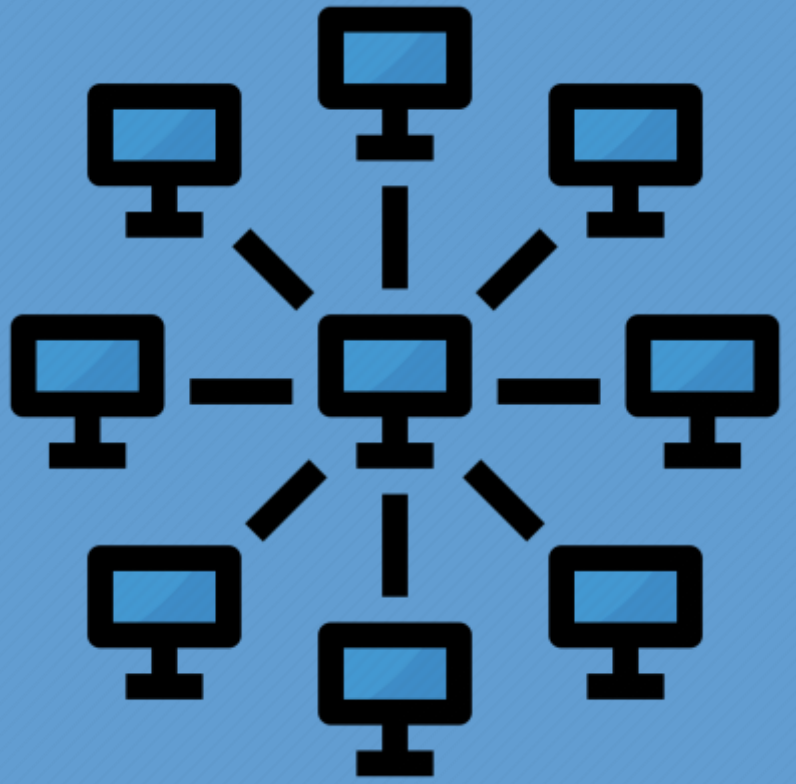
ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ. ЧАСТЬ 1



ЛЕКЦИЯ 7. АДРЕСАЦИЯ IPV4

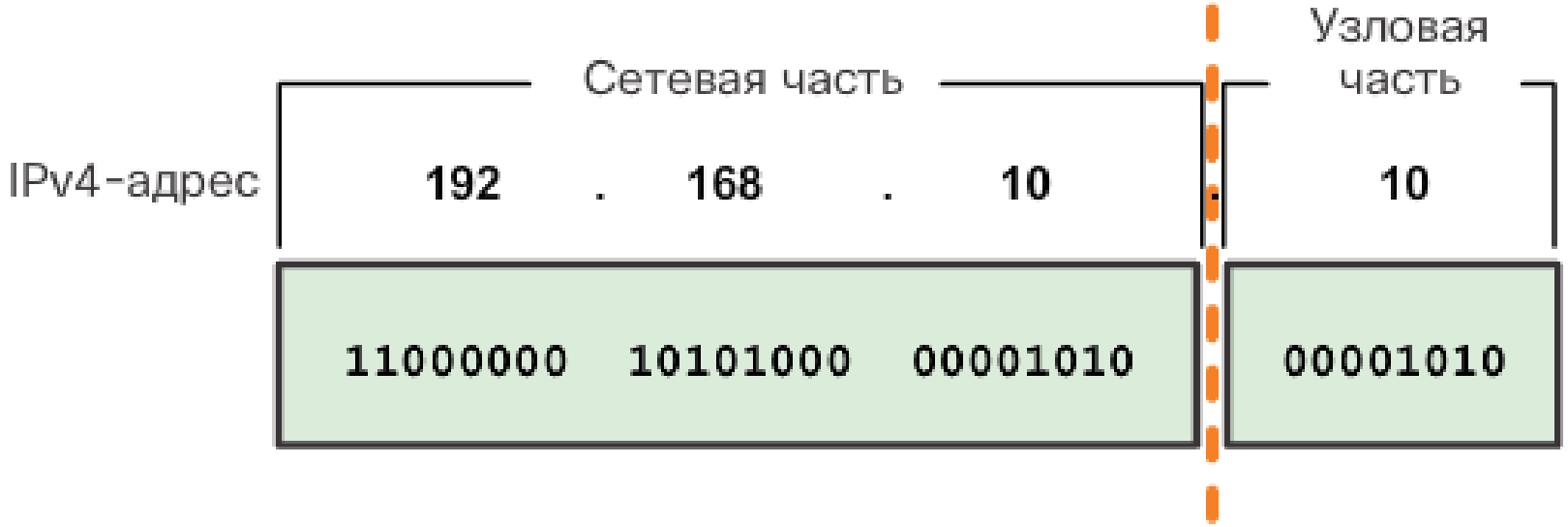
КАФЕДРА
ТЕЛЕКОММУНИКАЦИЙ

7.1. СТРУКТУРА АДРЕСА IPV4
7.1.1. СЕТЕВАЯ И ХОСТОВАЯ ЧАСТЬ

Адрес IPv4 является иерархическим и состоит из **сетевой** части и **хостовой** части.

Определяя ту или иную часть, необходимо обращать внимание не на десятичное значение, а на 32-битную запись.

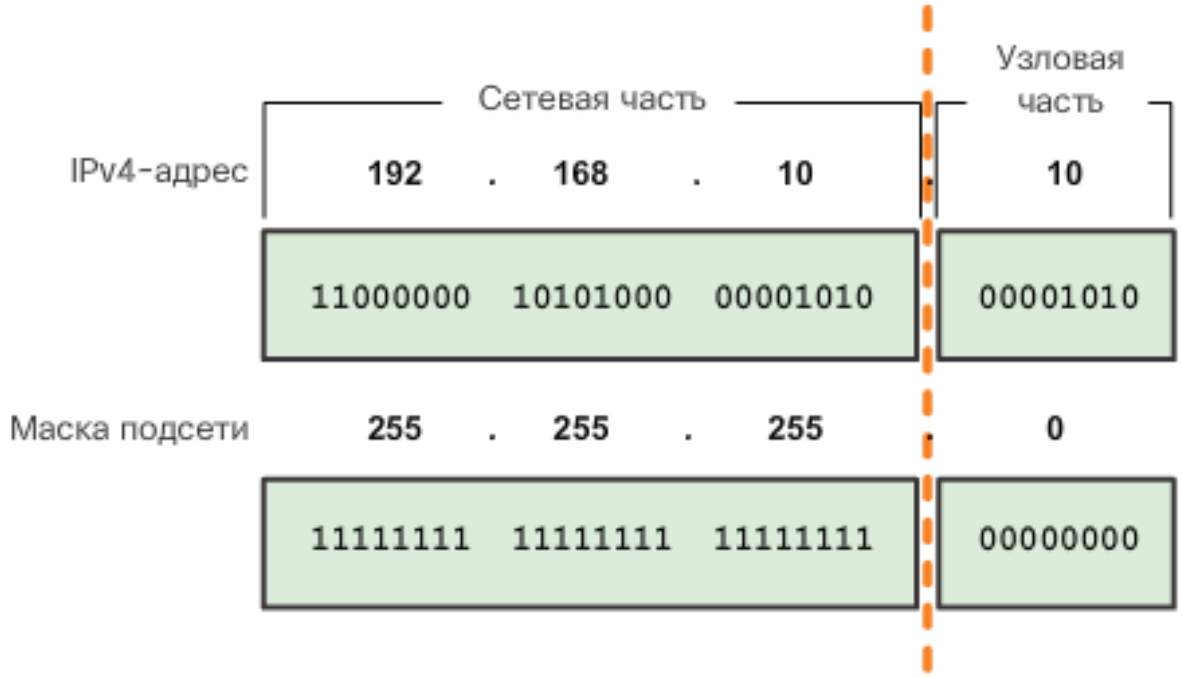
Маска подсети используется для определения сетевой и хостовой части адреса.



7.1. СТРУКТУРА АДРЕСА IPV4
7.1.2. МАСКА ПОДСЕТИ

Для идентификации сетевой и узловой части IPv4-адреса **маска подсети** побитово сравнивается с IPv4-адресом слева направо, как показано на рисунке.

Сам процесс, используемый для определения сетевой и узловой частей адреса, называется логической операцией И (AND).



7.1. СТРУКТУРА АДРЕСА IPV4
7.1.3. ДЛИНА ПРЕФИКСА

Длина префикса является менее громоздким методом, используемым для идентификации адреса маски подсети.

Длина префикса означает количество бит, установленных в единицу (1) в маске подсети.

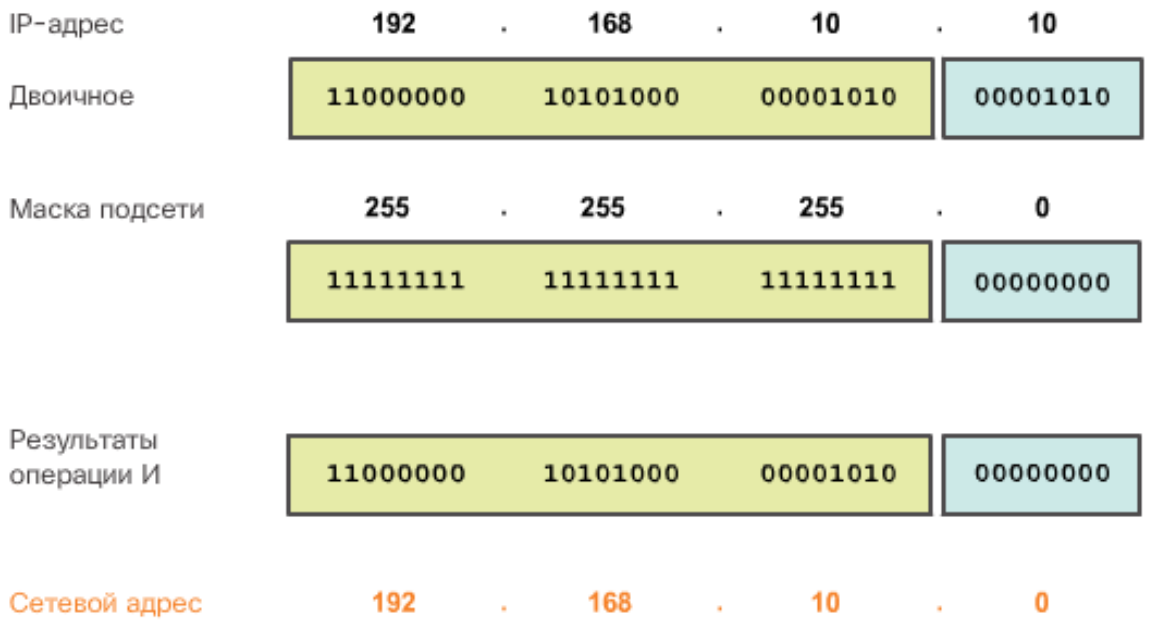
Следовательно, нужно подсчитать число битов в маске подсети и поставить перед этим значением косую черту.

Маска подсети	32-битный адрес	Префикс Длина
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.111111111111111.10000000	/25
255.255.255.192	11111111.11111111.111111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

7.1. СТРУКТУРА АДРЕСА IPV4
7.1.4. ДЛИНА ПРЕФИКСА

Логическая операция И – это сравнение двух битов.

В результате выполнения побитовой логической операции И между адресом и маской подсети получается соответствующий **адрес сети**.

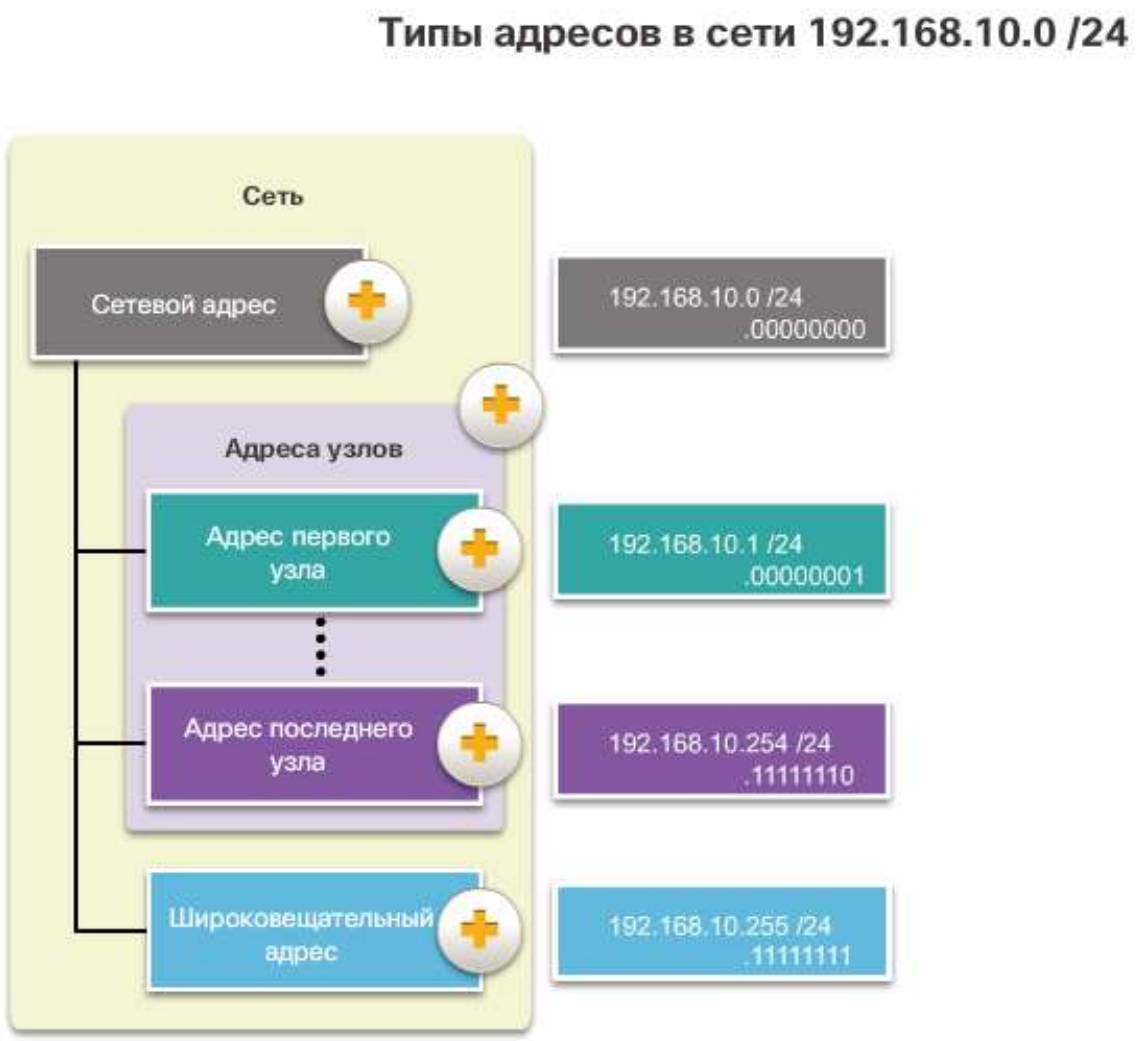


1 И 1 = 1
0 И 1 = 0
0 И 0 = 0
1 И 0 = 0

7.1. СТРУКТУРА АДРЕСА IPV4
7.1.4. ТИПЫ АДРЕСОВ

В каждой сети есть три типа IP-адресов:

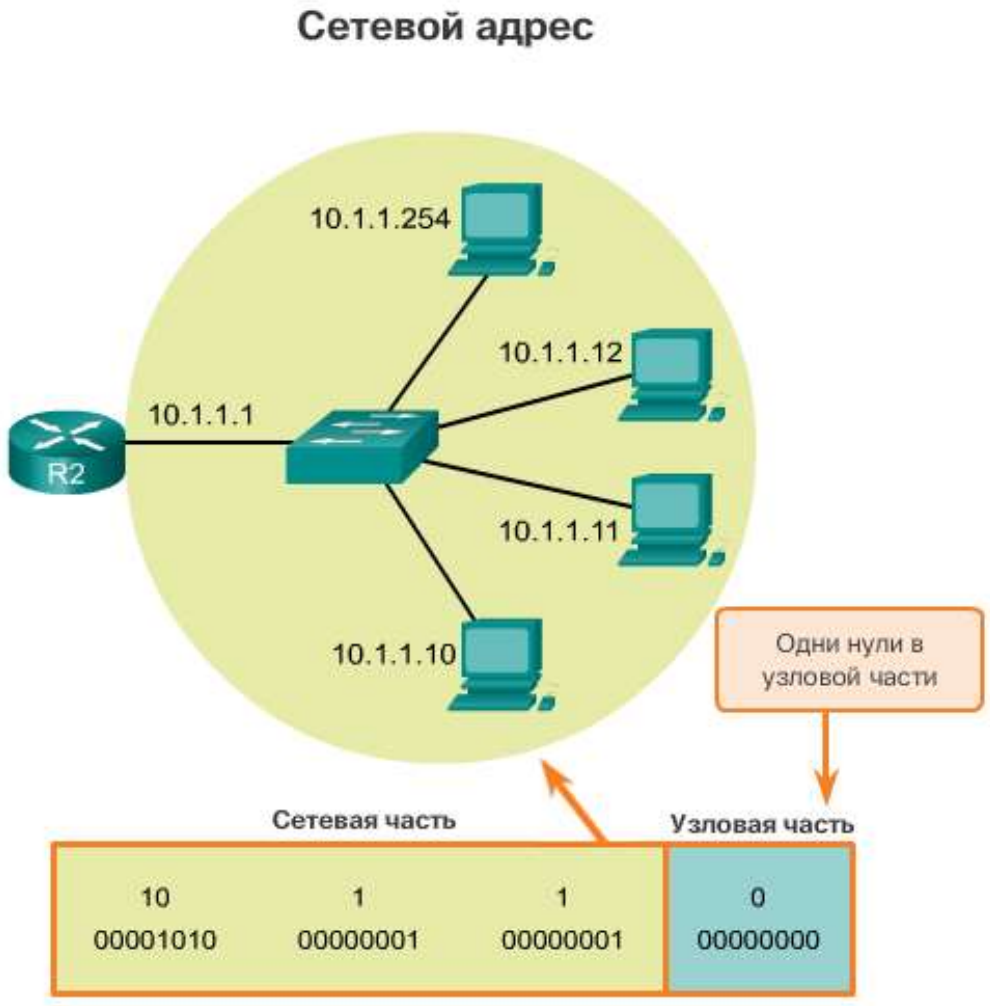
1. Сетевой адрес
2. Адрес хоста
3. Широковещательный адрес



7.1. СТРУКТУРА АДРЕСА IPV4
7.1.5. СЕТЕВОЙ АДРЕС

Сетевой адрес – это адрес, представляющий определенную сеть. Устройство принадлежит этой сети, если оно удовлетворяет трем критериям:

1. Он имеет ту же маску подсети, что и сетевой адрес.
2. Он имеет те же биты сети, что и сетевой адрес, как указано маской подсети.
3. Он расположен в том же домене широковещательной рассылки, что и другие узлы с тем же сетевым адресом.

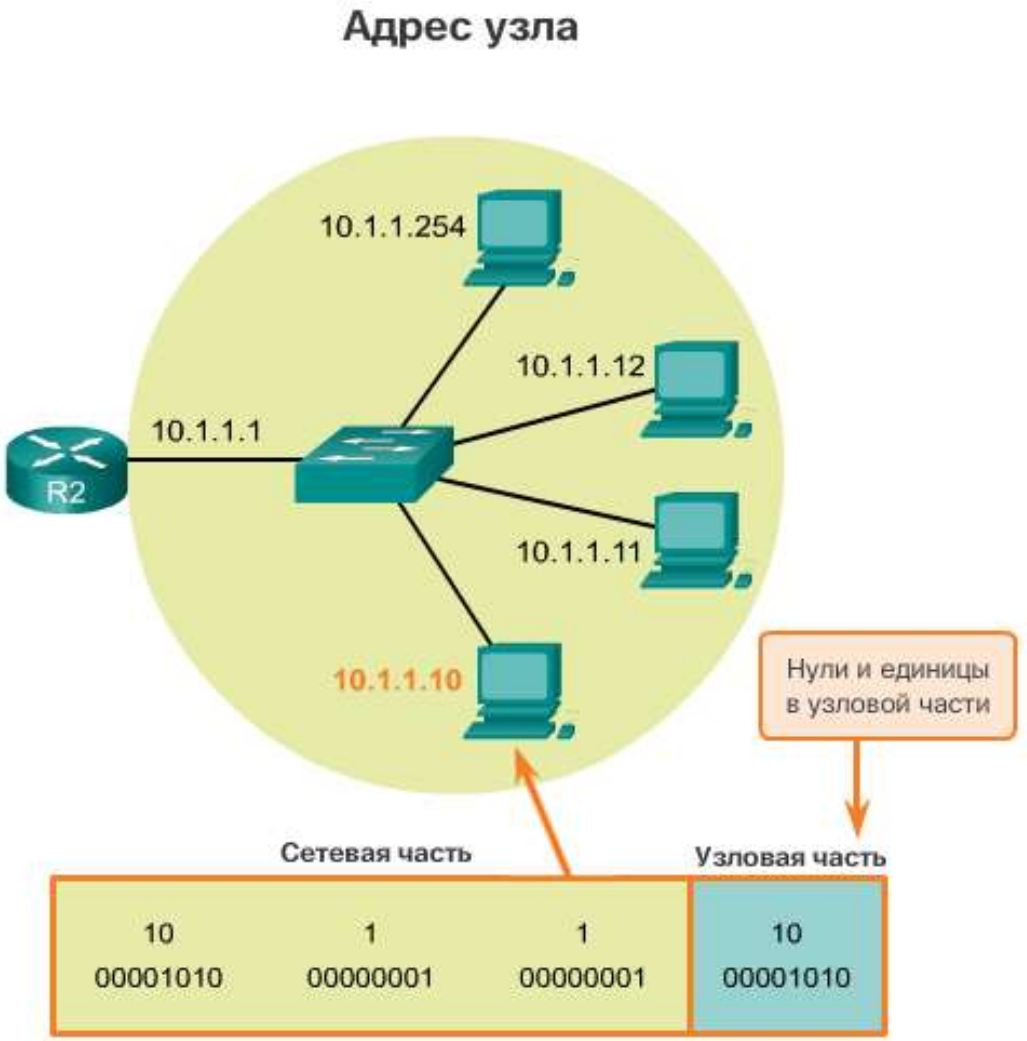


7.1. СТРУКТУРА АДРЕСА IPV4
7.1.6. АДРЕС УЗЛА

Адреса узлов – это адреса, которые могут быть назначены устройству, например компьютеру, ноутбуку, смартфону, веб-камере, принтеру, маршрутизатору и т.д.

Основной частью адреса являются биты, обозначенные 0 битами в маске подсети.

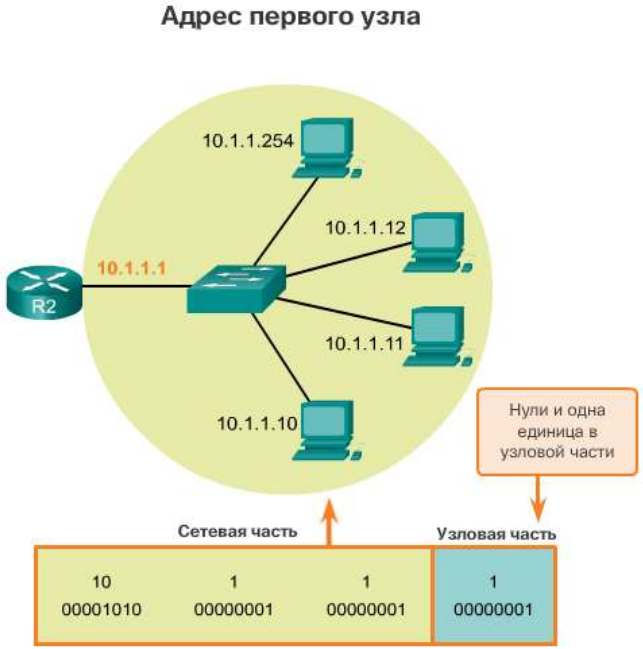
Адреса хоста могут иметь любую комбинацию битов в части хоста, за исключением всех 0 битов (это будет сетевой адрес) или всех 1 битов (это будет широковещательный адрес).

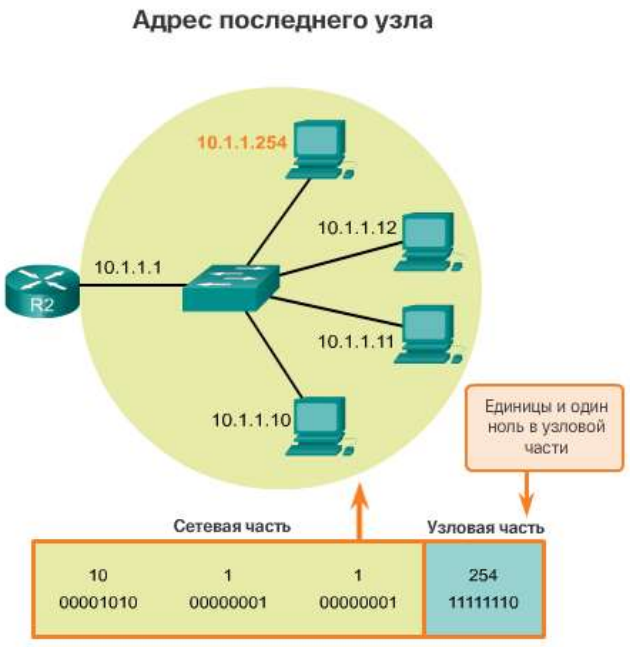


7.1. СТРУКТУРА АДРЕСА IPV4
7.1.7. АДРЕС ПЕРВОГО И ПОСЛЕДНЕГО УЗЛА

Первый используемый адрес – этот первый узел в сети имеет все 0 бит с последним (самым правым) битом в 1 бит. В этом примере это 10.1.1.1/24.

Последний используемый адрес – этот последний узел в сети имеет все 1 бит с последним (самым правым) битом в 0 бит. В этом примере это 10.1.1.254/24.



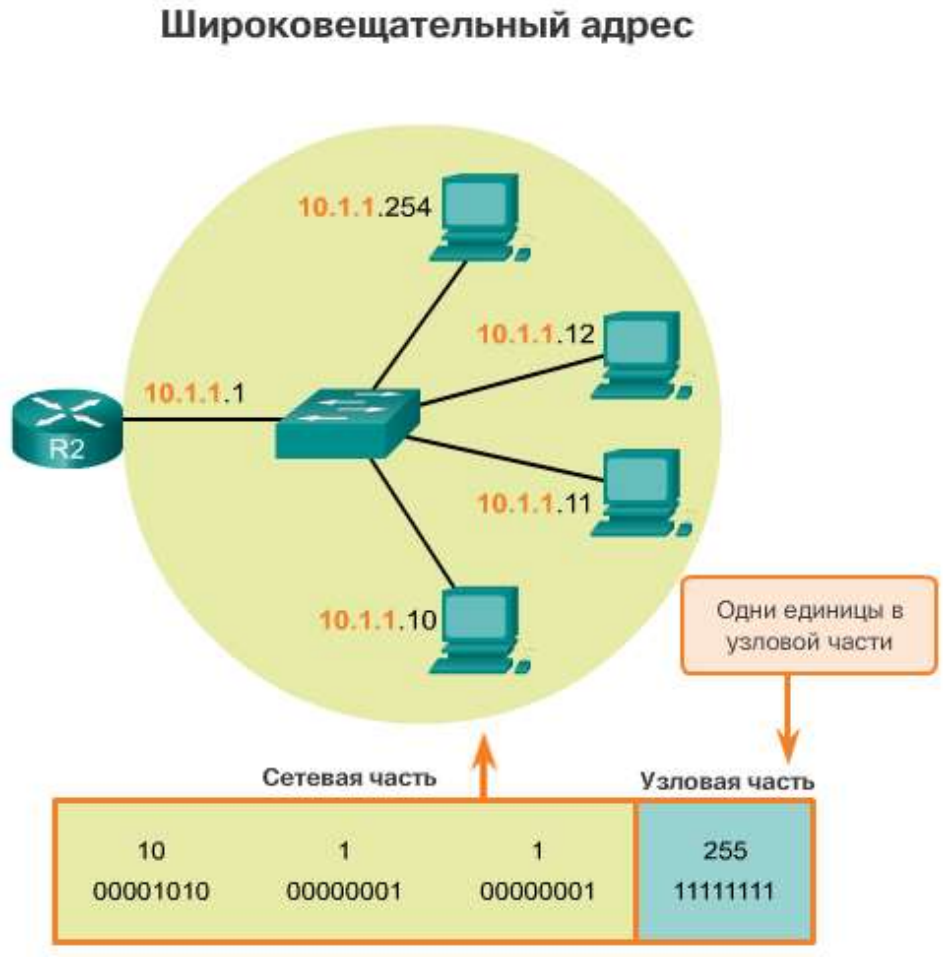


7.1. СТРУКТУРА АДРЕСА IPV4
7.1.8. ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС

Широковещательный адрес – это адрес, который используется, когда он необходим для доступа ко всем устройствам в IPv4-сети.

В этом примере сетевой адрес – 10.1.1.255/24

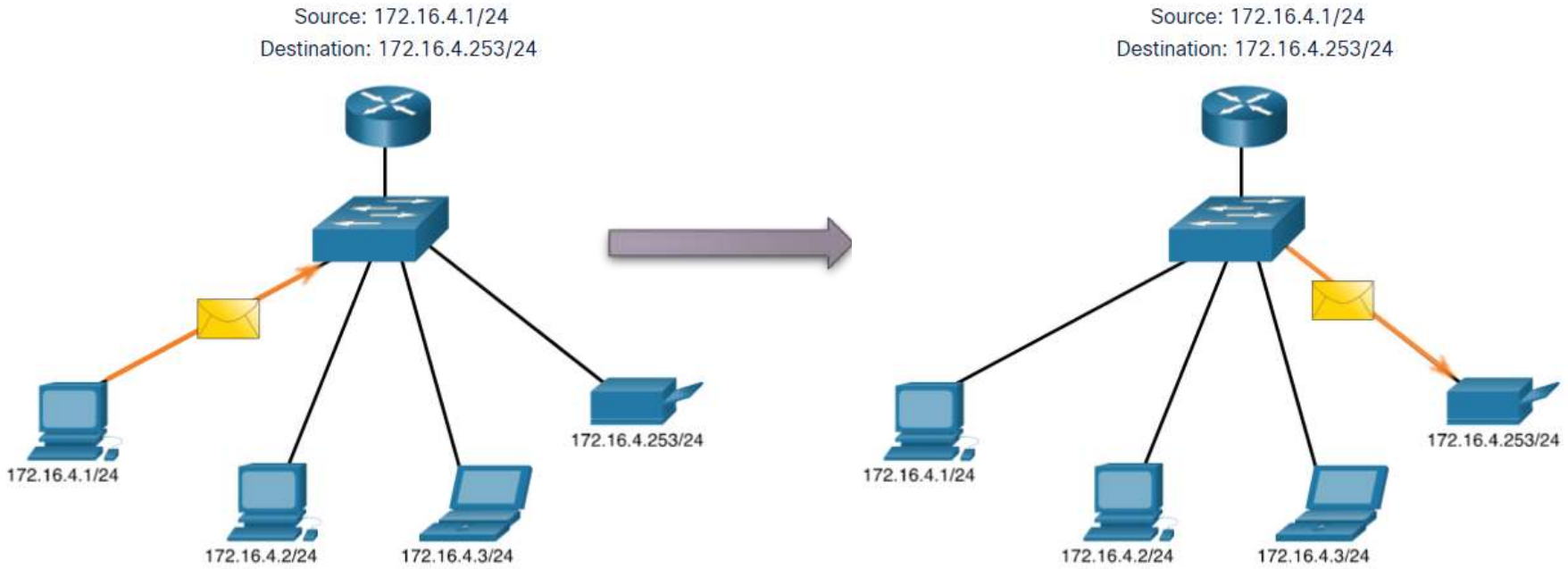
Широковещательный адрес не может быть назначен устройству.



7.2. ВИДЫ РАССЫЛОК
7.2.1. ОДНОАДРЕСНАЯ ПЕРЕДАЧА

Одноадресная передача отправляет пакет на один IP-адрес назначения.

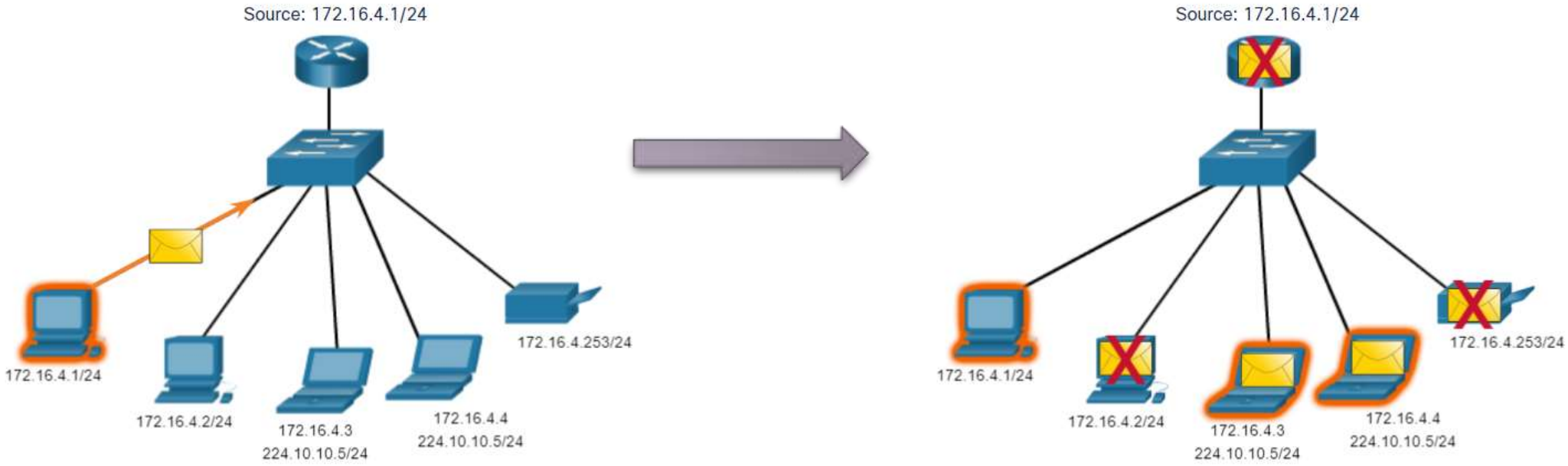
Например, компьютер с адресом 172.16.4.1 отправляет одноадресный пакет на принтер по адресу 172.16.4.253.



7.2. ВИДЫ РАССЫЛОК
7.2.2. МНОГОАДРЕСНАЯ ПЕРЕДАЧА

Многоадресная передача отправляет пакет в группу адресов многоадресной рассылки.

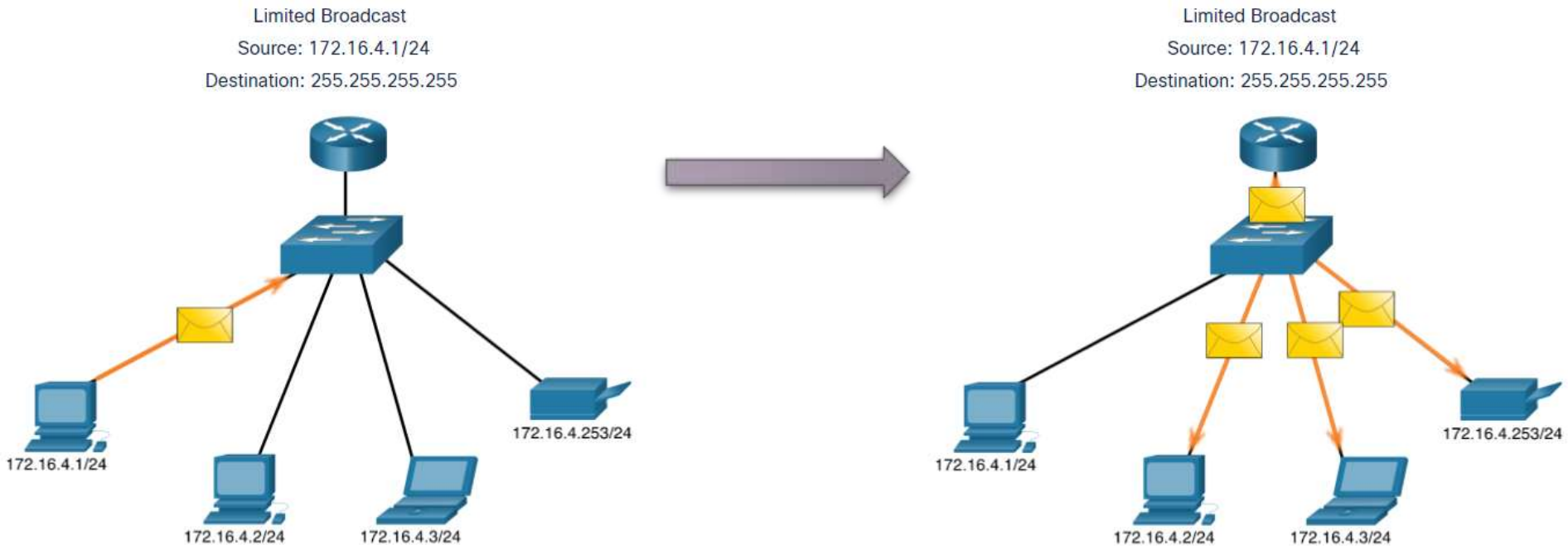
Например компьютер 172.16.4.1 отправляет многоадресный пакет на адрес группы многоадресной рассылки 224.10.10.5.



7.2. ВИДЫ РАССЫЛОК
7.2.2. ШИРОКОВЕЩАТЕЛЬНАЯ ПЕРЕДАЧА

Широковещательная передача отправляет пакет на все другие IP-адреса назначения.

Например, компьютер 172.16.4.1 отправляет широковещательный пакет всем узлам IPv4.



7.3. ТИПЫ IPV4 АДРЕСОВ
7.3.1. ПУБЛИЧНЫЕ И ЧАСТНЫЕ IPV4-АДРЕСА

Публичные IPv4-адреса представляют собой адреса, на глобальном уровне маршрутизируемые между маршрутизаторами интернет-провайдеров (Internet Service Provider, ISP).

Имеются блоки адресов, называемые **частными адресами**, которые в большинстве компаний назначаются в качестве IPv4-адресов внутренних хостов.

Частные адреса IPv4 не являются уникальными и могут использоваться в любой внутренней сети.

Однако частные адреса не являются глобально маршрутизируемыми.

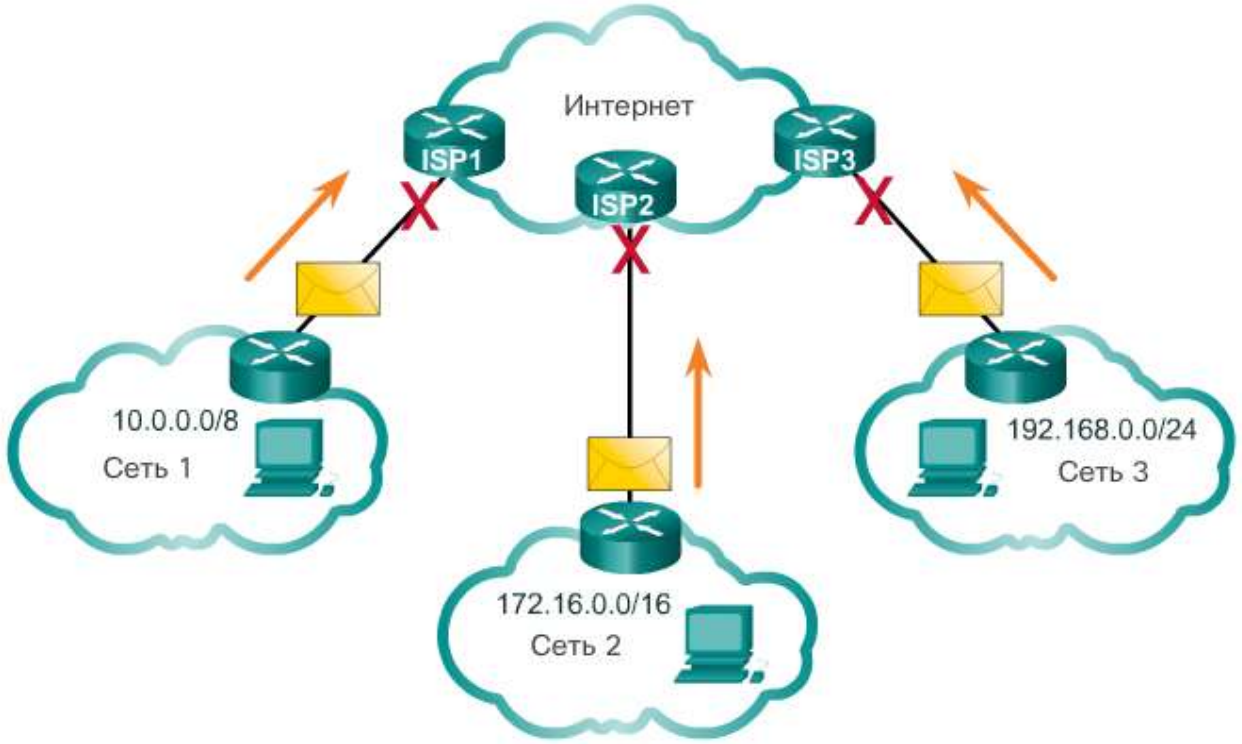
Сетевой адрес и префикс	Диапазон частных адресов RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

7.3. ТИПЫ IPV4 АДРЕСОВ
7.3.2. МАРШРУТИЗАЦИЯ В ИНТЕРНЕТ

Преобразование сетевых адресов (Network Address Translation, NAT) используется для преобразования частного IPv4-адреса в публичный IPv4-адрес.

NAT обычно включается на пограничном маршрутизаторе, подключенном к Интернету.

Он преобразует частные IP-адреса в публичные IP-адреса.



7.3. ТИПЫ IPV4 АДРЕСОВ
7.3.3. IPV4-АДРЕСА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Адреса обратной петли

127.0.0.0/8 или от 127.0.0.1 до 127.255.255.254.

Обычно идентифицируется только как 127.0.0.1.

Используется на хосте для проверки работоспособности конфигурации TCP/IP.

```
C:\Users\Ket>ping 127.0.0.1

Обмен пакетами с 127.0.0.1 по с 32 байтами данных:
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 127.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\Ket>
```

Локальные адреса каналов

169.254.0.0 /16 или от 169.254.0.1 до 169.254.255.254

Более известны как адреса автоматической частной IP-адресации (APIPA).

Используются клиентом с ОС Windows для автоматической настройки, если нет доступного DHCP-сервера.

7.3. ТИПЫ IPV4 АДРЕСОВ
7.3.4. ТРАДИЦИОННАЯ КЛАССОВАЯ АДРЕСАЦИЯ

RFC 790 (1981) выделил адреса IPv4 в классах:

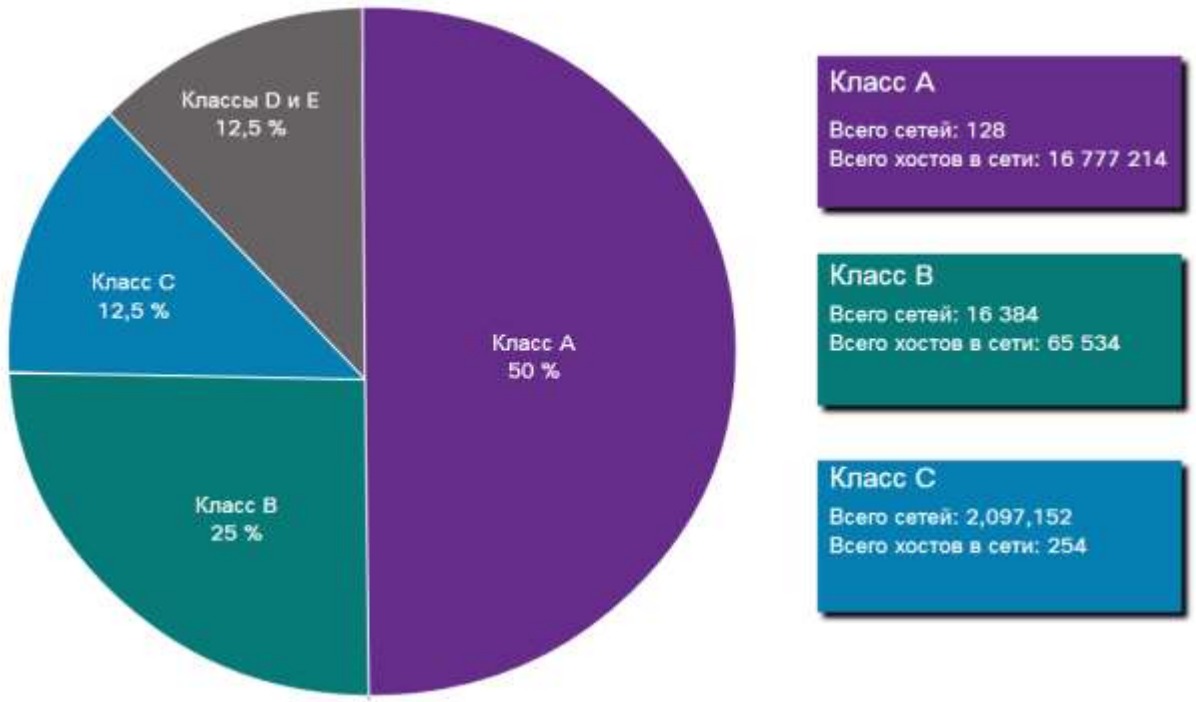
Класс A (0.0.0.0/8 – 127.0.0.0/8)

Класс B (128.0.0.0/16 – 191.255.0.0/16)

Класс C (192.0.0.0/24 – 223.255.255.0/24)

Класс D (224.0.0.0 – 239.0.0.0)

Класс E (240.0.0.0 – 255.0.0.0)



Классическая адресация потратила много адресов IPv4.

Классовое распределение адресов было заменено бесклассовой адресацией, которая игнорирует правила классов (A, B, C).

7.3. ТИПЫ IPV4 АДРЕСОВ
7.3.5. НАЗНАЧЕНИЕ IP-АДРЕСОВ

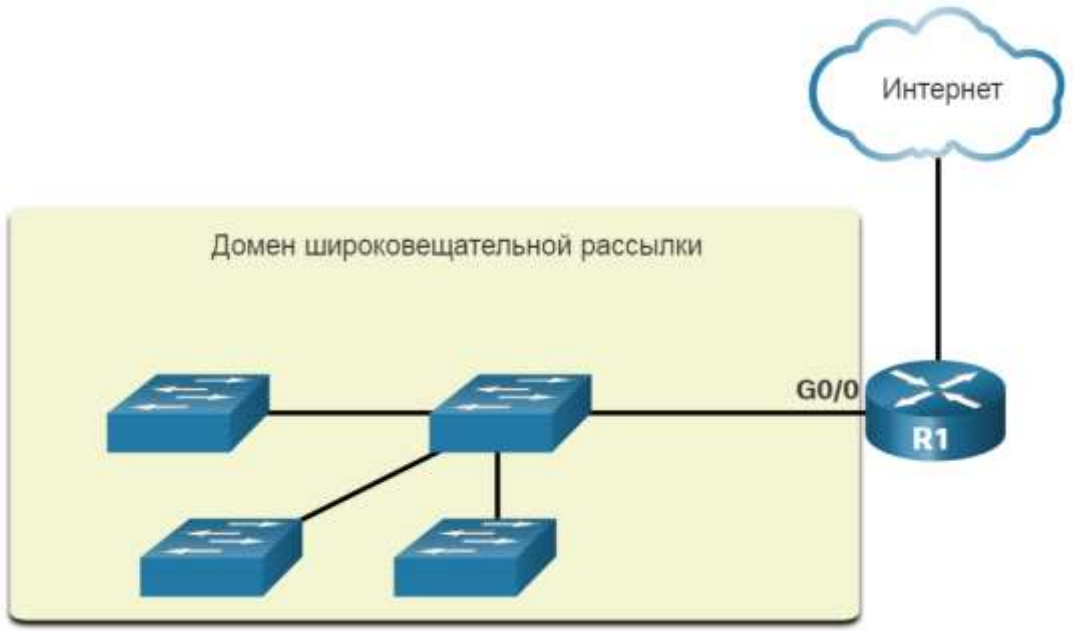
IANA управляет блоками IP-адресов и распределяет их между региональными интернет-регистраторами (RIR).

Региональные интернет-регистраторы (RIR) отвечают за распределение IP-адресов между интернет-провайдерами (ISP), которые, в свою очередь, предоставляют блоки IPv4-адресов организациям и менее крупным провайдерам.

7.4. СЕГМЕНТАЦИЯ СЕТИ
7.4.1. ДОМЕНЫ ШИРОКОВЕЩАТЕЛЬНОЙ РАССЫЛКИ

Многие протоколы используют широковещательные или многоадресные рассылки (например, **ARP** использует широковещательные рассылки для поиска других устройств, хосты отправляют широковещательные рассылки **DHCP** для поиска DHCP-сервера).

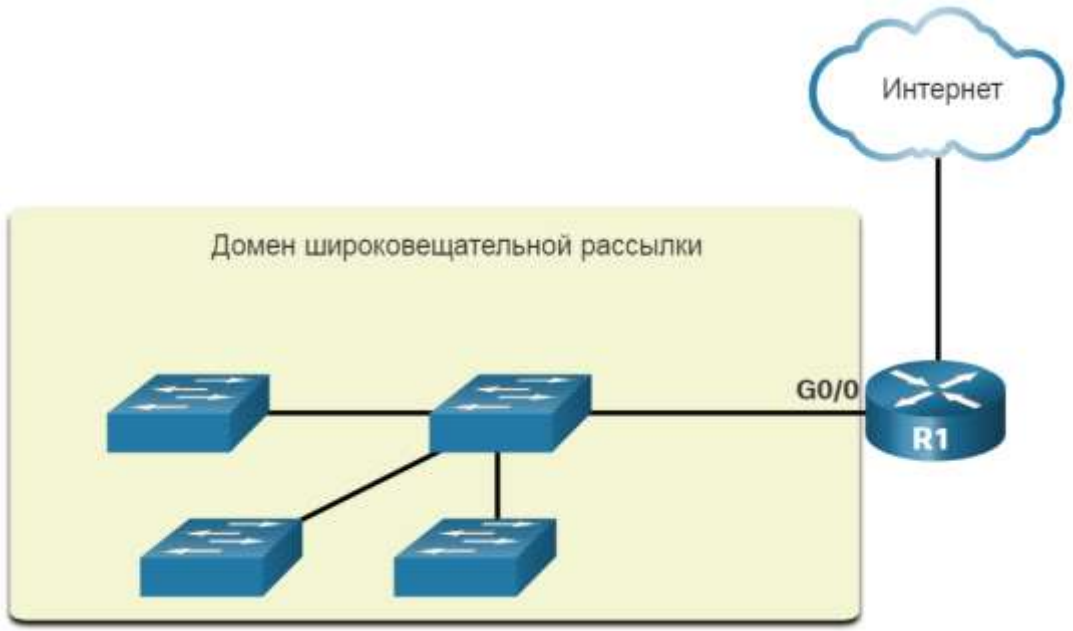
Коммутаторы выполняют широковещательную рассылку на все интерфейсы, за исключением того интерфейса, через который была получена рассылка.



7.4. СЕГМЕНТАЦИЯ СЕТИ
7.4.1. ДОМЕНЫ ШИРОКОВЕЩАТЕЛЬНОЙ РАССЫЛКИ

Единственным устройством, останавливающим широковещательные передачи, является **маршрутизатор**. Маршрутизаторы не выполняют широковещательную рассылку.

Таким образом, каждый интерфейс маршрутизатора подключен к широковещательному домену, и широковещательные рассылки выполняются только в рамках определенного домена рассылки.



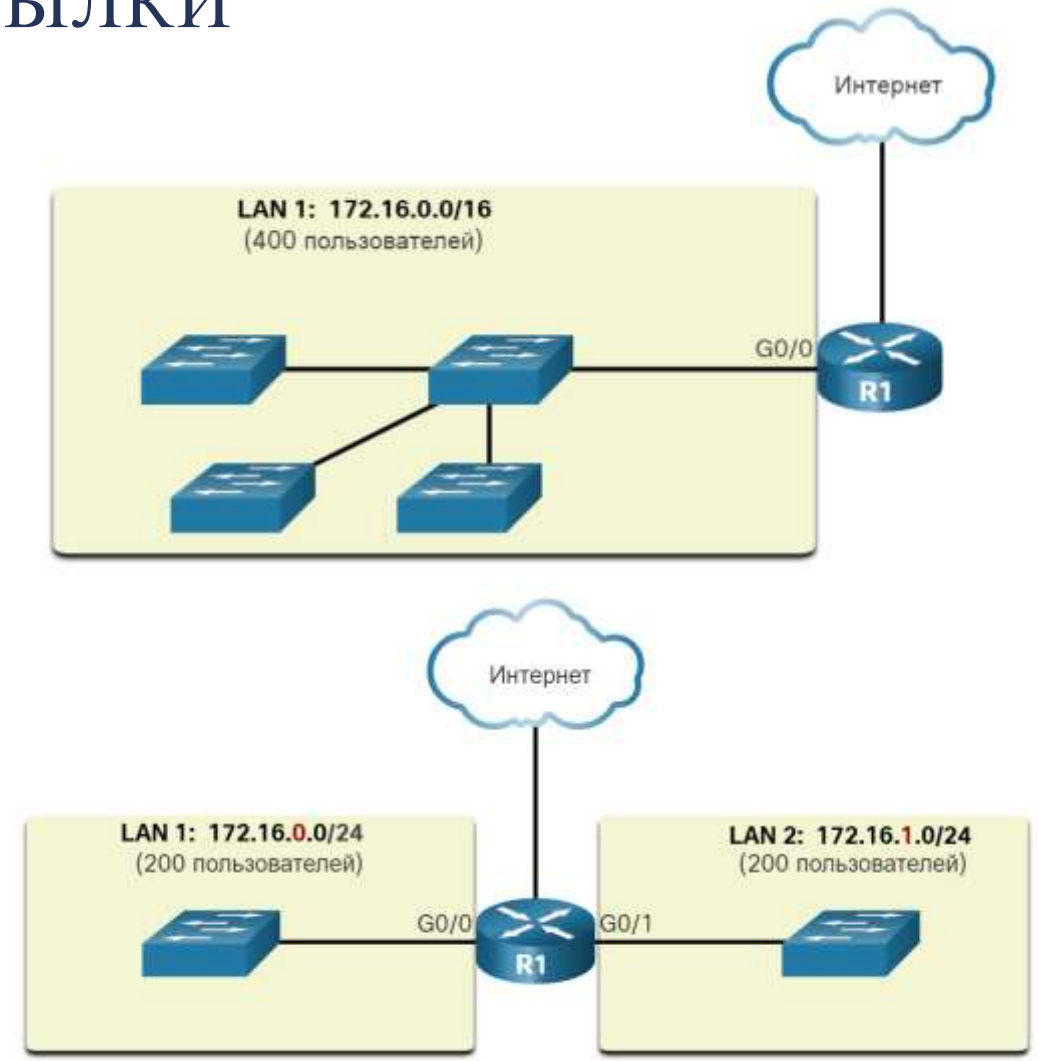
7.4. СЕГМЕНТАЦИЯ СЕТИ
7.4.2. ПРОБЛЕМЫ С КРУПНЫМИ ДОМЕНАМИ ШИРОКОВЕЩАТЕЛЬНОЙ РАССЫЛКИ

Проблема крупного домена широковещательной рассылки заключается в следующем: узлы могут генерировать избыточную рассылку и негативно влиять на работу сети.

Для решения этой проблемы надо сократить размер сети, создав меньшие домены широковещательной рассылки. Такой процесс называется **разделением на подсети**.

400 пользователей локальной сети LAN 1 с сетевым адресом 172.16.0.0 /16 были разделены на две подсети по 200 пользователей каждая – 172.16.0.0 /24 и 172.16.1.0 /24.

Рассылка ограничивается более мелкими доменами широковещательной рассылки.



7.4. СЕГМЕНТАЦИЯ СЕТИ
7.4.3. ПРИЧИНЫ ДЛЯ РАЗДЕЛЕНИЯ НА ПОДСЕТИ

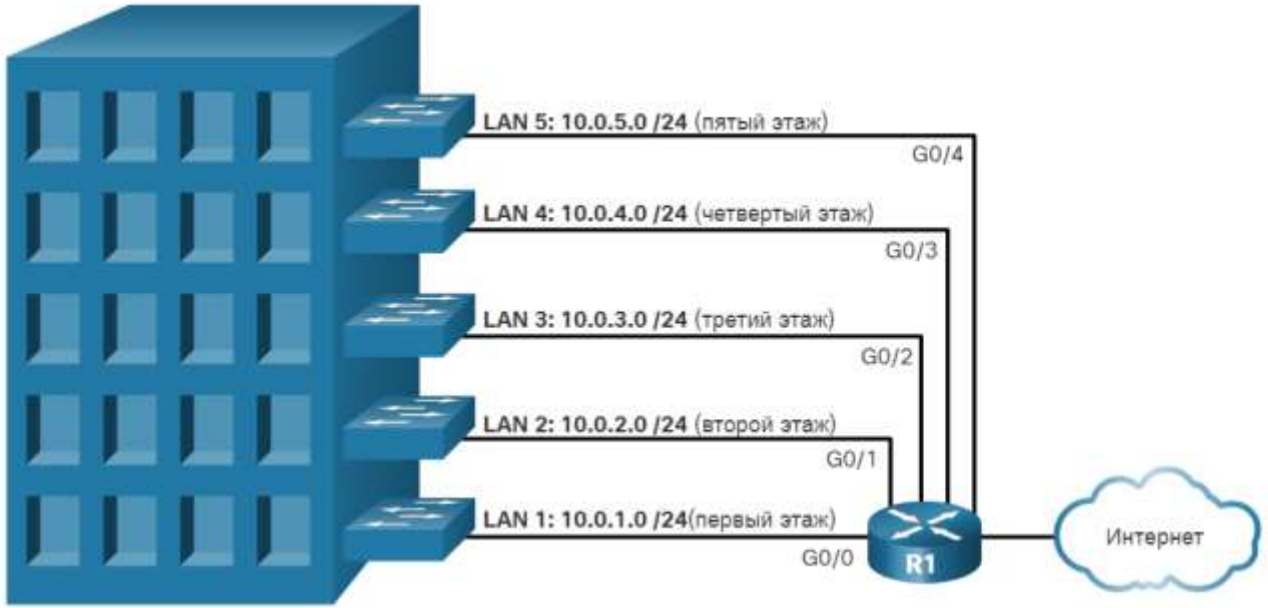
Разделение на подсети снижает общий объем сетевого трафика и повышает производительность сети.

Его можно использовать для реализации политик безопасности между подсетями.

Подсеть уменьшает количество устройств, затронутых аномальным широковещательным трафиком.

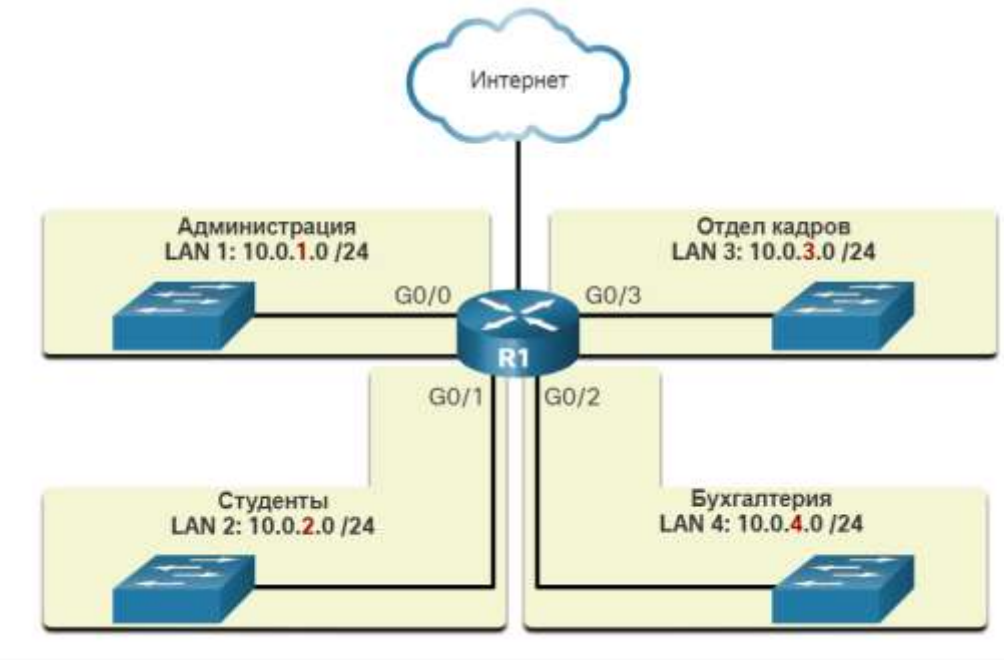
Существует несколько способов использования подсетей для управления сетевыми устройствами.

1. Местоположение

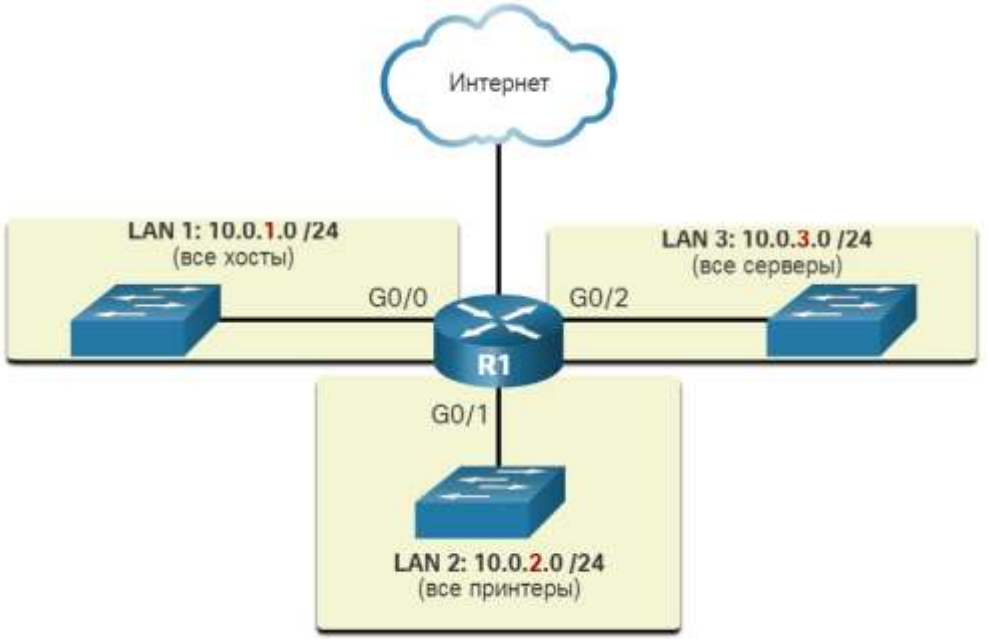


7.4. СЕГМЕНТАЦИЯ СЕТИ
7.4.3. ПРИЧИНЫ ДЛЯ РАЗДЕЛЕНИЯ НА ПОДСЕТИ

2. Группа или функция



3. Тип устройства



7.5. РАЗДЕЛЕНИЕ СЕТИ IPV4
7.5.1. РАЗДЕЛЕНИЕ НА ПОДСЕТИ НА ГРАНИЦЕ ОКТЕТОВ

Разделение сетей проще всего выполнить на границах октетов **/8**, **/16** и **/24**. В таблице указаны эти длины префикса.

Обратите внимание, что увеличение длины префикса сокращает число узлов в каждой подсети.

Длина префикса	Маска подсети	Маска подсети в двоичной системе (n = сеть, h = хост)	Количество узлов
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16 777 214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65 534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

7.5. РАЗДЕЛЕНИЕ СЕТИ IPV4
7.5.1. РАЗДЕЛЕНИЕ НА ПОДСЕТИ НА ГРАНИЦЕ ОКТЕТОВ

В первой таблице сеть 10.0.0.0/8 разделяется на подсети /16, а во второй таблице – /24.

Адрес подсети (256 возможных подсетей)	**Диапазон хостов** (65 534 возможных хоста в каждой подсети)	**Широковещательная рассылка**
10.0.0.0/**16**	**10.0**.0.1 – **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 – **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 – **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255**.**
10.4.0.0/**16**	**10.4**.0.1 - **10,4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**107**.0.1 - **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Адрес подсети (65,536 возможных подсетей)	**Диапазон узлов** (254 возможных узла в каждой подсети)	**Широковещательная рассылка**
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	10.0.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

7.5. РАЗДЕЛЕНИЕ СЕТИ IPV4
7.5.1. РАЗДЕЛЕНИЕ НА ПОДСЕТИ НА ГРАНИЦЕ ОКТЕТОВ

См. таблицу, чтобы увидеть шесть способов разделения сети /24 на подсети.

Длина префикса	Маска подсети	Маска подсети в двоичной системе (n = сеть, h = узел)	Количество подсетей	Количество узлов
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111. **1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111. **11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111. **111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111. **1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111. **11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111. **111111**00	**64**	2

7.6. ПОДСЕТИ /16 И /8
7.6.1. СОЗДАНИЕ ПОДСЕТЕЙ С ПРЕФИКСОМ /16

В таблице на рисунке представлены все возможные сценарии разделения на подсети сети с префиксом /16.

Длина префикса	Маска подсети	Сетевой адрес (n = сеть, h = хост)	Количество подсетей	Количество узлов
/17	255.255.**128**.0	nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh 11111111.11111111.**1**0000000.00000000	**2**	32766
/18	255.255.**192**.0	nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh 11111111.11111111.**11**000000.00000000	**4**	16382
/19	255.255.**224**.0	nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh 11111111.11111111.**111**00000.00000000	**8**	8 190
/20	255.255.**240**.0	nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh 11111111.11111111.**1111**0000.00000000	**16**	4 094
/21	255.255.**248**,0	nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh 11111111.11111111.**11111**000.00000000	**32**	2 046
/22	255.255.**252**.0	nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh 11111111.11111111.**111111**00.00000000	**64**	1 022
/23	255.255.**254**.0	nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh 11111111.11111111.**1111111**0.00000000	**128**	510

7.6. ПОДСЕТИ /16 И /8
7.6.1. СОЗДАНИЕ ПОДСЕТЕЙ С ПРЕФИКСОМ /16

(продолжение таблицы)

Длина префикса	Маска подсети	Сетевой адрес (n = сеть, h = хост)	Количество подсетей	Количество узлов
/24	255.255.**255.0**	nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh 11111111.11111111.**11111111.00000000**	**256**	254
/25	255.255.**255.128**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh 11111111.11111111.**11111111.1**0000000	**512**	126
/26	255.255.**255.192**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh 11111111.11111111.**11111111.11**000000	**1024**	62
/27	255.255.**255.224**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh 11111111.11111111.**11111111.111**00000	**2048**	30
/28	255.255.**255.240**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh 11111111.11111111.**11111111.1111**0000	**4 096**	14
/29	255.255.**255.248**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh 11111111.11111111.**11111111.11111**000	**8 192**	6
/30	255.255.**255.252**	nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh 11111111.11111111.**11111111.111111**00	**16 384**	2

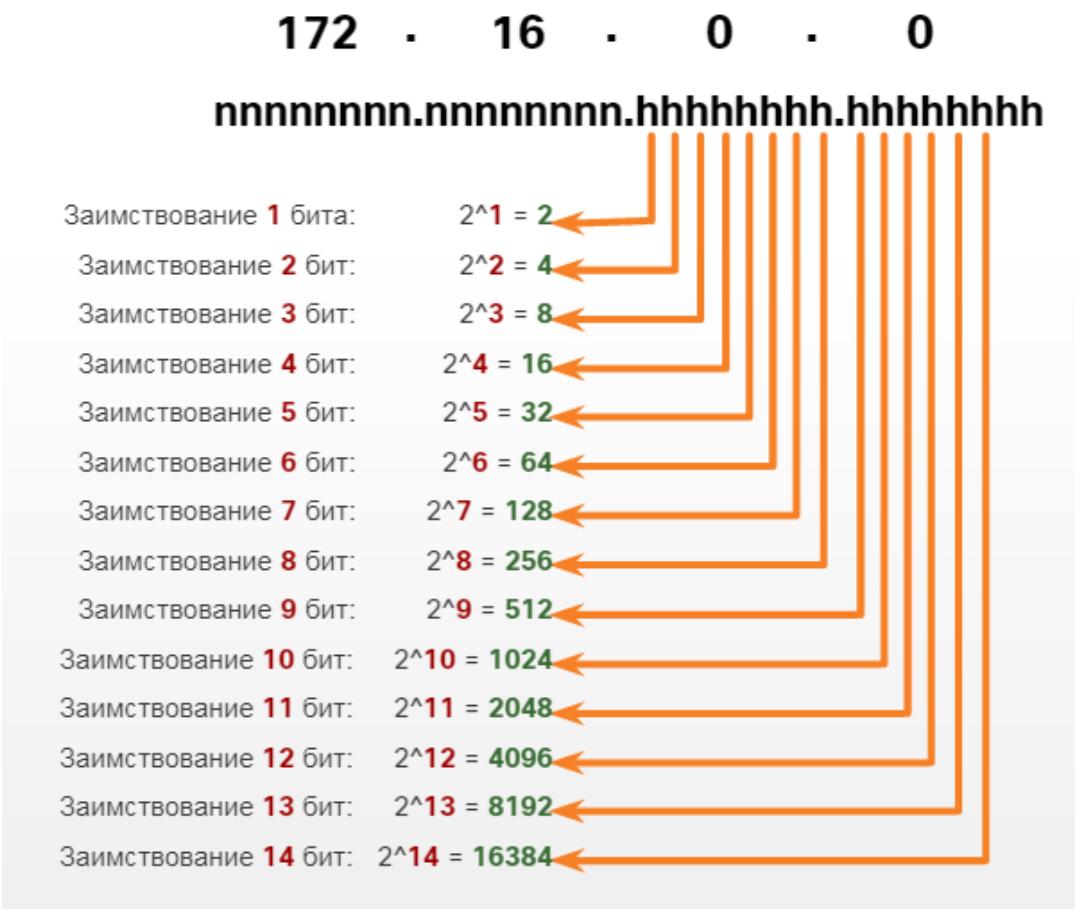
7.6. ПОДСЕТИ /16 И /8
7.6.1. СОЗДАНИЕ ПОДСЕТЕЙ С ПРЕФИКСОМ /16

Рассмотрим крупное предприятие, которому необходимо хотя бы 100 подсетей, и которое выбрало частный адрес **172.16.0.0/16** в качестве адреса внутренней сети.

На рисунке показано количество подсетей, которое может быть создано при заимствовании бит из третьего и четвертого октетов.

Обратите внимание, что теперь есть до 14 битов хоста, которые могут быть заимствованы (то есть, последние два бита не могут быть заимствованы).

Чтобы удовлетворить потребности предприятия, потребуется заимствовать 7 бит (то есть 2^7 = 128 подсетей), как показано на рисунке.



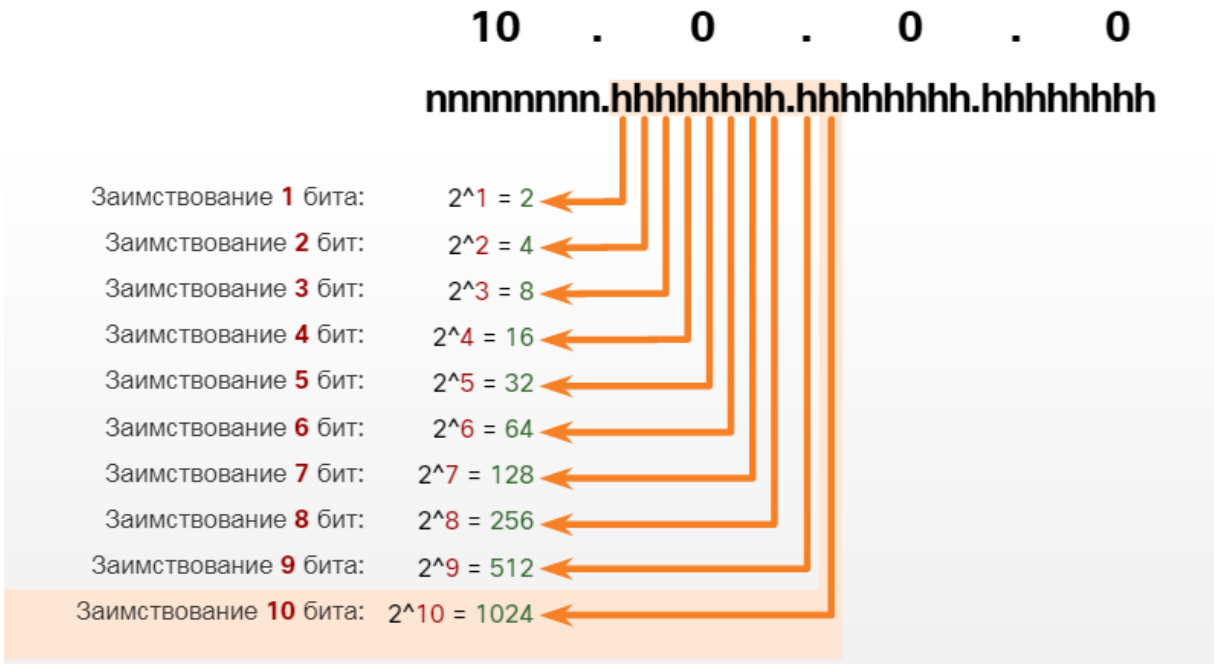
7.6. ПОДСЕТИ /16 И /8
7.6.2. СОЗДАНИЕ ПОДСЕТЕЙ С ПРЕФИКСОМ /8

Рассмотрим небольшой интернет-провайдер, который требует 1000 подсетей для своих клиентов, использующих сетевой адрес **10.0.0.0/8**, что означает, что в сетевой части есть 8 бит и 24 бита узла доступны для заимствования для подсетей.

На рисунке показано количество подсетей, которое может быть создано при заимствовании бит из третьего и четвертого октетов.

Обратите внимание, что теперь есть до 22 битов хоста, которые могут быть заимствованы (то есть, последние два бита не могут быть заимствованы).

Для выполнения требования 1000 подсетей для предприятия необходимо заимствовать 10 бит (т.е. 2^10 = 1024 подсетей.



7.6. ПОДСЕТИ /16 И /8
7.6.3. ФОРМУЛЫ ДЛЯ РАЗБИЕНИЯ ПО ПОДСЕТИ

Данная формула предназначена для расчета **количества необходимых подсетей**:

$$2^n$$

n= заимствованные биты

7.6. ПОДСЕТИ /16 И /8
7.6.3. ФОРМУЛЫ ДЛЯ РАЗБИЕНИЯ ПО ПОДСЕТИ

Данная формула предназначена для расчета **количества необходимых узлов**:

$$2^n-2$$

n= количество бит, оставшееся в узловой части

2^7 = 128 узлов для каждой подсети
2^7 - 2 = 126 допустимых узлов для каждой подсети

7.7. УЧЕТ ТРЕБОВАНИЙ СЕТИ
7.7.1. МИНИМИЗАЦИЯ НЕИСПОЛЬЗУЕМЫХ АДРЕСОВ IPV4 УЗЛОВ И МАКСИМИЗАЦИЯ ПОДСЕТЕЙ

При планировании подсетей нужно учесть два параметра.

1. Необходимое количество адресов узлов в каждой сети.

2. Необходимое количество подсетей.

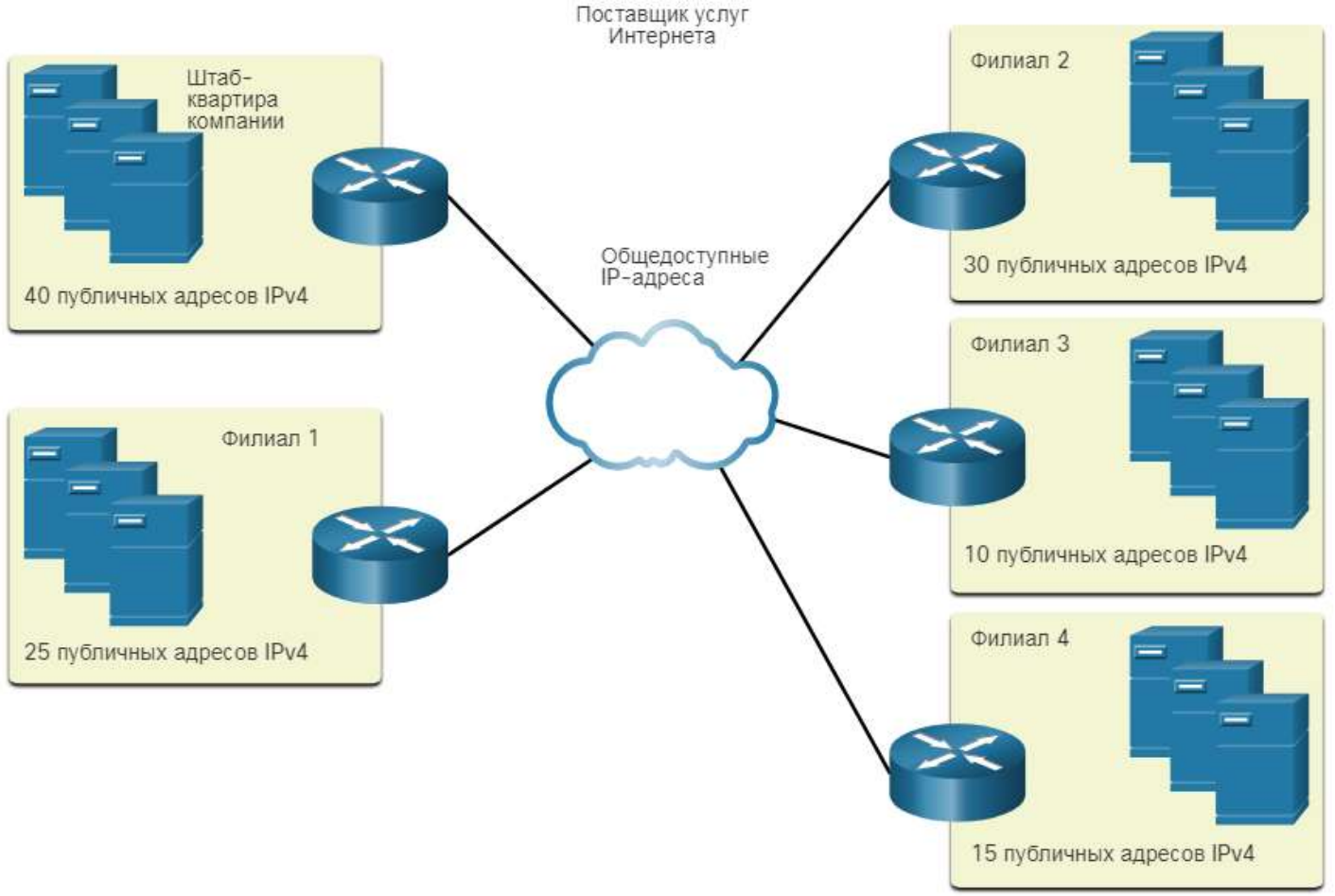
Длина префикса	Маска подсети	Маска подсети в двоичной системе (n = сеть, h = узел)	Количество подсетей	Количество узлов
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

7.7. УЧЕТ ТРЕБОВАНИЙ СЕТИ
7.7.2. ПРИМЕР: ЭФФЕКТИВНОЕ РАЗДЕЛЕНИЕ НА ПОДСЕТИ СЕТИ IPV4

В этом примере штаб-квартира оператора связи выделила адрес частной сети 172.16.0.0/22 (10 бит в узловой части) для филиала.

Существует пять областей, и поэтому пять интернет-соединений, что означает, что организация требует 10 подсетей, а самой большой подсети требуется 40 адресов.

По формуле определения количества подсетей получаем 16 подсетей: 2^4 = 16.



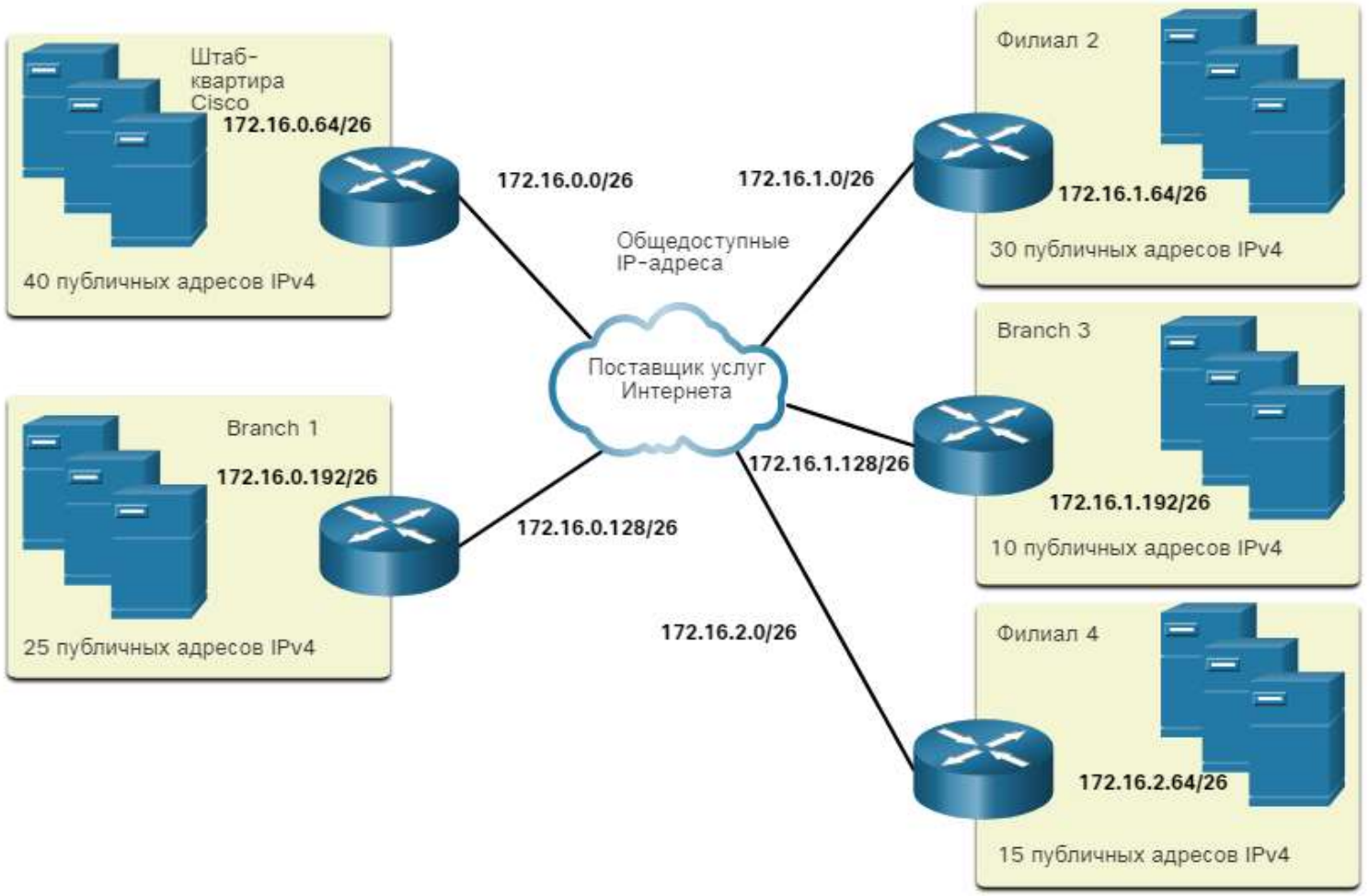
7.7. УЧЕТ ТРЕБОВАНИЙ СЕТИ
7.7.2. ПРИМЕР: ЭФФЕКТИВНОЕ РАЗДЕЛЕНИЕ НА ПОДСЕТИ СЕТИ IPV4

Поскольку самой крупной подсети требуется 40 узлов, для обеспечения их адресации требуется не менее 6 бит в узловой части.

Это число определяется по следующей формуле: 2^6 - 2 = 62 узла.

7.7. УЧЕТ ТРЕБОВАНИЙ СЕТИ
7.7.2. ПРИМЕР: ЭФФЕКТИВНОЕ РАЗДЕЛЕНИЕ НА ПОДСЕТИ СЕТИ IPV4

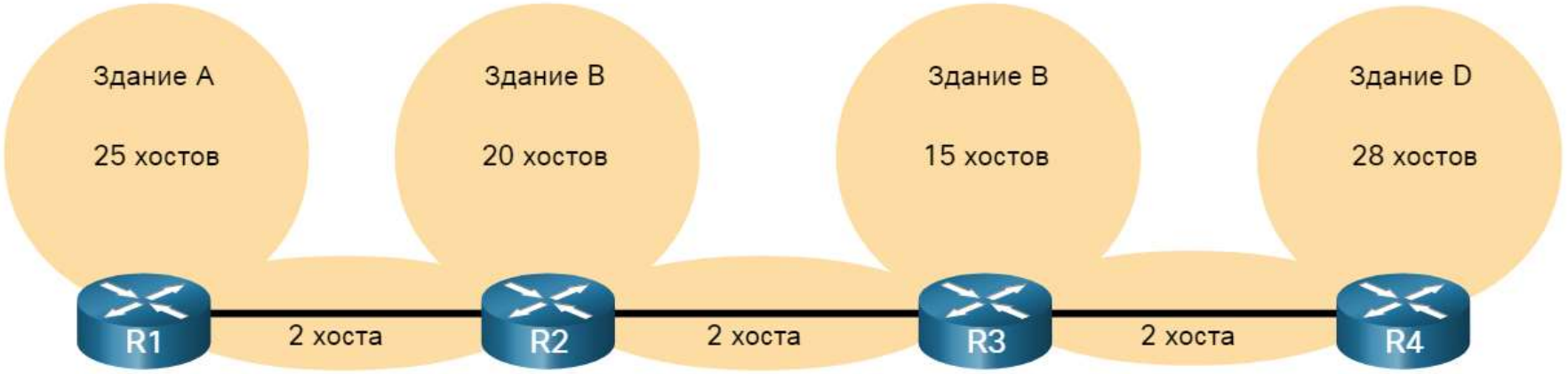
Как показано на рисунке, подсети можно назначить сегментам локальной сети (LAN) и соединениям между маршрутизаторами.



7.8. ОСНОВЫ VLSM
7.8.1. СОХРАНЕНИЕ АДРЕСОВ IPV4

В **традиционном разбиении на подсети** каждой подсети выделяется одинаковое количество адресов. Если все подсети имеют одинаковые требования к количеству узлов, такие блоки адресов фиксированного размера будут эффективными. Как правило, с публичными адресами IPv4 это не так.

Например, в топологии, показанной на рисунке, используются семь подсетей: по одной для каждой из четырех локальных сетей (LAN) и по одной для каждого из трех каналов сети WAN между маршрутизаторами.

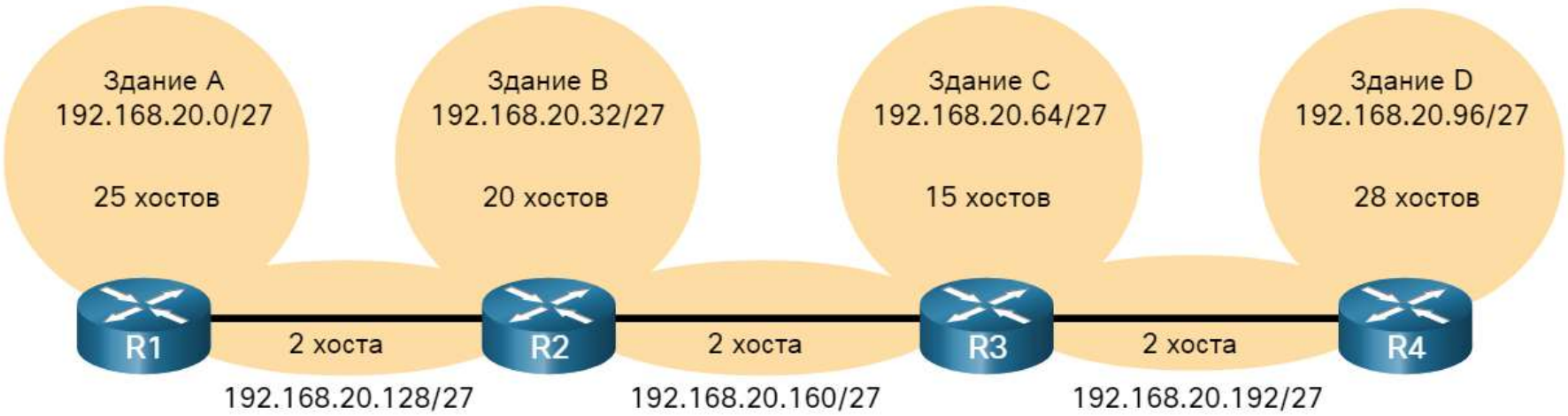


7.8. ОСНОВЫ VLSM
7.8.1. СОХРАНЕНИЕ АДРЕСОВ IPV4

Однако для связи WAN «точка-точка» требуется только два адреса и поэтому теряют по 28 адресов каждый из них в общей сложности 84 неиспользуемых адреса.

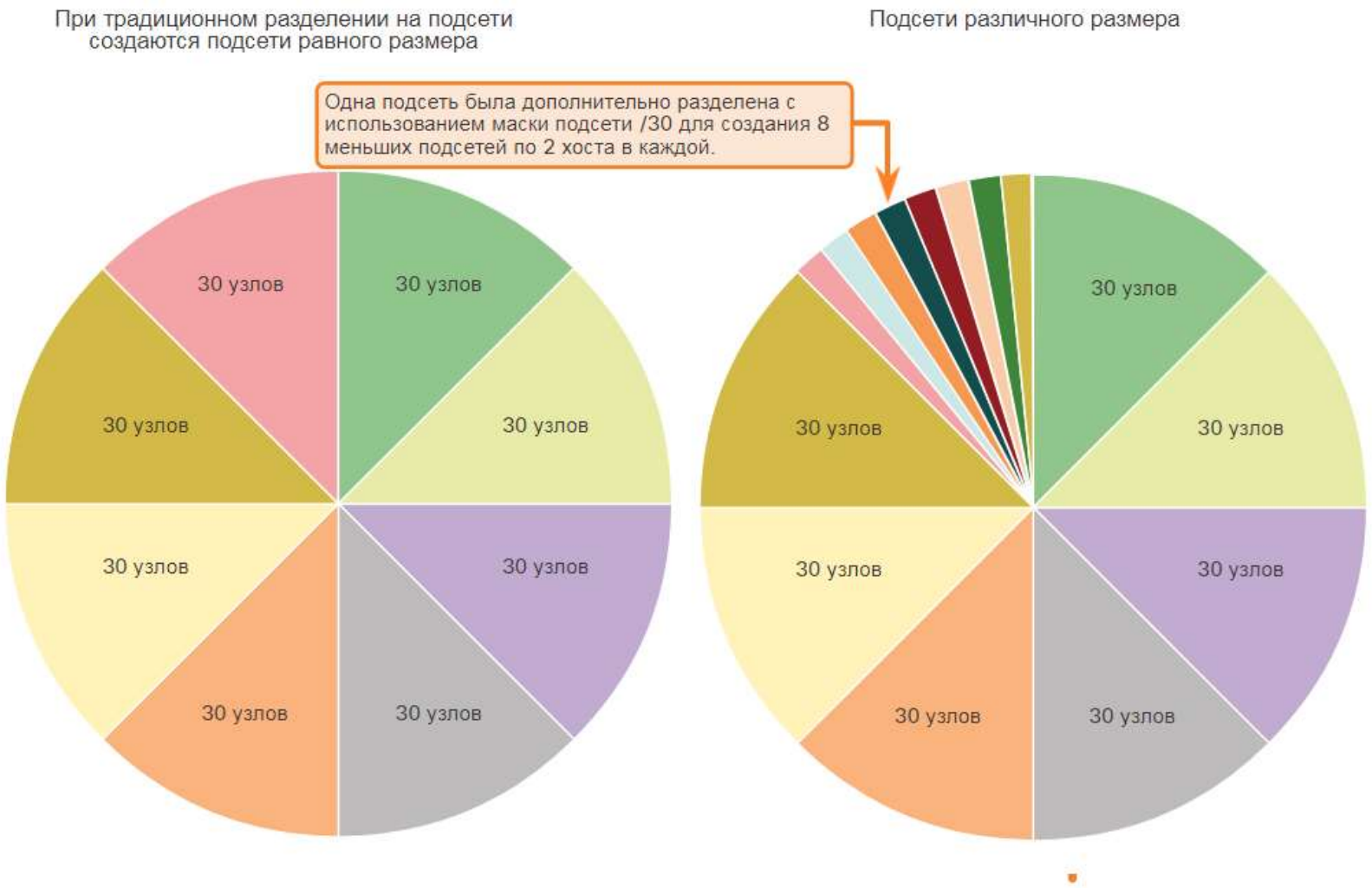
Применение традиционной схемы разделения на подсети по такому сценарию не является эффективным и подразумевает нецелесообразное расходование ресурсов.

VLSM был разработан, чтобы избежать потери адресов, позволяя нам делить подсеть на подсети.



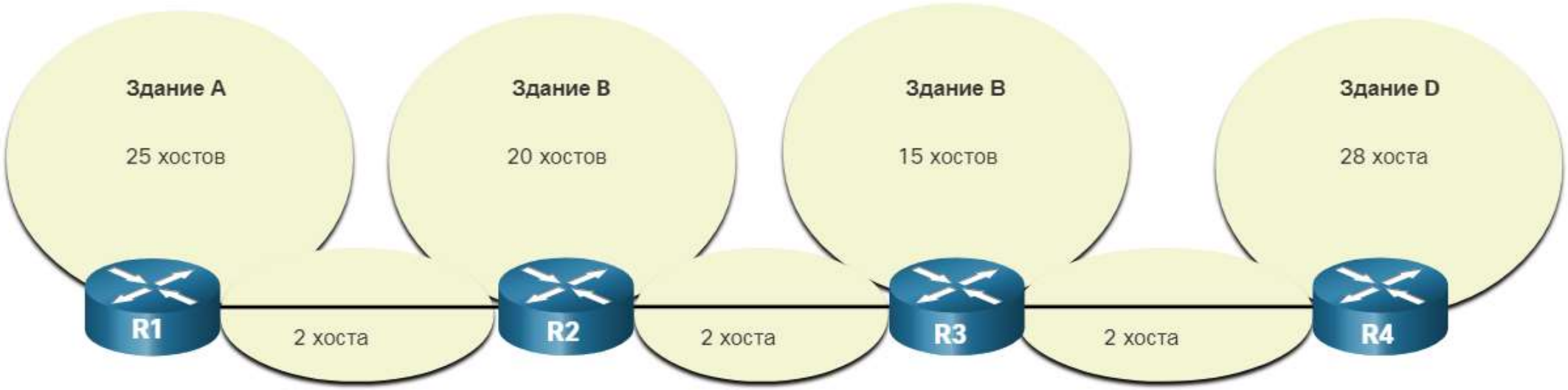
7.8. ОСНОВЫ VLSM
7.8.2. VLSM

Левая сторона отображает традиционную схему подсетей (т.е. же маску подсети), а правая сторон показывает, как **VLSM** можно использовать для разделения на подсети одной из подсетей.



7.8. ОСНОВЫ VLSM
7.8.2. VLSM

При использовании VLSM всегда начинайте с удовлетворения требований к узлу самой большой подсети и продолжайте создание подсетей до тех пор, пока не будут удовлетворены требования к узлу самой маленькой подсети.



7.8. ОСНОВЫ VLSM
7.8.3. РАЗБИЕНИЕ БЕЗ VLSM

На рисунке показано, как сеть 192.168.20.0/24 разбилась на восемь подсетей одинакового размера с 30 используемыми адресами узлов в каждой подсети.

Четыре подсети использовались для локальных сетей (LAN), а три подсети – для каналов между маршрутизаторами.

7.8. ОСНОВЫ VLSM
7.8.4. РАЗБИЕНИЕ С VLSM

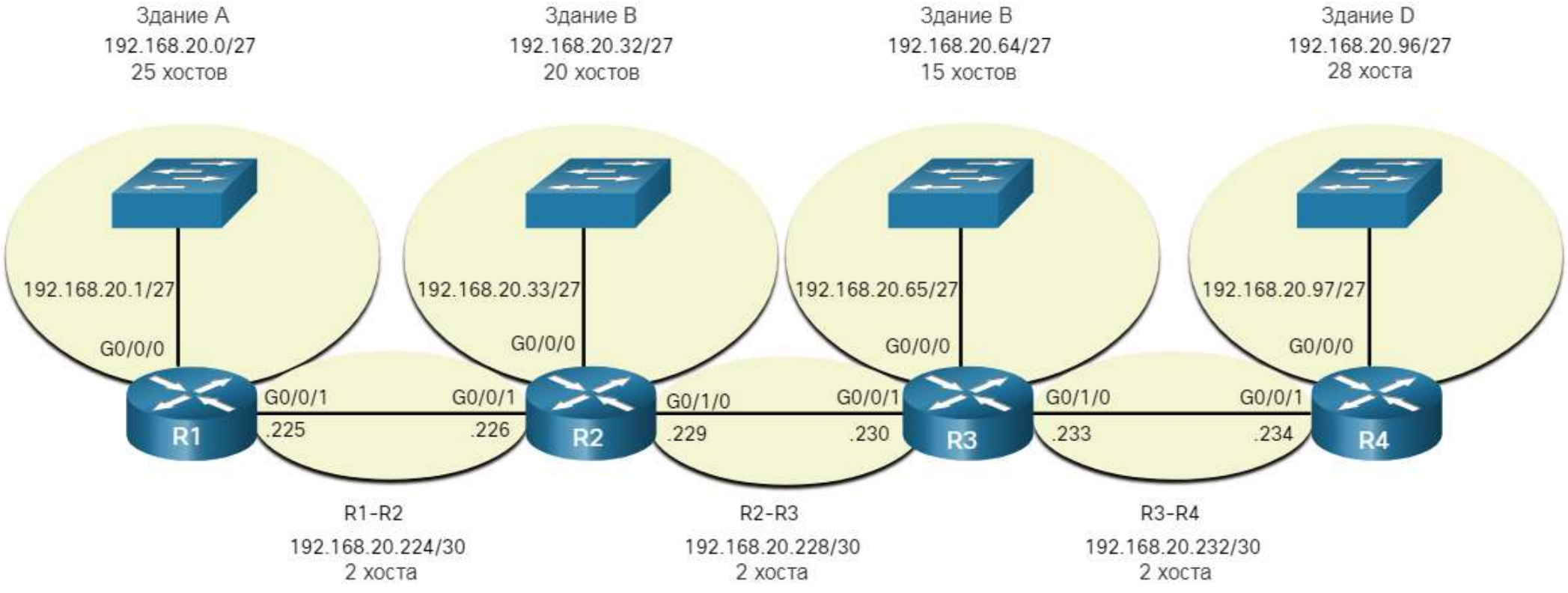
Чтобы создать более мелкие подсети для каналов сети между маршрутизаторами, одна из подсетей будет разделена.

В этом примере последняя подсеть 192.168.20.224/27 будет дополнительно разбита на подсети.

На рисунке показано, что она была дополнительно поделена на подсети с помощью маски подсети 255.255.255.252 или /30.

7.8. ОСНОВЫ VLSM
7.8.4. РАЗБИЕНИЕ С VLSM

На рисунке показано, как четыре подсети /27 были назначены локальным сетям и три подсети /30 были назначены каналам между маршрутизаторами.



7.9. ПРОЕКТИРОВАНИЕ СЕТИ
7.9.1. ПЛАНИРОВАНИЕ АДРЕСАЦИИ СЕТИ

Планирование IP-сетей имеет решающее значение для разработки масштабируемого решения для корпоративной сети.

Чтобы разработать схему адресации для сети IPv4, нужно знать, сколько подсетей необходимо, сколько узлов требуется для конкретной подсети, какие устройства являются частью подсети, какие сети используют частные адреса, какие используют общедоступные и многие другие определяющие факторы.

При планировании подсетей необходимо учитывать требования организации к использованию сети и предполагаемую структуру подсетей:

1. Выполните исследование требований к сети, изучив всю сеть, чтобы определить, как каждая область будет сегментирована.
2. Определите количество доступных адресов узлов и количество необходимых подсетей.
3. Определите пулы адресов DHCP и пулы VLAN.

7.9. ПРОЕКТИРОВАНИЕ СЕТИ
7.9.2. НАЗНАЧЕНИЕ АДРЕСОВ УСТРОЙСТВ

В сети существуют устройства различных типов, которым нужны адреса, включая следующие:

Конечные пользователи – большинство из них используют DHCP для уменьшения количества ошибок и нагрузки на персонал службы поддержки сети. Клиенты IPv6 могут получить сведения об адресе с помощью DHCPv6 или SLAAC.

Серверы и периферийные устройства – они должны иметь предсказуемый статический IP-адрес.

Серверы, доступные из Интернета – серверы должны иметь публичный IPv4 адрес, к которому чаще всего обращаются с помощью NAT.

Промежуточные устройства – таким устройствам адреса назначаются для управления сетью, ее мониторинга и обеспечения безопасности.

Шлюз – маршрутизаторы и устройства брандмауэра являются шлюзом для узлов в этой сети.

При проектировании схемы IP-адресации обычно рекомендуется использовать готовый шаблон назначения адресов каждому типу устройств.

ВОПРОСЫ ДЛЯ ПРОВЕРКИ

1. Для чего нужна маска посети?
2. Какие бывают виды рассылок?
3. Что из себя представляют частные и публичные IP-адреса?
4. Для чего используются адреса обратной петли и локальные адреса каналов?
5. В чем суть традиционной классовой адресации?
6. Какое устройство ограничивает широковещательную рассылку?
7. Для чего необходимо делить сети на подсети?
8. Какие формулы используются для разбиения на подсети?
9. Что из себя представляет технология VLSM?
10. Какие факторы нужно использовать при планировании адресации сети?