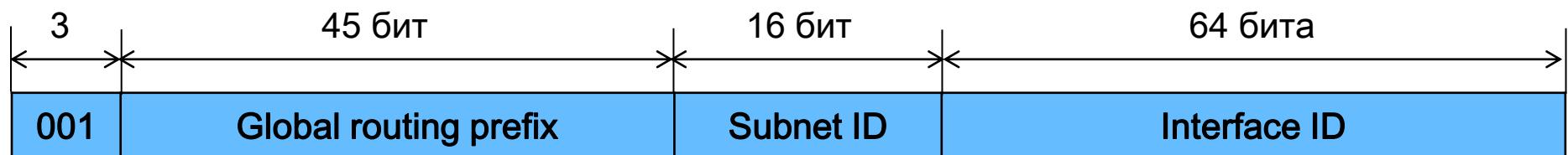
- ❑ Интерфейс всегда имеет адреса Link-Local, Unique-Local и Global.
- ❑ Для каждого типа индивидуальных адресов определен свой диапазон:



## Global Unicast-адреса:

- ❖ используются для идентификации устройств в глобальной сети и являются аналогом публичных IPv4-адресов;
- ❖ назначаются локальными интернет-регистраторами;
- ❖ в настоящее время назначаются с префикса 2000::/3.

□ Общий формат Global Unicast IPv6-адреса следующий:



- **Global routing prefix** – глобальный адрес, назначенный сети;
- **Subnet ID** – идентификатор подсети внутри сети;
- **Interface ID** – идентификатор интерфейса.

## Unique-Local Unicast-адреса:

- ❖ используются для идентификации устройств внутри организации и не передаются через интернет;
  - ❖ эквивалентны частным IPv4-адресам, однако в отличие от них являются уникальными в рамках глобальной сети;
  - ❖ начинаются с префикса FC00::/7.
- Общий формат Unique-Local Unicast IPv6-адреса следующий:



□ Бит L разбивает префикс FC00::/7 на два поддиапазона:

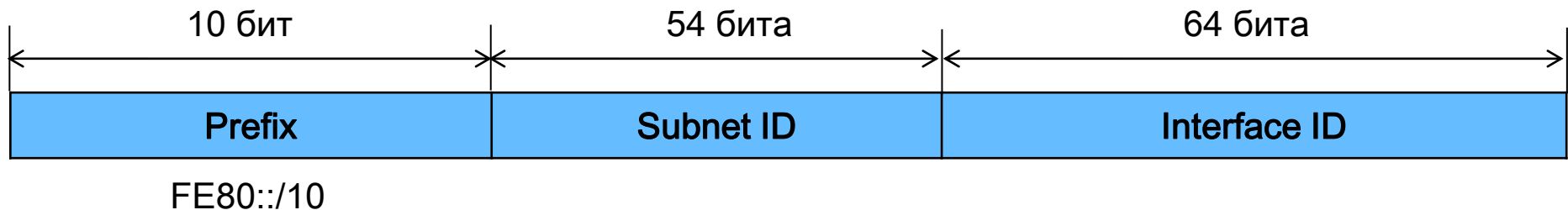
- FD00::/8 – локально назначенный уникальный адрес;
- FC00::/8 – зарезервирован для будущих применений.

- **Global ID** – глобальный идентификатор, который определяет организацию (назначается с помощью псевдослучайного алгоритма);
- **Subnet ID** – идентификатор подсети внутри сети;
- **Interface ID** – идентификатор интерфейса.

## Link-Local Unicast-адреса:

- ❖ предназначены для взаимодействия внутри сегмента сети или по каналу связи «точка-точка»;
- ❖ используются только в пределах канала связи;
- ❖ маршрутизаторы не передают Link-Local Unicast-пакеты через другие каналы связи;
- ❖ автоматически назначаются узлы независимо от наличия в сети маршрутизатора или DHCPv6-сервера;
- ❖ начинаются с префикса FE80::/10.

❑ Общий формат Link-Local Unicast IPv6-адреса следующий:



- **Subnet ID** – идентификатор подсети внутри сети (заполняется нулями);
- **Interface ID** – идентификатор интерфейса.

## Групповые IPv6-адреса:

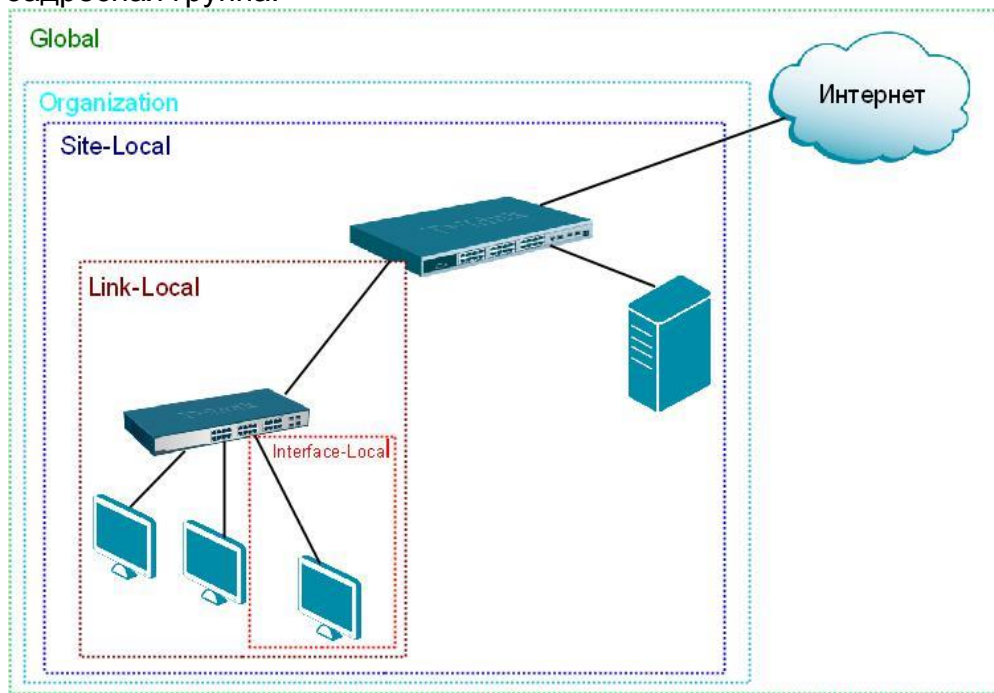
- ❖ идентифицируют группу интерфейсов, участвующую в получении одного и того же контента (например, видео);
- ❖ начинаются с префикса FF00::/8.

❑ Общий формат группового IPv6-адреса следующий:



## Групповые IPv6-адреса

- Поле **Scope** определяет область действия данного группового адреса, т. е. показывает, как далеко друг от друга могут находиться члены одной многоадресной группы.
- ❑ На данный момент определено шесть значений этого поля, остальные зарезервированы для будущих применений:
  - **Interface-Local** – многоадресная группа определена в рамках одного узла;
  - **Link-Local** – многоадресная группа определена в пределах канала связи;
  - **Admin-Local** – многоадресная группа определена внутри области, задаваемой администратором сети;
  - **Site-Local** – многоадресная группа определена в рамках локальной сети;
  - **Organization** – многоадресная группа определена в рамках распределенной сети;
  - **Global** – глобальная многоадресная группа.



## Групповые IPv6-адреса

- Функцию широковещательных адресов в протоколе IPv6 выполняют специальные групповые адреса, которые не назначаются многоадресным группам:
  - **FF01::1** – идентифицирует группу, включающую в себя все IPv6-узлы в пределах диапазона Interface-Local;
  - **FF02::1** – идентифицирует группу, включающую в себя все IPv6-узлы в пределах диапазона Link-Local;
  - **FF01::2** – идентифицирует группу всех IPv6-маршрутизаторов в пределах диапазона Interface-Local;
  - **FF02::2** – идентифицирует группу всех IPv6-маршрутизаторов в пределах диапазона Link-Local;
  - **FF05::2** – идентифицирует группу всех IPv6-маршрутизаторов в пределах диапазона Site-Local.

## Специальный групповой адрес Solicited-Node:

- ❖ используется в процессе разрешения IPv6-адресов для сегмента сети;
- ❖ присваивается каждому интерфейсу вместе с индивидуальными адресами;
- ❖ используется только на канале связи или в сегментах сети.

### ❑ Генерация адреса:

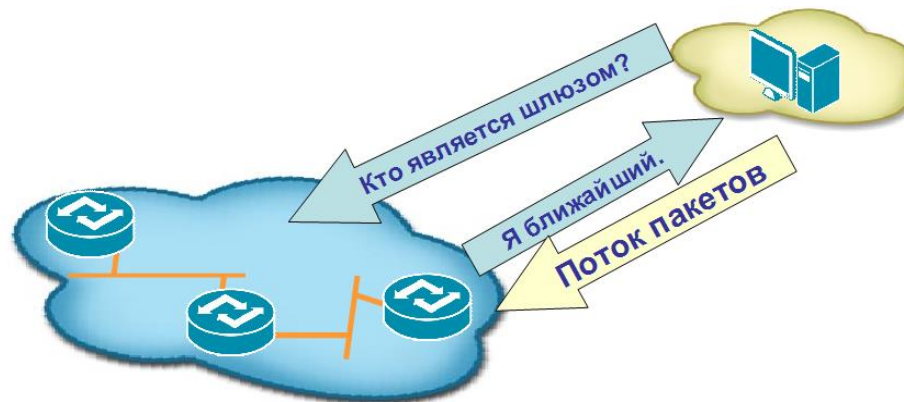
младшие 24 бита поля Interface ID индивидуального или альтернативного адреса  
+  
префикс FF02:0:0:0:0:1:FF00::/104

### Пример:

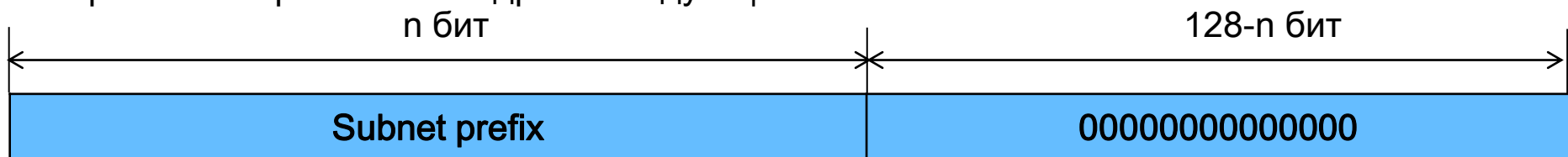
Адрес IPv6: FE80::0202:B3FF:FE1E:8329  
Префикс Solicited-Node: FF02:0000:0000:0000:0000:0001:FF00:0000  
Групповой адрес Solicited-Node: FF02:0000:0000:0000:0000:0001:FF1E:8329  
или  
FF02::1:FF1E:8329

## Альтернативные IPv6-адреса

- ❑ Альтернативный IPv6-адрес назначается нескольким интерфейсам. При этом пакет, отправленный на этот адрес, направляется на «ближайший» (имеющий минимальную метрику маршрутизации) интерфейс.



- ❑ Формат альтернативного адреса следующий:



### ❑ Альтернативный адрес:

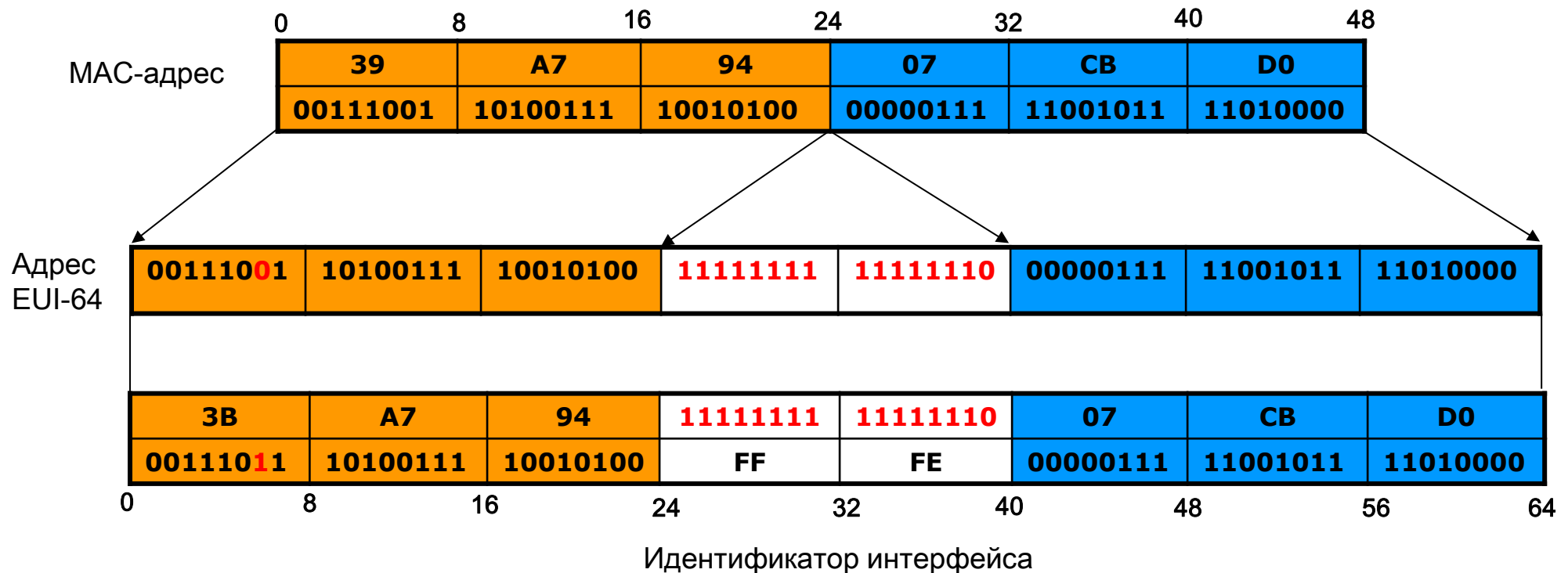
- входит в адресное пространство индивидуальных адресов;
- не может использоваться в качестве адреса отправителя пакета;
- назначается **только маршрутизаторам** и может применяться для идентификации группы маршрутизаторов, принадлежащих интернет-провайдеру.

## Идентификатор интерфейса

- ❑ Идентификатор интерфейса – 64-битное поле IPv6-адреса, используемое для идентификации интерфейса в сегменте сети.
  
- ❑ Уникальный идентификатор интерфейса может быть получен несколькими способами:
  - настроен вручную;
  - назначен с помощью протокола DHCPv6;
  - сгенерирован автоматически случайным образом;
  - сформирован из 48-битного MAC-адреса путем его преобразования в формат Modified EUI-64.

## Формирование идентификатора интерфейса из MAC-адреса

- ❑ MAC-адрес состоит из 48-бит, для идентификатора необходимо 64 бита, поэтому требуется расширение MAC-адреса преобразованием его в адрес EUI-64:
  1. MAC-адрес делится на две части по 24 бита;
  2. Между ними вставляется блок битов FFEF;
  3. Бит «universal/local» (7 бит слева) изменяется с 0 на 1 (бит, определяющий является ли MAC-адрес универсальным или локально администрируемым).



## Генерация псевдослучайного идентификатора интерфейса

- ❑ Когда идентификатор формируется из MAC-адреса, существует возможность идентификации и отслеживания трафика конкретного узла.
- ❑ Для обеспечения определенного уровня анонимности в RFC 3041 описан метод генерации узлом псевдослучайного идентификатора интерфейса, изменяемого с течением времени.
- ❑ Итоговый IPv6-адрес, основанный на таком псевдослучайном идентификаторе интерфейса, называют *временным адресом*, который рекомендуется для использования в интернете.

## Способы настройки IPv6-адреса

- ☐ Автоматическая конфигурация:
  - Stateless autoconfiguration;
  - Stateful autoconfiguration;
- ☐ Статическая конфигурация.

## Автоматическая конфигурация IPv6-адреса

- ❑ В отличие от протокола IPv4, где настройка параметров узла проводилась либо вручную, либо с помощью протокола DHCP, в протоколе IPv6 узел может практически самостоятельно сконфигурировать параметры своих интерфейсов.
  
- ❑ В протоколе IPv6 определены два механизма автоконфигурации:
  - **Stateless autoconfiguration:**
    - описан в RFC 4862;
    - позволяет узлам генерировать свой собственный адрес на основе комбинации доступной информации, объявляемой маршрутизаторами. Маршрутизаторы объявляют префиксы, идентифицирующие подсеть (или подсети), а узлы самостоятельно генерируют идентификаторы интерфейсов. При отсутствии маршрутизаторов узлы могут автоматически генерировать Link-Local Unicast IPv6-адрес.
  
  - **Stateful autoconfiguration:**
    - описан в RFC 3315;
    - позволяет узлам получать адрес интерфейса и/или конфигурационные параметры с помощью протокола DHCPv6.
  
- ❑ Механизмы автоконфигурации stateless и stateful могут дополнять друг друга и использоваться совместно.

## Stateless autoconfiguration

- ❑ Рассмотрим последовательность действий, которые выполняются в процессе автоконфигурации узла:

**Шаг 1. Генерация Link-Local Unicast-адреса** с префиксом FE80::/10;

**Шаг 2. Тестирование адреса на уникальность.** Узел проверяет используется ли уже такой адрес а локальном сегменте. Для этого он отправляет сообщение *Neighbor Solicitation* протокола Neighbor Discovery Protocol (NDP). Если в ответ на него получено сообщение *Neighbor Advertisement*, значит этот адрес уже используется другим узлом. В этом случае процесс автоконфигурации завершается и требуется ручная настройка;

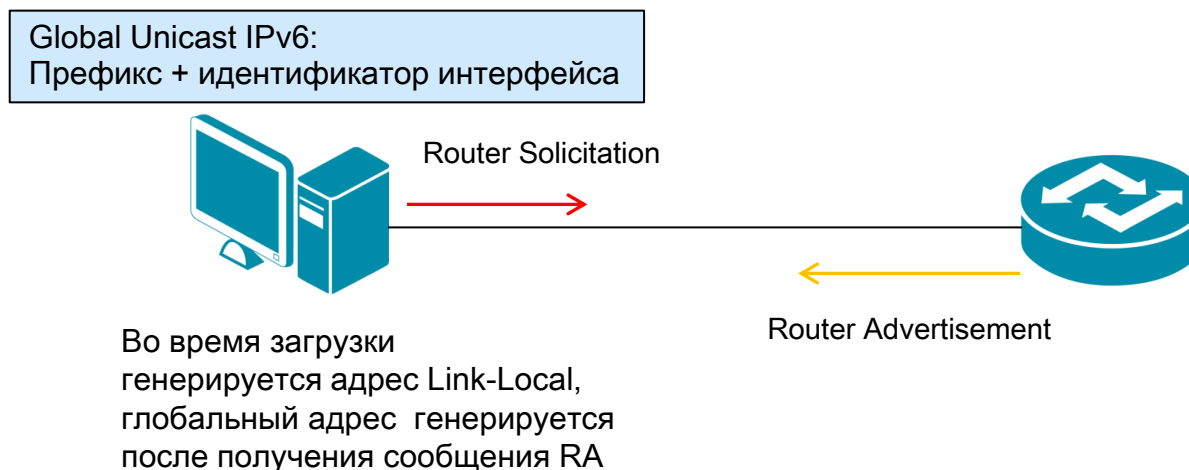
**Шаг 3. Присвоение адреса Link-Local Unicast.** Если тест на уникальность пройден успешно, узел присваивает сгенерированный на шаге 1 IPv6-адрес;

**Шаг 4. Обнаружение маршрутизатора.** После присвоения интерфейсу Link-Local-адреса узел отправляет сообщение *Router Solicitation* (RS) протокола NDP. Если в сети имеются маршрутизаторы, они отвечают сообщением *Router Advertisement* (RA) и сообщают узлам, каким образом продолжать процесс автоконфигурации;

## Stateless autoconfiguration

### Шаг 5. Генерация Global Unicast-адреса.

- В случае *Stateless autoconfiguration* Global Unicast-адреса состоит из префикса, предоставленного маршрутизатором и идентификатора интерфейса, созданного на шаге 1.

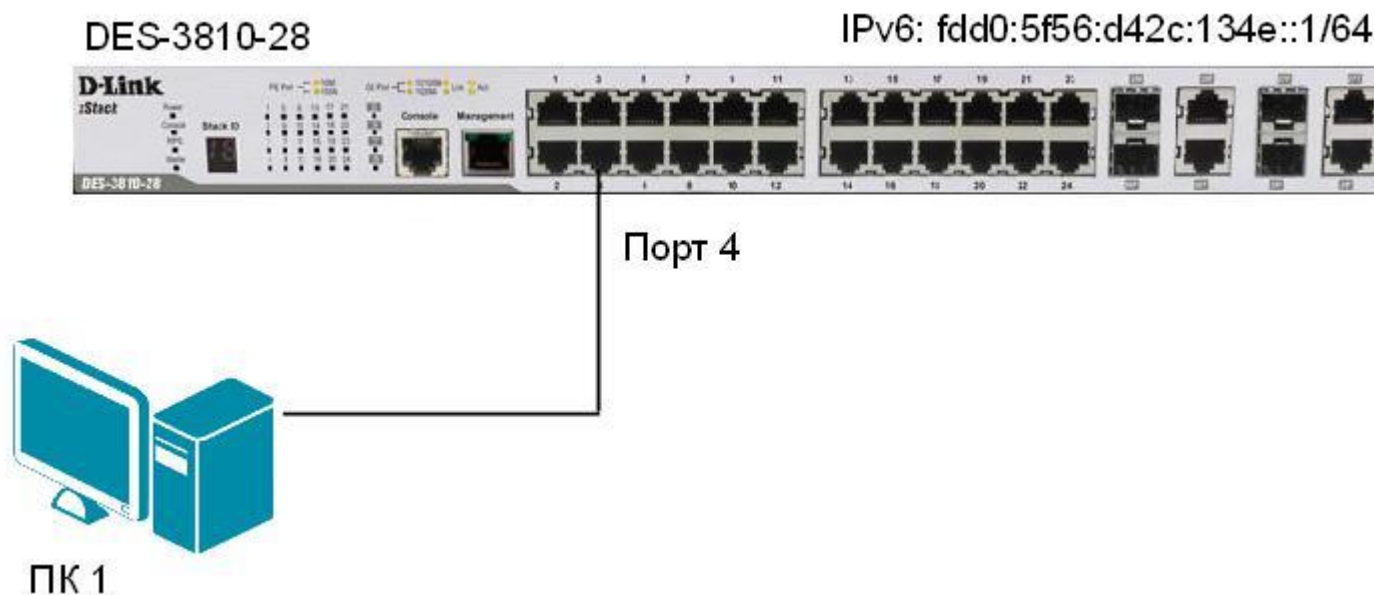


- В случае *Stateful autoconfiguration* узел отправляет запрос к DHCPv6-серверу об аренде IPv6-адреса/длины префикса и других сетевых параметров. Главное отличие протокола DHCPv6 от DHCPv4 заключается в том, что DHCPv6-сервер не рассылает DHCPv6-клиентам информацию о шлюзе по умолчанию.

## Настройка Stateless autoconfiguration

### Пример:

- ❑ Рассмотрим пример реализации автоматической настройки (Stateless autoconfiguration) Unique-Local Unicast-адресов узлов локальной сети с помощью коммутатора 3-го уровня DES-3810-28.
- ❑ Коммутатор отправляет узлам локальной сети информацию о префиксе после получения от них сообщения RS. Узлы автоматически формируют свои Unique-Local Unicast-адреса на основе данных, полученных от коммутатора.



## Настройка коммутатора DES-3810-28

- Настроить Unique-Local Unicast-адрес на интерфейсе System:

```
config ipif System ipv6 ipv6address fdd0:5f56:d42c:134e::1/64
```

- Активизировать автоматическую конфигурацию адреса на интерфейсе System:

```
config ipif nd ra ipif System state enable
```

- В качестве префикса, рассылаемого узлам, будет использоваться префикс адреса интерфейса System (в данном случае fdd0:5f56:d42c:134e::1/64)

## Статическая конфигурация IPv6-адреса

- ❑ В протоколе IPv6, так же как и в протоколе IPv4, существует возможность ручной настройки на интерфейсе IPv6-адреса, шлюза по умолчанию, длины префикса.



- ❑ Ручная настройка обычно используется для конфигурации интерфейсов маршрутизаторов или других сетевых устройств.
- ❑ Ручная настройка для конфигурации интерфейсов узлов может использоваться:
  - если в сети нет маршрутизаторов, которые рассылают объявления с информацией, требуемой для автоматической конфигурации;
  - в случае обнаружения дублирования адресов при автоматической конфигурации узлов.

## Планирование подсетей IPv6

### Задача:

- Организация планирует использовать в своей сети Unique-Local Unicast-адреса и хочет разбить сеть на 5 подсетей.

### Решение:

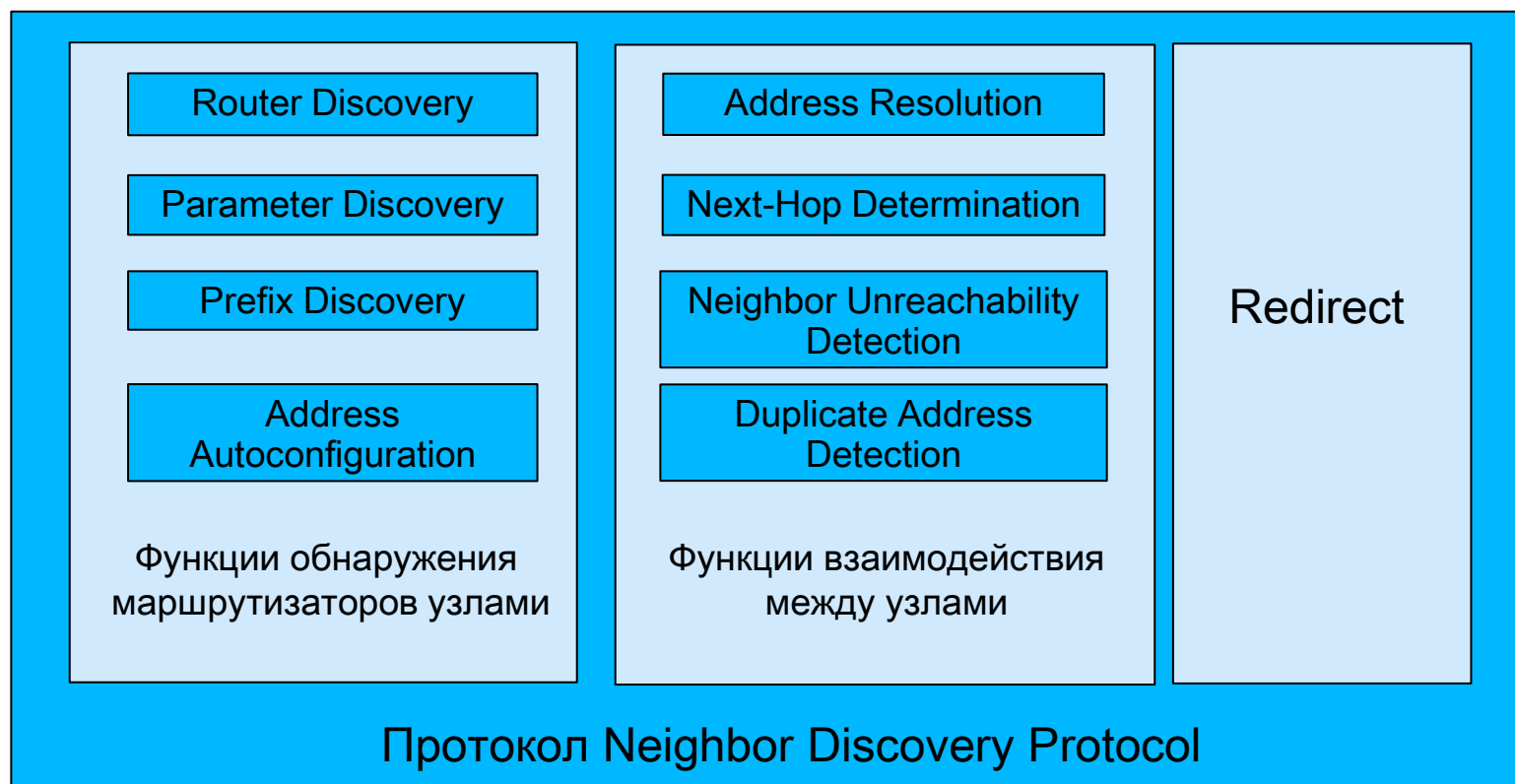
- Формируется префикс сети. Unique-Local Unicast-адреса начинаются с префикса FD00::/8;
- С помощью генератора локальных адресов IPv6 получаем Global ID (40 бит), например 895a473947.
- Назначаем 5 номеров подсети (Subnet ID) разрядностью 16 бит. Можно также воспользоваться генератором для получения номера подсети.

| Номер подсети | Префикс сети             | Диапазон адресов                                                       |
|---------------|--------------------------|------------------------------------------------------------------------|
| 0710          | fd89:5a47:3947:0710::/64 | fd89:5a47:3947:710:0:0:0:0 –<br>fd89:5a47:3947:710:ffff:ffff:ffff:ffff |
| 0711          | fd89:5a47:3947:0711::/64 | fd89:5a47:3947:711:0:0:0:0 –<br>fd89:5a47:3947:711:ffff:ffff:ffff:ffff |
| 0712          | fd89:5a47:3947:0712::/64 | fd89:5a47:3947:712:0:0:0:0 –<br>fd89:5a47:3947:712:ffff:ffff:ffff:ffff |
| 0713          | fd89:5a47:3947:0713::/64 | fd89:5a47:3947:713:0:0:0:0 –<br>fd89:5a47:3947:713:ffff:ffff:ffff:ffff |
| 0714          | fd89:5a47:3947:0714::/64 | fd89:5a47:3947:714:0:0:0:0 –<br>fd89:5a47:3947:714:ffff:ffff:ffff:ffff |

Идентификаторы в каждой подсети могут быть сформированы динамически одним из описанных ранее способов или вручную.

## Протокол Neighbor Discovery Protocol (NDP)

- ❑ Протокол Neighbor Discovery Protocol (NDP) – протокол стека TCP/IPv6. Определен в RFC 4861.
- ❑ Протоколом NDP реализованы ряд функций, относящихся к взаимодействию устройств локальной сети и функция разрешения адресов.
- ❑ В RFC 4861 определены девять функций, выполняемых протоколом NDP:



## Функции обнаружения маршрутизаторов узлами:

- **Router Discovery** – позволяет узлам локальной сети обнаруживать маршрутизаторы и получать от них сетевые параметры, необходимые для автоконфигурации;
- **Parameter Discovery** – позволяет узлам получать параметры локальной сети и/или маршрутизаторов, например MTU локального канала связи;
- **Prefix Discovery** – используется для определения префикса сети;
- **Address Autoconfiguration** – необходима для автоконфигурации узлов и взаимодействия между ними.

## Функции взаимодействия между узлами:

- **Address Resolution** – функция разрешения IPv6-адресов в адресе канального уровня;
- **Next-Hop Determination** – позволяет определить IPv6-адрес назначения пакета и его путь до следующего маршрутизатора;
- **Neighbor Unreachability Detection** – позволяет отслеживать состояние каналов связи между соседними узлами локальной сети;
- **Duplicate Address Detection** – позволяет определить дублирование адресов узлов локальной сети.
- **Redirect** – используется маршрутизаторами для уведомления узлов о наилучшем маршруте к пункту назначения.

## Протокол Neighbor Discovery Protocol (NDP)

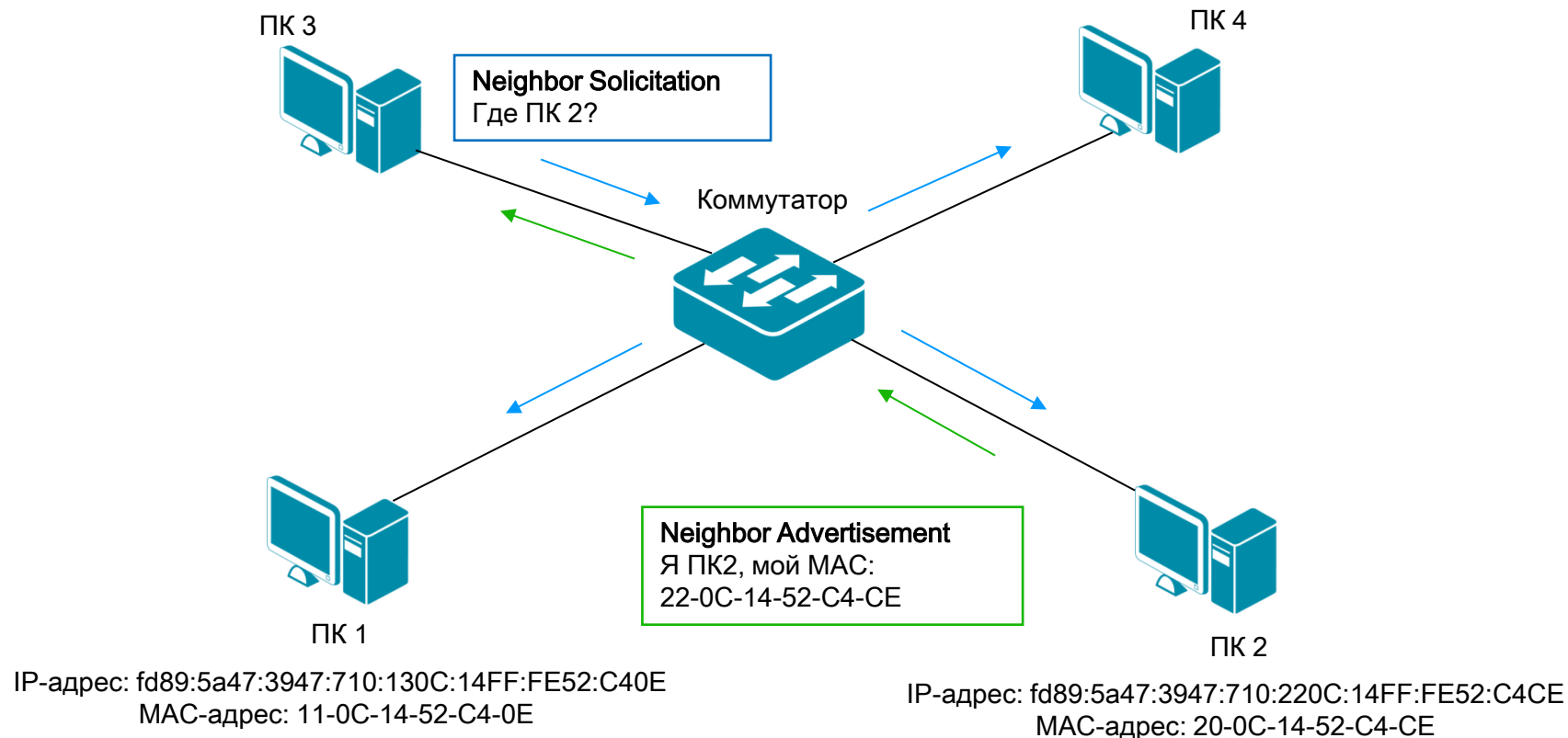
- ❑ Большинство функций протокола NDP выполняется с использованием пяти сообщений протокола ICMPv6:
  - **Router Solicitation** – отправляется узлами для того, чтобы запросить любой локальный маршрутизатор отправить сообщение Router Advertisement, не дожидаясь момента следующего периодического объявления. Используется при автоконфигурации узла;
  - **Router Advertisement** – регулярно отправляются маршрутизаторами для того, чтобы объявить о своем существовании в сети и предоставить узлам информацию о префиксе и/или дополнительных параметрах. Это сообщение также может быть отправлено в ответ на сообщение Router Solicitation;
  - **Neighbor Solicitation** - отправляется узлом для того, чтобы определить адрес канального уровня соседнего устройства или проверить доступность соседа с помощью адреса канального уровня, хранимый в NDP-таблице. Также используется для определения дублирования адресов (Duplicate Address Detection);
  - **Neighbor Advertisement** - отправляется в ответ на сообщение Neighbor Solicitation. Это сообщение может быть отправлено узлом при изменении адреса канального уровня.
  - **Redirect** - используется маршрутизаторами для уведомления узлов о наилучшем маршруте к пункту назначения.

## Разрешение IPv6-адресов с помощью протокола NDP

- Для выполнения функции разрешения адресов в протоколе NDP используется два сообщения ICMPv6:
  - **Neighbor Solicitation (NS)** – для того чтобы узнать адрес канального уровня, узел отправляет сообщение на групповой адрес Solicited-Node.
  - **Neighbor Advertisement (NA)** – ответ на сообщение Neighbor Solicitation, в котором содержится адрес канального уровня.

ПК 3  
IP-адрес: fd89:5a47:3947:710:330C:14FF:FE52:C4CE  
MAC-адрес: 31-0C-14-52-C4-CE

ПК 4  
IP-адрес: fd89:5a47:3947:710:4A0C:14FF:FE52:C4CE  
MAC-адрес: 44-0C-14-52-C4-CE

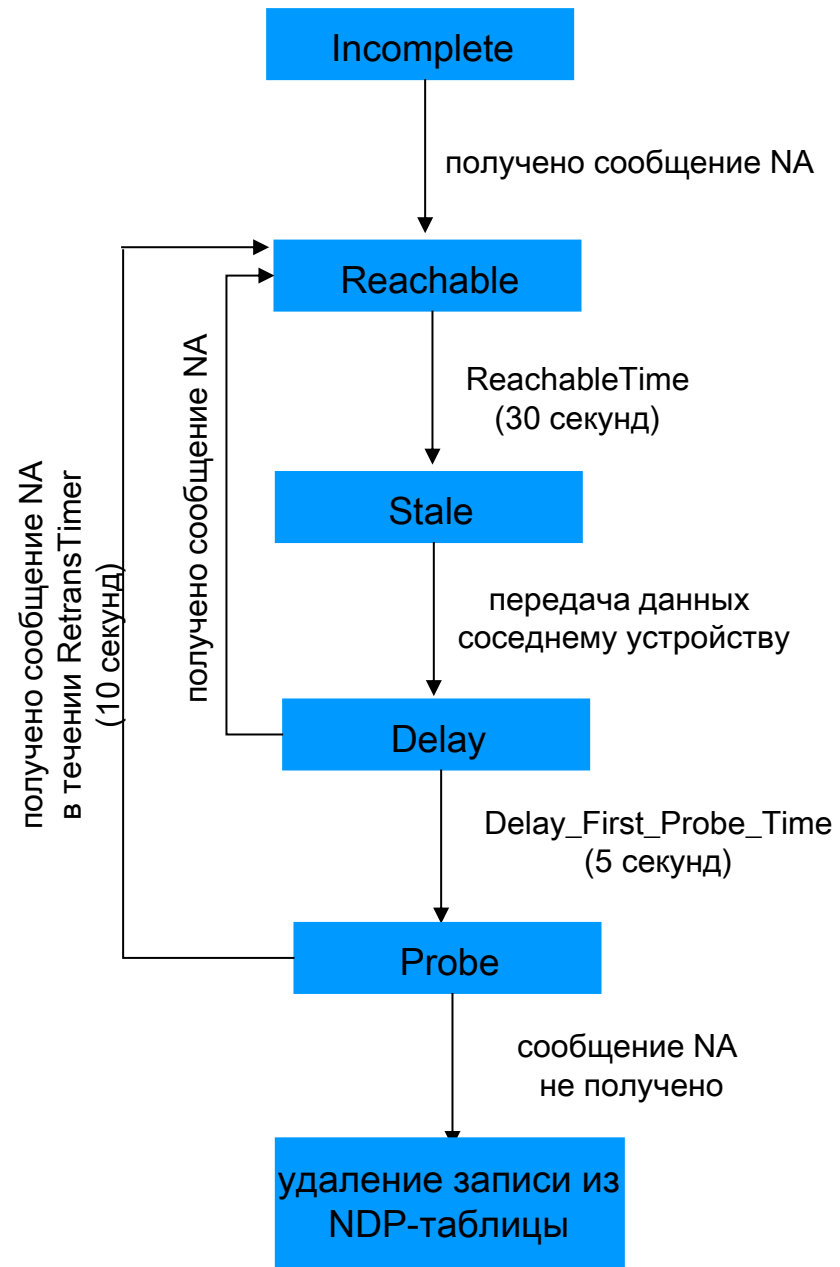


## Разрешение IPv6-адресов с помощью протокола NDP

- ❑ На основании полученного сообщения Neighbor Advertisement устройство добавляет в NDP-таблицу (neighbor cache) новую запись, связывающую IPv6-адрес с соответствующим MAC-адресом соседнего устройства, от которого это сообщение получено.
- ❑ Так же, как и в ARP-таблице, в NDP-таблице могут храниться и *статические*, и *динамические* записи.

❑ Динамическая запись в NDP-таблице может находиться в одном из пяти состояний:

- **Incomplete** – состояние, когда сообщение Neighbor Solicitation отправлено на групповой адрес Solicited-Node, но ответное сообщение Neighbor Advertisement еще не получено;
- **Reachable** – состояние, когда сообщение Neighbor Advertisement получено. Продолжительность этого состояния записи в NDP-таблице ограничено таймером ReachableTime (по умолчанию 30 секунд);
- **Stale** – состояние, в которое переходит запись по истечении времени таймера ReachableTime с момента последнего получения сообщения Neighbor Advertisement;
- **Delay** – состояние, в которое переходит запись при передаче данных соседнему устройству. При этом устанавливается таймер Delay\_First\_Probe\_Time (по умолчанию 5 секунд). Если по истечении времени таймера запись все еще остается в состоянии Delay, статус записи меняется на Probe. Если же подтверждение достижимости было получено, состояние записи меняется на Reachable.
- **Probe** – состояние записи, при котором устройство отправляет сообщение Neighbor Solicitation через промежутки времени, определяемые таймером RetransTimer (по умолчанию 10 секунд). Если в течение трех последовательных передач сообщения Neighbor Solicitation получено сообщение Neighbor Advertisement, то запись переходит в состояние Reachable, в противном случае запись удаляется из NDP-таблицы.



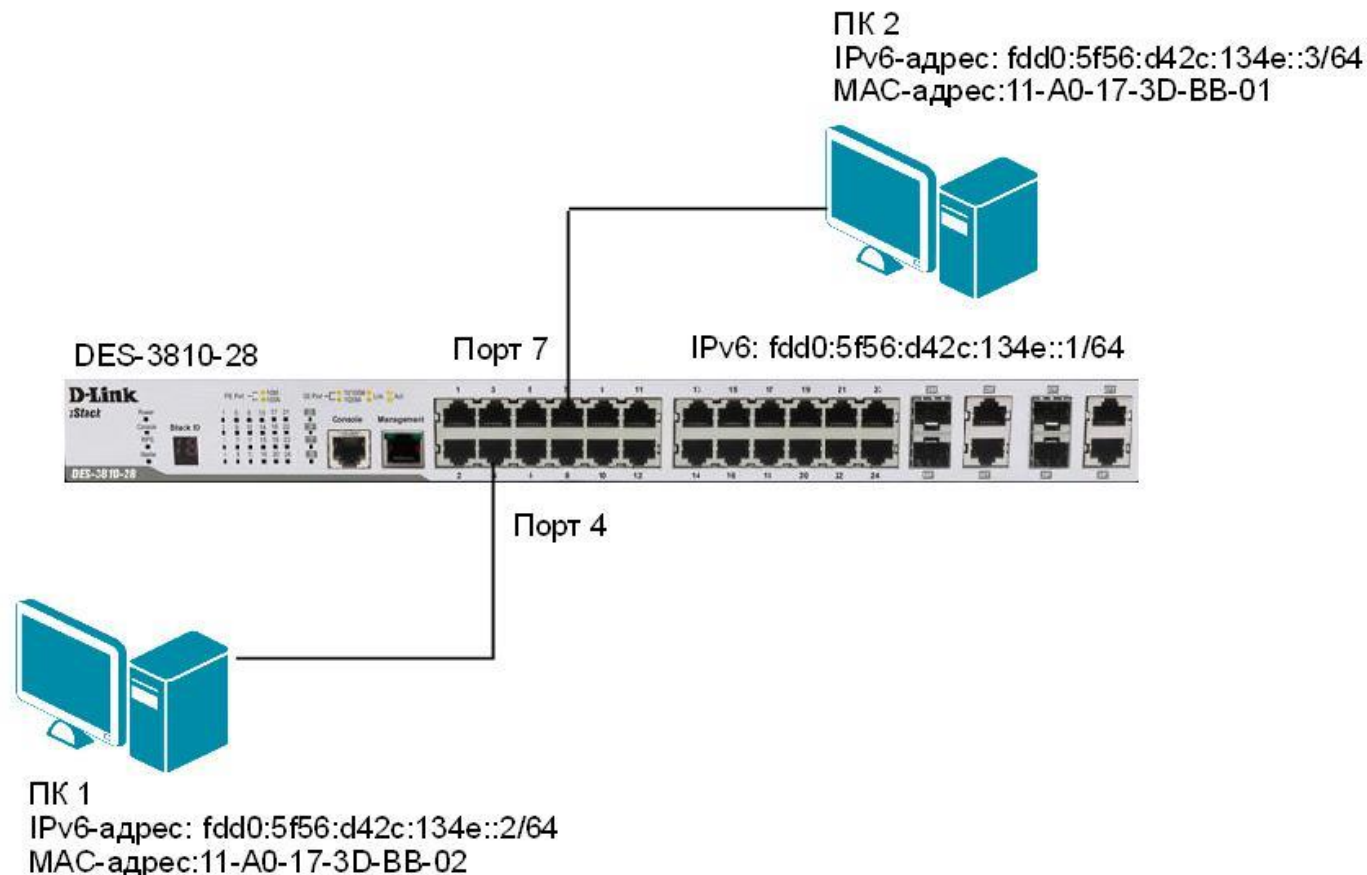
## Определение недоступности соседа (Neighbor Unreachability Detection, NUD)

- ❑ Функция NUD позволяет отслеживать состояние каналов связи между соседними узлами локальной сети.
- ❑ Функция NUD использует сообщения Neighbor Solicitation и Neighbor Advertisement.
- ❑ Операции функции NUD выполняются параллельно с отправкой пакетов соседним устройствам, и если между ними нет обмена данными, то сообщения Neighbor Solicitation и Neighbor Advertisement не отправляются.

## Настройка разрешения IPv6-адресов с помощью протокола NDP

### Пример:

- ❑ Рассмотрим пример формирования NDP-таблицы (neighbor cache) на коммутаторе 3-го уровня DES-3810-28.



## Настройка коммутатора DES-3810-28

- Создать статическую запись для ПК1 в NDP-таблице:

```
create ipv6 neighbor_cache ipif System fdd0:5f56:d42c:134e::2  
11:A0:17:3D:BB:02
```

- Настроить время периодической отправки сообщений Neighbor Solicitation с интерфейса System для создания динамических записей в NDP-таблице:

```
config ipv6 nd ns ipif System retrans_time 400
```

- Посмотреть информацию о соседних устройствах, подключенных к интерфейсу System (NDP-таблицу):

```
show ipv6 neighbor_cache ipif System all
```

## Определение дублирования адресов (Duplicate Address Detection, DAD)

- ❑ При использовании механизма автоконфигурации IPv6-адреса необходимо определить, что адрес Link-Local, который сегментирован узлом, уже не используется другим узлом, т. е. проверить *дублирование адресов* (Duplicate Address Detection, DAD).
- ❑ Для этого в сеть отправляется сообщение Neighbor Solicitation, если в ответ на него получено сообщение Neighbor Advertisement, это означает, что данный адрес уже используется другим узлом.
- ❑ В этом случае процесс автоконфигурации завершается и требуется ручная настройка интерфейса.

## Обнаружение маршрутизатора (Router Discovery)

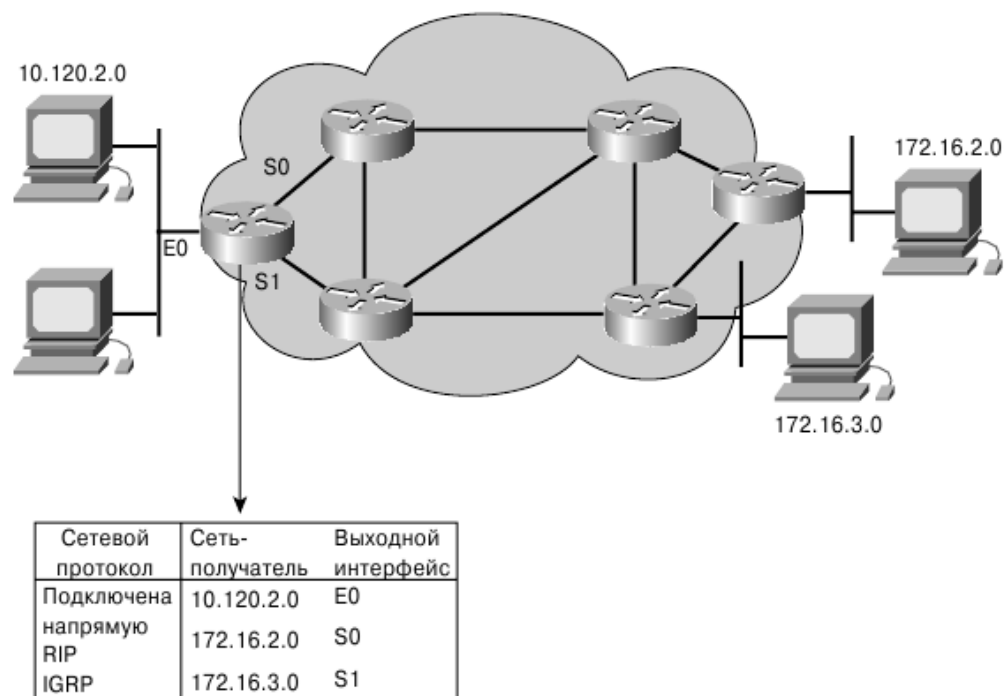
- ❑ Одной из важных функций протокола NDP является реализация процесса обнаружения узлами локальных маршрутизаторов – *Router Discovery*. При этом узлы локальной сети обнаруживают соседние маршрутизаторы и получают от них сетевые параметры, необходимые для автоконфигурации.
- ❑ Операция обнаружения узлами маршрутизаторов выполняется с помощью сообщений ICMPv6 *Router Advertisement* и *Router Solicitation*.
- ❑ В процессе обнаружения маршрутизаторов (коммутаторов 3-го уровня) узлы выполняют следующие функции:
  - **Рассылка объявлений.** Узлы прослушивают объявления Router Advertisement, передаваемые маршрутизаторами (коммутаторами L3) в локальной сети через определенные интервалы времени и обрабатывают их. Объявления содержат список префиксов, в том числе необходимых для автоконфигурации, а также могут включать информацию о шлюзе по умолчанию;
  - **Генерация запросов.** При определенных условиях (например, узел загружается и ему требуются параметры для конфигурации интерфейса) узлы могут генерировать сообщения Router Solicitation. С помощью этого сообщения узел запрашивает любой локальный маршрутизатор о мгновенном предоставлении информации, т.е. отправке сообщения Router Advertisement;
  - **Автоконфигурация.** Если в сети настроен механизм автоконфигурации Stateless autoconfiguration, то узел будет использовать информацию, полученную от локального маршрутизатора, чтобы автоматически сконфигурировать свой IPv6-адрес и другие сетевые параметры.

**Маршрутизация** представляет собой процесс, который используется маршрутизатором для пересылки пакета в сеть получателя. Маршрутизатор принимает решения, основываясь на IP-адресе получателя пакета. Для того чтобы переслать пакет в требуемом направлении, все устройства на пути его следования используют IP-адрес получателя, что позволяет пакету достичь требуемого пункта назначения. Для принятия правильного решения маршрутизаторы должны знать направления к удаленным сетям, которые могут задаваться в ручную(статически) или динамически, когда направление к удаленным сетям маршрутизатор узнает от других маршрутизаторов сети.

**Маршрутизируемый (routed protocol)**, или сетевой, протокол — это любой сетевой протокол, предоставляющий в своем адресе сетевого уровня достаточно информации для пересылки пакета от одного узла другому на основе используемой схемы адресации

**Маршрутизирующий протокол (routing protocol)** — это протокол, который обеспечивает работу маршрутизируемого протокола, предоставляя механизмы совместного использования информации о маршрутах.

Процесс нахождения оптимального пути, по которому следует передать пакет, выполняется на третьем уровне эталонной модели OSI (сетевом). Эта процедура позволяет маршрутизатору оценить существующие маршруты к получателю и выбрать среди них наиболее предпочтительный.



Процесс поиска маршрута для пакета можно сравнить с поездкой из одной части города в другую. У водителя есть карта, где указаны улицы, выбирая которые, он движется к пункту назначения. Отрезок от одного перекрестка до другого аналогичен прохождению пакетом расстояния между двумя маршрутизаторами, который обычно называют **транзитным переходом**.

Чтобы найти маршрут, по которому следует передавать данные, протоколы маршрутизации создают и поддерживают таблицы маршрутизации. Информация о маршруте может отличаться в зависимости от используемого протокола маршрутизации.

Маршрутизаторы хранят и обновляют следующую важную информацию в таблицах маршрутизации:

**Тип протокола** - информацию о протоколе маршрутизации, создавшем запись в таблице маршрутизации;

**Связка получатель/следующий узел** - сообщает маршрутизатору о том, что определенный получатель либо подключен непосредственно, либо может быть достигнут через другой маршрутизатор, называемый следующим транзитным узлом (next hop), находящийся на пути к пункту назначения. Маршрутизатор анализирует адрес получателя во входящих пакетах и сравнивает его на соответствие с записями в таблице маршрутизации;

**Метрики маршрутизации.** Различные протоколы маршрутизации используют разные метрики, которые помогают определить предпочтительность маршрута.

**Выходной интерфейс** - интерфейс, через который должны быть отправлены данные, чтобы достичь пункта назначения.

- **Оптимальность** описывает способности протокола и алгоритма по выбору наиболее оптимального маршрута на основании метрик и их весовых значений, используемых при расчетах.
- **Простота и низкие накладные расходы.** Идеальная эффективность работы алгоритма маршрутизации может быть достигнута, когда загрузка процессора и памяти маршрутизатора минимальны. Эта характеристика важна для масштабируемости сети, которая в предельном случае может быть расширена до размеров сети Internet.
- **Устойчивость и надежность.** Алгоритм маршрутизации должен корректно функционировать даже при наличии нестандартных и непредвиденных обстоятельств, таких, как сбой оборудования, высокая загрузка и ошибки эксплуатации.
- **Быстрая конвергенция.** Конвергенцией называется процесс установления договоренности между всеми маршрутизаторами об имеющихся маршрутах.
- **Гибкость.** Алгоритм и протокол маршрутизации должны быстро адаптироваться к разнообразным изменениям в сети. Изменениями в сети считаются изменения в состоянии устройств, в частности, маршрутизаторов, изменение пропускной способности каналов, изменение размера очередей или сетевой задержки.
- **Масштабируемость.** Некоторые протоколы разработаны таким образом, что могут быть масштабируемы лучше других.

**Ширина полосы пропускания** представляет собой средство оценки объема информации, который может быть передан по каналу связи (канал Ethernet со скоростью 10 Мбит/с более предпочтителен, чем выделенная линия со скоростью 64 Кбит/с).

**Задержка** — промежуток времени, необходимый для перемещения пакета по каждому из каналов связи от отправителя получателю. Задержка зависит от пропускной способности промежуточных каналов, размера очередей в портах маршрутизаторов, загрузки сети и физического расстояния.

**Загрузка** — объем операций, выполняемых сетевым устройством, таким, как маршрутизатор, или средняя загруженность канала связи.

**Надежность** обычно обозначает относительное значение количества ошибок для каждого из каналов связи.

**Счетчик транзитных узлов** — количество маршрутизаторов, через которые должен пройти пакет, прежде чем достигнет пункта назначения. Если существует несколько путей, маршрутизатор выбирает тот, для которого значение счетчика узлов наименьшее.

**Стоимость** — значение, обычно вычисляемое на основе пропускной способности, денежной стоимости или других единиц измерения, назначаемых администратором.

## Маршрутизация

- ❑ *Маршрутизация* является одним из процессов, который выполняется на сетевом уровне модели OSI, и позволяет объединять IP-сегменты в единую сеть.
- ❑ Маршрутизация выполняется *маршрутизаторами* или *коммутаторами 3-го уровня*, которые перенаправляют пакеты из одной IP-сети в другую, даже в том случае, если заранее неизвестно расположение получателя пакета.
- ❑ *Таблица маршрутизации* хранится на маршрутизаторе и содержит записи, представляющие собой список наилучших маршрутов в соответствующие сети.



## Таблица маршрутизации

❑ Существует четыре типа записей в таблицы маршрутизации:

- Статический маршрут (*Static Route*);
- Динамический маршрут (*Dynamic Route*);
- Маршрут по умолчанию (*Default Route*);
- Локальный маршрут (*Local Route*).

Routing Table

| IP Address/Netmask | Gateway    | Interface | Cost | Protocol |
|--------------------|------------|-----------|------|----------|
| 10.0.0.0/8         | 0.0.0.0    | System    | 1    | Local    |
| 172.16.0.0/23      | 172.16.8.2 | iptv-1    | 2    | RIP      |
| 172.16.2.0/23      | 172.16.8.2 | iptv-1    | 2    | RIP      |
| 172.16.8.0/30      | 0.0.0.0    | iptv-1    | 1    | Local    |
| 172.16.8.4/30      | 0.0.0.0    | iptv-2    | 1    | Local    |
| 172.16.8.8/30      | 172.16.8.6 | iptv-2    | 2    | RIP      |
| 172.16.8.12/30     | 0.0.0.0    | stream    | 1    | Local    |

Total Entries: 7

## Таблица маршрутизации

- Каждая запись таблицы маршрутизации содержит следующую информацию:
- **адрес назначения (IP Address)** — адрес сети (в некоторых случаях узла) назначения;
  - **маска сети (Netmask)** — маска, соответствующая адресу назначения (для сетей IPv4 маска /32 (255.255.255.255) позволяет указать единичный узел сети);
  - **адрес шлюза (Gateway)** — сообщает маршрутизатору о том, что получатель пакета подключен непосредственно или доступен через другой маршрутизатор (коммутатор L3), который называется следующим транзитным узлом (next hop);
  - **интерфейс (Interface)** — идентификатор интерфейса, через который пакет покидает устройство;
  - **метрика (Cost)** — числовой показатель, определяющий предпочтительность маршрута. Чем меньше значение метрики, тем более предпочтителен маршрут;
  - **тип протокола (Protocol)** – информация о методе создания записи в таблице маршрутизации.

Routing Table

| IP Address/Netmask | Gateway    | Interface | Cost | Protocol |
|--------------------|------------|-----------|------|----------|
| 10.0.0.0/8         | 0.0.0.0    | System    | 1    | Local    |
| 172.16.0.0/23      | 172.16.8.2 | iptv-1    | 2    | RIP      |
| 172.16.2.0/23      | 172.16.8.2 | iptv-1    | 2    | RIP      |
| 172.16.8.0/30      | 0.0.0.0    | iptv-1    | 1    | Local    |
| 172.16.8.4/30      | 0.0.0.0    | iptv-2    | 1    | Local    |
| 172.16.8.8/30      | 172.16.8.6 | iptv-2    | 2    | RIP      |
| 172.16.8.12/30     | 0.0.0.0    | stream    | 1    | Local    |

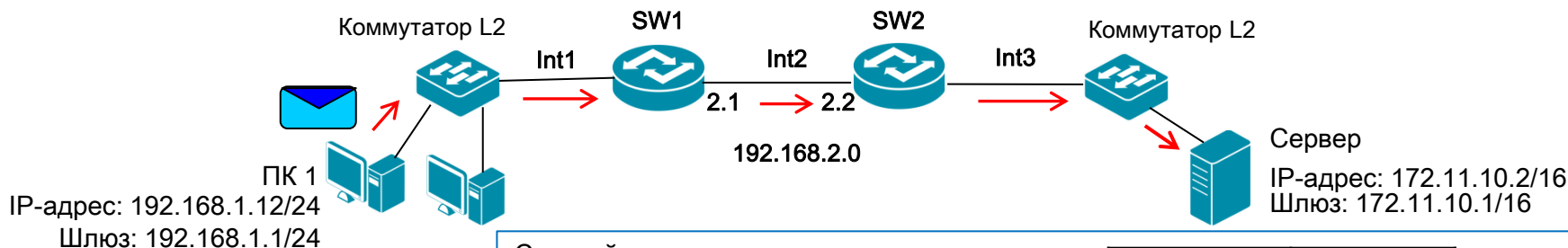
Total Entries: 7

## Процесс обработки пакета маршрутизирующим устройством

1. Маршрутизатор SW1 получает кадр на интерфейс Int1 и проверяет его целостность;
2. Если кадр не поврежден, SW1 удаляет его заголовок и концевик;
3. Извлекает из заголовка сетевого уровня IP-адрес назначения;
4. Сравнивает IP-адрес назначения с записями в таблице маршрутизации. Если соответствие найдено, данные передаются на нужный интерфейс, если нет – пакет отбрасывается и отправителю отправляется ICMP-сообщение «Destination Unreachable» (получатель недоступен).
5. Интерфейс Int2 маршрутизатора SW1 формирует новый кадр, инкапсулируя в него пакет;
6. Пересылает пакет маршрутизатору SW2, найденному в соответствии с таблицей маршрутизации.

| Routing Table (SW1) |             |           |      |
|---------------------|-------------|-----------|------|
| IP Address          | Gateway     | Interface | Cost |
| 192.168.1.0/24      | 0.0.0.0     | Int1      | 1    |
| 192.168.2.0/24      | 0.0.0.0     | Int1      | 1    |
| 172.11.0.0/16       | 192.168.2.2 | Int2      | 2    |

| Routing Table (SW2) |             |           |      |
|---------------------|-------------|-----------|------|
| IP Address          | Gateway     | Interface | Cost |
| 172.11.0.0/16       | 0.0.0.0     | Int3      | 1    |
| 192.168.2.0/24      | 0.0.0.0     | Int2      | 1    |
| 192.168.1.0/24      | 192.168.2.1 | Int2      | 2    |



Сетевой уровень

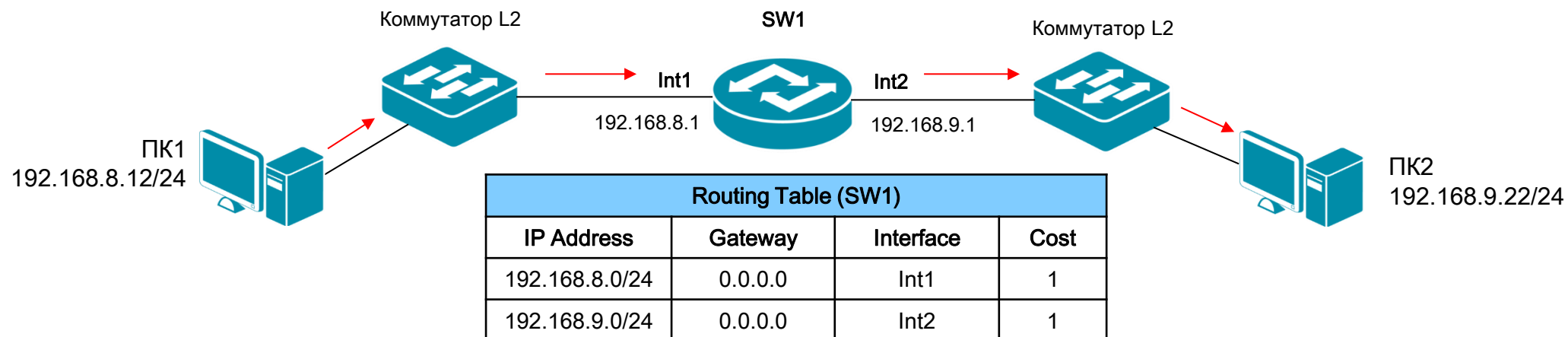
|              |             |
|--------------|-------------|
| 192.168.1.12 | 172.11.10.2 |
|--------------|-------------|

Канальный уровень

| DA     | SA       |              |             |  |
|--------|----------|--------------|-------------|--|
| Сервер | SW2.Int2 | 192.168.1.12 | 172.11.10.2 |  |

## Процесс поиска маршрута в таблице маршрутизации

- ❑ После того, как маршрутизатор извлек из заголовка пакета IP-адрес назначения, он сравнивает сетевую часть IP-адреса с записями в таблице маршрутизации и принимает решение о дальнейшем пути пакета.



IP-адрес назначения  
Первая запись в таблице маршрутизации

|              |          |          |                  |          |
|--------------|----------|----------|------------------|----------|
| 192.168.9.22 | 11000000 | 10101000 | 0000100 <b>1</b> | 00010110 |
| 192.168.8.0  | 11000000 | 10101000 | 0000100 <b>0</b> | 00000000 |

Нет совпадений

IP-адрес назначения  
Вторая запись в таблице маршрутизации

|              |          |          |                  |          |
|--------------|----------|----------|------------------|----------|
| 192.168.9.22 | 11000000 | 10101000 | 0000100 <b>1</b> | 00010110 |
| 192.168.9.0  | 11000000 | 10101000 | 0000100 <b>1</b> | 00000000 |

Есть совпадение

## Коммутация третьего уровня

- ❑ Коммутаторы 3-го уровня имеют некоторые особенности, отличающие их от традиционных маршрутизаторов 2-го уровня:
  - одновременная поддержка функций маршрутизации и коммутации;
  - обязательная поддержка VLAN;
  - реализация функций маршрутизации на аппаратном уровне с использованием ASIC.
  
- ❑ Благодаря использованию контроллеров ASIC коммутаторы 3-го уровня маршрутизируют пакеты в среднем в 10-100 раз быстрее, чем традиционные маршрутизаторы.

**Новые маршруты могут добавляться в таблицу маршрутизации с помощью:**

- **Статической маршрутизации:** записи о маршрутах в сети назначения добавляются и изменяются в таблицах маршрутизации вручную.
- **Динамической маршрутизации:** записи о маршрутах заносятся и обновляются в таблицах с помощью протоколов маршрутизации (routing protocols).

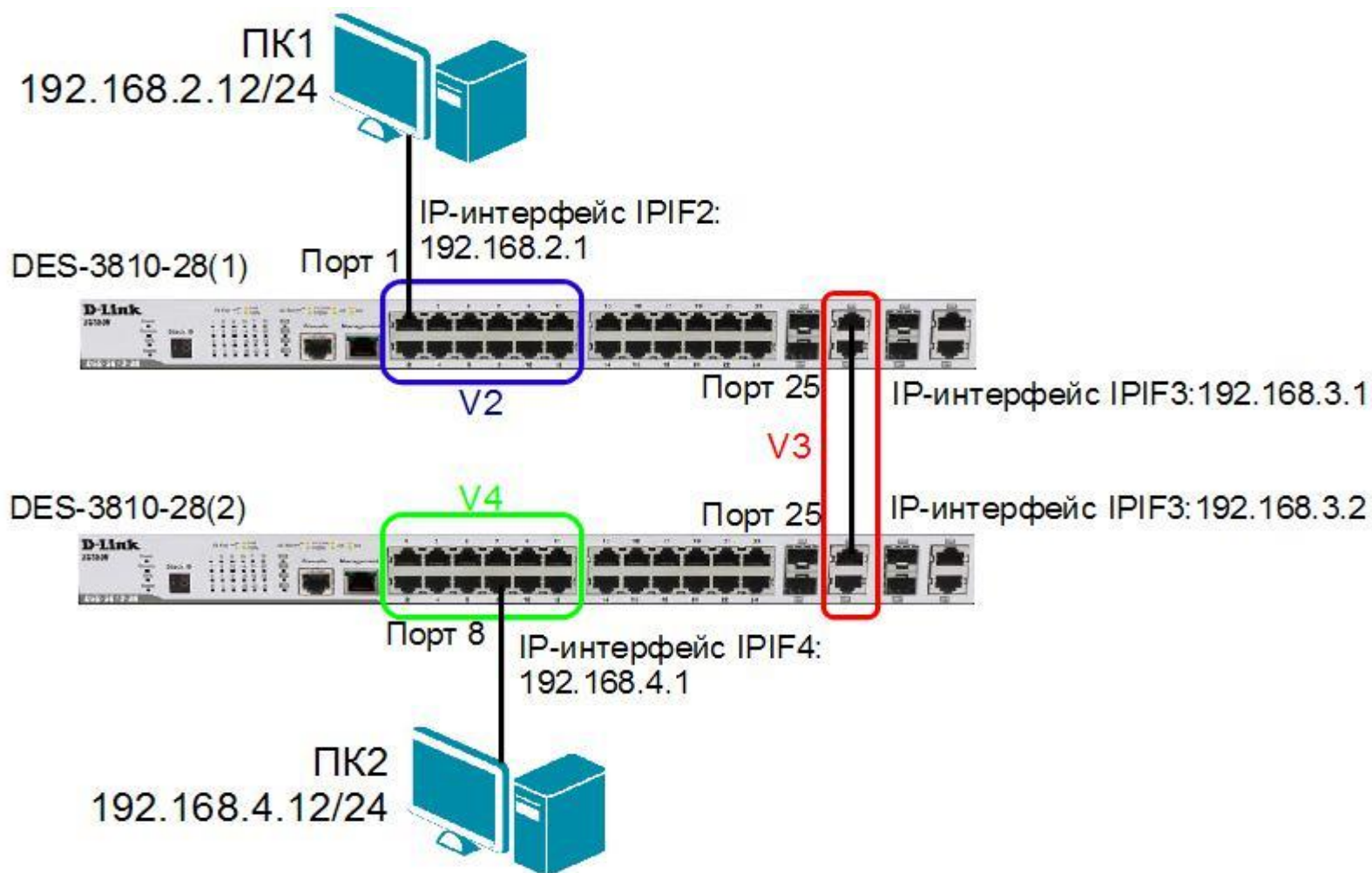
## Статическая и динамическая маршрутизация

- ❖ **Статическую маршрутизацию полезно использовать если:**
  - к сети назначения имеется небольшое количество маршрутов и администратор вручную может задать наилучший маршрут;
  - требуется скрыть маршрутную информацию.
  
- ❖ **Динамическая маршрутизация выполняет две важные функции:**
  - обслуживание таблиц маршрутизации;
  - обмен данными о маршрутах между маршрутизаторами в форме обновлений.

## Настройка статической IPv4-маршрутизации

### Пример:

- ❑ Рассмотрим пример настройки статической IPv4-маршрутизации. Сеть сегментирована с использованием VLAN. Требуется настроить маршрутизацию между VLAN v2 и v4 на коммутаторах D-Link DES-3810-28.



## Настройка коммутатора DES-3810-28 (1)

- Удалить порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

- Создать VLAN v2 и v3 и добавить в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v2 tag 2
```

```
config vlan v2 add untagged 1-12
```

```
create vlan v3 tag 3
```

```
config vlan v3 add untagged 25
```

- Создать IP-интерфейсы для VLAN v2 и v3 с именами IPIF2 и IPIF3 соответственно:

```
create ipif IPIF2 192.168.2.1/24 v2 state enable
```

```
create ipif IPIF3 192.168.3.1/24 v3 state enable
```

- Создать статический маршрут к сети 192.168.4.0/24:

```
create iproute 192.168.4.0/24 192.168.3.2
```

## Настройка коммутатора DES-3810-28 (2)

- Удалить порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

- Создать VLAN v4 и v3 и добавить в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan v4 tag 4
```

```
config vlan v4 add untagged 1-12
```

```
create vlan v3 tag 3
```

```
config vlan v3 add untagged 25
```

- Создать IP-интерфейсы для VLAN v4 и v3 с именами IPIF4 и IPIF3 соответственно:

```
create ipif IPIF4 192.168.4.1/24 v4 state enable
```

```
create ipif IPIF3 192.168.3.2/24 v3 state enable
```

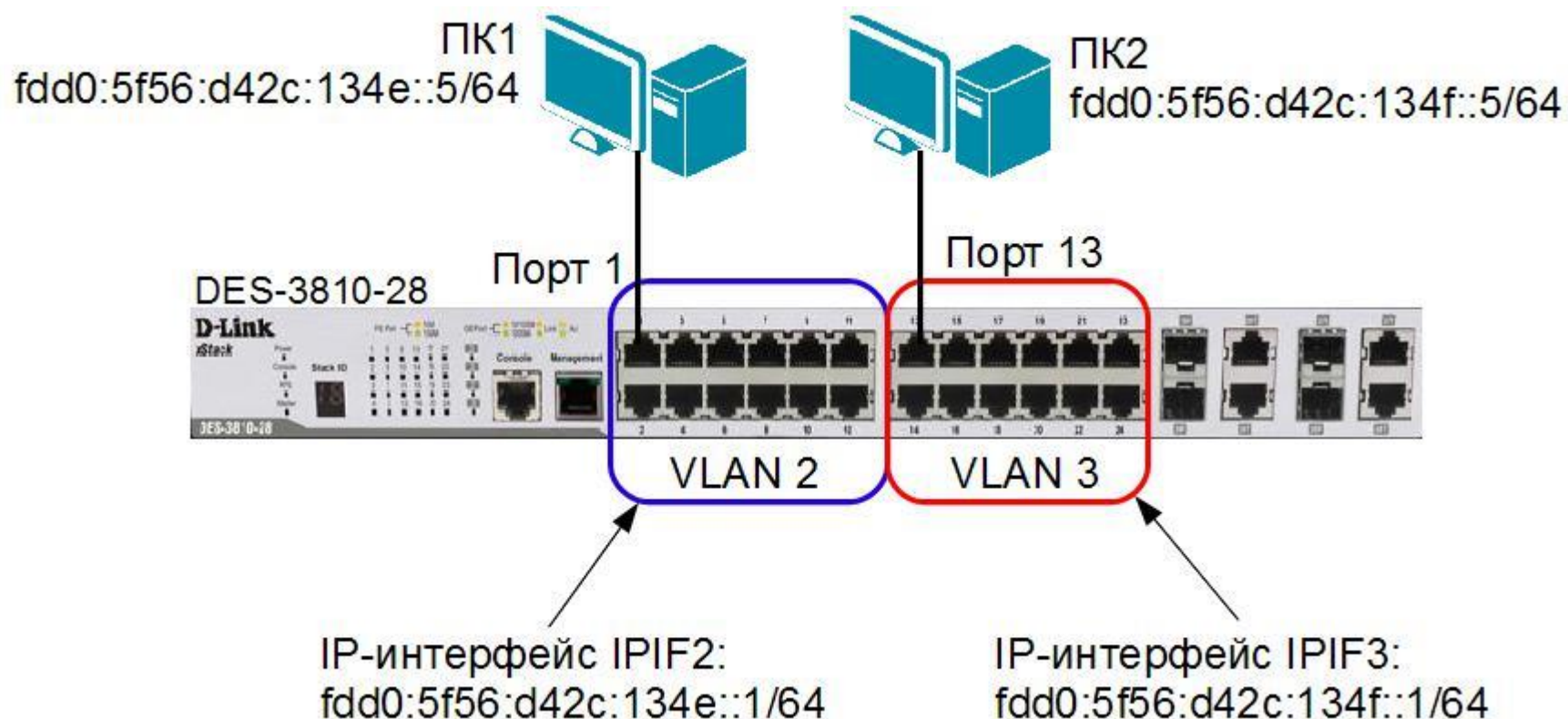
- Создать статический маршрут к сети 192.168.2.0/24:

```
create iproute 192.168.2.0/24 192.168.3.1
```

## Настройка статической IPv6-маршрутизации

### Пример:

- ❑ Рассмотрим пример настройки статической IPv6-маршрутизации между VLAN в пределах одного коммутатора D-Link DES-3810-28.



В пределах одного коммутатора 3-го уровня маршрутизация между VLAN включается автоматически при настройке IP-интерфейсов.

## Настройка коммутатора DES-3810-28

- Удалить порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

```
config vlan default delete 1-24
```

- Создать VLAN v2 и v3 и добавить в соответствующие VLAN порты, которые необходимо настроить немаркированными:

```
create vlan vlan2 tag 2
```

```
config vlan vlan2 add untagged 1-12
```

```
create vlan vlan3 tag 3
```

```
config vlan vlan3 add untagged 13-24
```

- Создать IP-интерфейсы для VLAN v2 и v3 с именами IPIF2 и IPIF3 соответственно:

```
create ipif IPIF2 vlan2 state enable
```

```
create ipif IPIF3 vlan3 state enable
```

- Настроить IPv6-адрес для интерфейсов IPIF2 и IPIF3:

```
config ipif IPIF2 ipv6 ipv6address fdd0:5f56:d42c:134e::1/64
```

```
config ipif IPIF3 ipv6 ipv6address fdd0:5f56:d42c:134f::1/64
```

**Спасибо за внимание!**

