Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационной безопасности

Кафедра защиты информации

Е. С. Белоусова

АДРЕСАЦИЯ В IPV4- И IPV6-СЕТЯХ. ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях»

Минск БГУИР 2022

УДК 004.77(076)
ББК 32.971.35я73
Б43

Р е ц е н з е н т ы:

кафедра телекоммуникационных систем
учреждения образования «Белорусская государственная академия связи»
(протокол №2 от 29.09.2021);

доцент кафедры правовой информатики
учреждения образования «Академия МВД Республики Беларусь»
кандидат технических наук, доцент Н. М. Бобович

Белоусова, Е. С.

Б43 Адресация в IPv4- и IPv6-сетях. Практикум : учеб.-метод. пособие / Е. С. Белоусова. – Минск : БГУИР, 2022. – 78 с. : ил.

ISBN 978-985-543-673-8.

Состоит из восьми практических работ, содержащих краткие теоретические сведения, примеры для выполнения практических заданий, вопросы для самоконтроля, ответы на которые оцениваются программной экспертной системой.

Предназначено для студентов, изучающих дисциплину «Маршрутизация в информационных сетях».

УДК 004.77(076)
ББК 32.971.35я73

ISBN 978-985-543-673-8

СОДЕРЖАНИЕ

ПРАКТИЧЕСКАЯ РАБОТА №1
КОНВЕРТАЦИЯ IPV4-АДРЕСОВ

Цель: научиться представлять IPv4-адреса в двоичной системе счисления (СС), овладеть навыками перевода двоичного представления IPv4-адреса в десятичную форму представления.

1.1 Теоретическая часть

Адресация – это основная функция протоколов сетевого уровня, которая позволяет узлам обмениваться данными вне зависимости от того, находятся ли узлы в одной или нескольких сетях.

Чтобы устройства обнаружили друг друга и установили сквозное подключение по сети Интернет, используются IP-адреса, существует два стандарта адресов: IPv4 и IPv6. Фактически IP-адреса обеспечивают связь между устройствами от источника до назначения и обратно в любом сетевом взаимодействии. Структура адреса IPv4 – это точечно-десятичное представление в виде четырёх десятичных чисел в диапазоне от 0 до 255. Они имеют логическую природу, поскольку предоставляют информацию о местоположении устройства.

IP-адреса могут быть присвоены физическим портам и виртуальным интерфейсам на всех устройствах. Виртуальный интерфейс означает, что с данным устройством не связано дополнительное физическое оборудование.

Для понимания принципа работы устройств в сети необходимо рассматривать адресацию в том виде, в которой используют её устройства. Для этого необходимо перевести IP-адрес из десятичного представления с точками в двоичное значение.

В IP-сетях адрес представлен с помощью серии из 32 бит (единиц и нулей), разделенных на 4 октета, каждый из которых по 8 бит или 1 байту (рисунок 1.1). Такое представление адреса называется десятично-точечной нотацией. Каждый октет представляет собой 1 байт десятичного числа от 0 до 255.

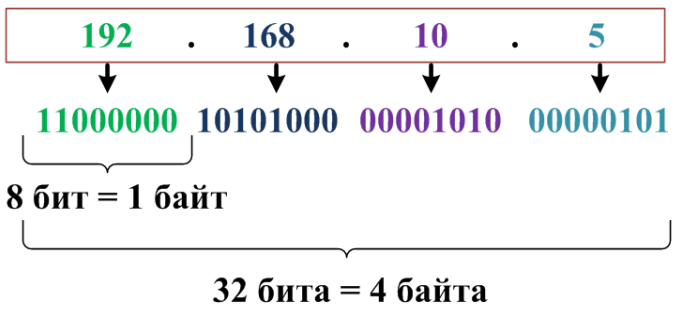

Рисунок 1.1 – Представление IPv4-адреса в двоичной системе счисления

Большинству людей сложно понять строку из 32 бит и тем более сложно её запомнить. Поэтому вместо двоичной системы для представления IPv4-адресов используется десятичный формат с разделительными точками.

В позиционном представлении цифра представляет разные значения в зависимости от своего расположения. Основанием системы позиционного представления является корень. В десятичной системе корнем является 10. Корень для двоичной системы – 2. Значение, представленное цифрой, умножается на основание, или корень, который представлен позицией, занимаемой цифрой. Например, для десятичного числа 192 единица (1) представляет значение $1 \cdot 10^2$. Единица находится на позиции сотни (100). Позиционное представление передаёт эту позицию как основание 2, поскольку основание – это 10, а степень – это 2. Цифра 9 представлена как $9 \cdot 10^1$. С помощью позиционного представления в системе счисления с корнем 10 число 192 представлено следующим образом: $192 = 1 \cdot 10^2 + 9 \cdot 10^1 + 2 \cdot 10^0$. Корнем для двоичной системы счисления является 2. Таким образом, каждое расположение представляет значение в степени 2. В 8-битных двоичных числах расположения представлены в таблице 1.1.

Таблица 1.1 – Представление десятичного числа 168 в двоичной системе счисления

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
1	0	1	0	1	0	0	0

В таблице 1.1 показано представление десятичного числа 168 в двоичном формате. Единица (1) в определённой позиции означает, что это значение должно учитываться в общей сумме. При сложении 128+32+8 получаем сумму 168_{10}, в двоичной системе счисления 10101000_2. В представленных значениях 168_{10} и 10101000_2 индексы означают систему счисления, десятичную и двоичную соответственно. Для преобразования IPv4-адрес из двоичной системы счисления необходимо выполнить следующие действия (рисунок 1.2).

1. Разделить 32 бита на 4 октета.
2. Преобразовать каждый октет в десятичное число.
3. Добавить «точку» между десятичными числами.

Аналогичным образом производится преобразование маски подсети.

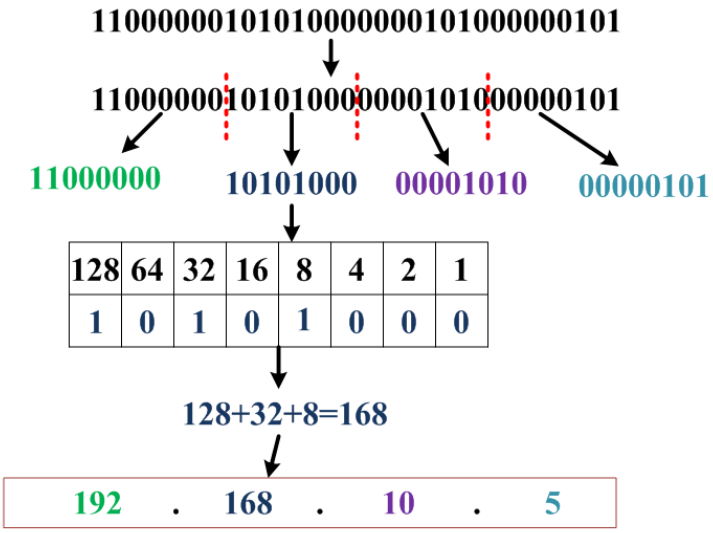

Рисунок 1.2 – Представление IPv4-адреса в десятичной системе счисления

1.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. Осуществить преобразование десятичных чисел в двоичные. В соответствии с шифром из таблицы 1.2 выбрать десятичные числа и осуществить их преобразование в двоичную СС. Результаты перевода представить в виде таблицы 1.3.

Таблица 1.2 – Десятичные числа для перевода в двоичную СС

Номер второй цифры шифра	Десятичные числа для перевода в двоичную СС	Номер третьей цифры шифра	Десятичные числа для перевода в двоичную СС
0	30; 68; 213; 108	0	27; 60; 206; 101
1	27; 75; 107; 153	1	115; 58; 39; 254
2	39; 62; 245; 143	2	22; 44; 73; 234
3	72; 54; 101; 219	3	65; 9; 208; 173
4	41; 69; 224; 98	4	45; 35; 135; 215
5	81; 29; 248; 115	5	243; 19; 88; 149
6	24; 104; 48; 159	6	85; 93; 116; 252
7	114; 151; 19; 79	7	25; 95; 168; 225
8	18; 82; 219; 170	8	49; 71; 182; 239
9	221; 103; 58; 94	9	36; 82; 172; 204

Таблица 1.3 – Представление результатов перевода из одной СС в другую

Десятичное число	Результат перевода в двоичную СС	Двоичное число	Результат перевода в десятичную СС

2. Осуществить преобразование двоичных чисел в десятичные. В соответствии с шифром из таблицы 1.4 выбрать двоичные числа и осуществить их преобразование в десятичную СС. Результаты перевода представить в виде таблицы 1.3.

Таблица 1.4 – Двоичные числа для перевода в десятичную двоичную СС

Номер первой цифры шифра	Двоичные числа для перевода в десятичную СС	Номер второй цифры шифра	Двоичные числа для перевода в десятичную СС
0	00011101; 00111110 11010011; 01101001	0	00100001; 00001110 10001011; 10110001
1	01101111; 00111011 00100101; 11111101	1	00011100; 01001001 01101100; 10011100
2	00010101; 00100010 00111111; 11101110	2	00100101; 01000001 11111000; 10010111
3	00110111; 00000111 11001110; 10001000	3	01001010; 00111000 01100111; 11100001
4	00101010; 00100001 10000101; 11010110	4	00101100; 01000111 11100100; 01100011
5	11101001; 00001111 01010001; 10010010	5	01010010; 00011110 11110011; 01110001
6	01001011; 01011100 01101010; 11111011	6	00011100; 01100110 00101010; 10011010
7	00010111; 01011101 10011110; 11111010	7	01110000; 10000011 00010100; 01010000
8	00111011; 01010001 10101100; 11111001	8	00010011; 01010011 11011100; 10101011
9	00100011; 01010000 10011111; 11001110	9	11011110; 10101001 00110101; 01011111

3. Перевести IP-адреса в двоичный эквивалент. В соответствии с шифром из таблицы 1.5 выбрать IP-адреса и осуществить их преобразование в двоичную СС. Результаты перевода представить в виде таблицы 1.6.

Таблица 1.5 – IP-адреса для перевода в десятичную СС

Номер третьей цифры шифра	IP-адреса
0	192.168.100.245; 255.255.248.0; 10.29.165.75; 172.18.215.136
1	192.168.114.224; 255.255.252.0; 10.145.156.20; 172.20.241.86
2	192.168.127.36; 255.255.255.240; 10.250.128.15; 172.29.228.156
3	192.168.186.125; 255.255.224.0; 10.25.165.40; 172.25.12.169
4	192.168.85.135; 255.255.255.192; 10.112.220.86; 172.31.52.175
5	192.168.77.168; 255.128.0.0; 10.244.58.39; 172.26.142.56
6	192.168.52.79; 255.255.255.128; 10.185.68.145; 172.17.150.38
7	192.168.147.2; 255.255.255.224; 10.99.172.19; 172.19.65.25
8	192.168.250.93; 255.255.255.248; 10.54.92.203; 172.30.64.193
9	192.168.46.249; 255.255.255.252; 10.27.86.227; 172.16.54.129

Таблица 1.6 – Результат перевода IPv4-адреса в двоичную СС

IP-адрес в десятичной СС	IP-адрес в двоичной СС

4. Перевести двоичные числа в IPv4-адрес. В соответствии с шифром из таблицы 1.8 выбрать двоичные числа и осуществить их преобразование в IPv4-адрес. Результаты перевода представить в виде таблицы 1.7.

Таблица 1.7 – Результат перевода двоичного числа в IPv4-адрес

Двоичное число	IP-адрес в десятичной СС

Таблица 1.8 – Двоичные числа для перевода в IP-адреса

Номер третьей цифры шифра	Двоичные числа
0	10101100010001010000101000011010; 11000000101010000011010001001111; 11111111111111111111111111110000; 00001010101110010100010010010001
1	11000000101010000010111011111001; 11111111111111111111111111000000; 00001010011100001101110001010110; 10101100000100000011011010000001
2	11000000101010000101010110000111; 11111111100000000000000000000000; 00001010000111011010010101001011; 10101100000110101000111000111000
3	11111111111111111111111111111100; 11000000101010001001001100000010; 00001010111101000011101000100111; 11000000101010000110010011110101
4	11111111111111111110000000000000; 11000000101010000111001011100000; 10101100000101001111000101010110; 00001010000110110101011011100011
5	11111111111111111111111111111000; 00001010011000111010110000010011; 10101100000100101101011110001000; 11000000101010000111111100100100
6	11111111111111111111100000000000; 00001010111110101000000000001111; 11000000101010000101010110000111; 10101100000110010000110010101001
7	11111111111111111111111111000000; 11000000101010001011101001111101; 00001010100100011001110000010100; 10101100000100011001011000100110
8	11000000101010000100110110101000; 11111111111111111111110000000000; 10101100000111110011010010101111; 00001010000110011010010100101000
9	10101100000100110100000100011001; 11111111111111111111111111100000; 00001010001101100101110011001011; 10101100000111011110010010011100

1.3 Содержание отчёта

1. Цель работы, исходные данные из таблиц 1.2, 1.4, 1.5, 1.8.
2. Результаты произведённых вычислений (заполненные таблицы 1.3, 1.6, 1.8).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

1.4 Контрольные вопросы

1. Как представляется IPv4-адрес?
2. Что такое октет?
3. Как перевести десятичное значение в двоичное?
4. Как осуществляется преобразование IPv4-адреса из двоичной системы счисления?

ПРАКТИЧЕСКАЯ РАБОТА №2
СЕТЕВАЯ И УЗЛОВАЯ ЧАСТЬ IPV4-АДРЕСА

Цель: овладеть навыками определения адреса сети, первого IP-адреса сети и широковещательного адреса.

2.1 Теоретическая часть

IP-адрес является иерархическим адресом и состоит из двух частей: сетевой и узловой. При настройке оконечного устройства ему присваивается не только IP-адрес, но и маска подсети. Маска, так же как и IP-адрес, состоит из 32 бит и определяет, какая часть IP-адреса относится к сети и к узлу. Маска подсети для простоты использования также представляется в десятичном формате с разделительными точками. Маска подсети настраивается на узловом устройстве в сочетании с IPv4-адресом и необходима для того, чтобы узел мог определить, к какой сети он принадлежит. Для этого устройство сравнивает маску с IP-адресом побитно, слева направо, единицы в маске соответствуют сетевой части, а нули – адресу узла. Таким образом, в маске подсети единицы в каждой позиции бита обозначают сетевую часть. Размещение нуля в каждой позиции бита маски подсети обозначает узловую часть IP-адреса (рисунок 2.1). Необходимо отметить, что маска подсети не содержит сетевую или узловую часть IPv4-адреса; она необходима устройствам для определения узловой и сетевой части в IPv4-адресах.

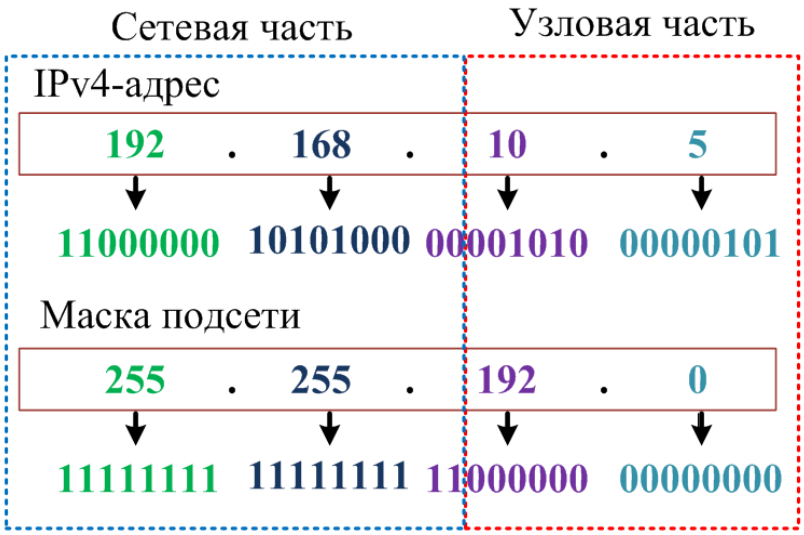

Рисунок 2.1 – Сетевая и узловая часть IPv4-адреса

Биты в сетевой части адреса должны быть одинаковыми для всех устройств, которые находятся в одной и той же сети. Биты в узловой части адреса должны быть уникальными, чтобы можно было определить конкретный узел в сети. Независимо от того, совпадают ли десятичные числа в двух IPv4-адресах, если два узла имеют одну битовую комбинацию в определённой

сетевой части 32-битного потока, то эти два узла находятся в одной и той же сети.

Префикс – это способ представления маски подсети. Значение префикса означает количество бит, установленных в единицу в маске подсети. Она обозначается наклонной чертой вправо («/»), после которой идёт набор единиц. Например, если маска подсети 255.255.255.0, то в двоичной версии маски подсети первые 24 бита единицы, поэтому значение префикса составляет 24 бита и обозначается /24. Например, для адреса 192.168.10.5 на рисунке 2.1 префикс может обозначаться следующим образом: /18, так как 18 первых бит в маске подсети установлены в единицу. По сути, назначение префикса и маска подсети одинаковое – представление сетевой части адреса.

В зависимости от количества узлов в сети префикс может различаться. Различный префикс приводит к изменению диапазона узлов и широковещательного адреса для каждой сети.

В сети узлы могут взаимодействовать одним из трёх следующих способов:

– **одноадресная рассылка** – процесс отправки пакета с одного узла на другой;

– **широковещательная рассылка** – процесс отправки пакета с одного узла на все узлы в сети;

– **многоадресная рассылка** – процесс отправки пакета с одного узла выбранной группе узлов.

Эти три типа связи используются в сетях передачи данных для различных целей. Во всех трёх типах IPv4-адрес исходного узла размещён в заголовке пакета в качестве адреса источника.

Одноадресная передача используется для обычного обмена данными между узлами. Для одноадресной рассылки пакетов в качестве адреса назначения используются адреса целевого устройства. Во время процесса инкапсуляции исходный узел размещает свой IPv4-адрес в заголовке пакета одноадресной рассылки в качестве адреса источника, а IPv4-адрес узла назначения – в заголовке пакета в качестве адреса назначения.

В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы. Это означает, что пакеты получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих сетевых протоколах, например в протоколе DHCP. Когда узел получает пакет, отправленный на сетевой широковещательный адрес, узел обрабатывает этот пакет так же, как обрабатывает пакет, отправленный по одноадресной рассылке.

Многоадресная передача предназначена для сохранения пропускной способности IPv4-сети. Такая передача сокращает трафик, позволяя узлу отправлять один пакет выбранной группе узлов, которые являются частью подписной группы мультивещания. Чтобы достичь множества целевых узлов с помощью одноадресной связи, узел-источник должен отправлять отдельный

пакет на каждый адрес. В случае с многоадресной рассылкой узел-источник может отправлять один пакет, который достигает нескольких тысяч узлов назначения.

Независимо от того, является ли пункт назначения, определивший пакет, одноадресным, широковещательным или многоадресным, источник всегда является индивидуальным адресом исходного узла.

В каждой сети IPv4 существуют три типа адресов:

– сетевой адрес;

– узловые адреса;

– широковещательный адрес

Сетевой адрес – это стандартный способ обозначения сети. Маска подсети или префикс используются при обозначении сетевого адреса. Например, сеть, показанную на рисунке 2.2, можно обозначить как 192.168.10.0 255.255.255.0 или 192.168.10.0/24. Все узлы в сети 192.168.10.0/24 будут иметь одинаковую сетевую часть.

Как показано на рисунке 2.2, в диапазоне IPv4-адресов первый из них (192.168.10.0) зарезервирован для обозначения всей сети в целом. В каждом узловом бите узловой части адреса указан нуль.

Для обмена данными по сети каждому оконечному устройству необходим уникальный адрес. В IPv4-адресах значения между сетевым и широковещательным адресами могут быть назначены оконечным устройствам в сети. Как показано на рисунке 2.2, в узловой части этот адрес может иметь любую комбинацию нулей и единиц, но при этом не может состоять только из нулей или только из единиц. Таким образом для примера сети, показанном на рисунке 2.2, узловые адреса могут иметь значение в последнем октете от 1 до 254. Обычно первый IP-адрес присваивается устройству, ограничивающему данную сеть (маршрутизатор).

Широковещательный IPv4-адрес – это особый адрес для каждой сети, который осуществляет связь для всех узлов, расположенных в этой сети. Для единовременной отправки данных на все узлы в сети узел может отправить один пакет, назначенный широковещательному адресу сети, а каждый узел в этой сети, который получит этот пакет, обработает его содержимое.

Для широковещательной рассылки используется наивысший адрес диапазона сети. В этом адресе все части узла представлены единицами (1). Сумма единиц октета в двоичной форме равняется значению 255 в десятичном формате. Таким образом, для сети 192.168.10.0/24, в которой последний октет используется для узловой части, широковещательный адрес будет равен 192.168.10.255. Также этот адрес называют прямой широковещательной рассылкой. Необходимо отметить, что узловая часть не всегда представлена всем октетом целиком.

Чтобы не возникало проблем в сети, всем узлам в сети назначается уникальный IP-адрес внутри диапазона сети, для этого важно уметь определять адреса первого и последнего узлов. Узловая часть первого адреса узла будет содержать все нулевые биты с единицей в крайнем справа бите (рисунок 2.3).

Значение этого адреса всегда на единицу больше сетевого адреса. Часто во многих схемах адресации первый адрес узла используется для маршрутизатора или шлюза по умолчанию.

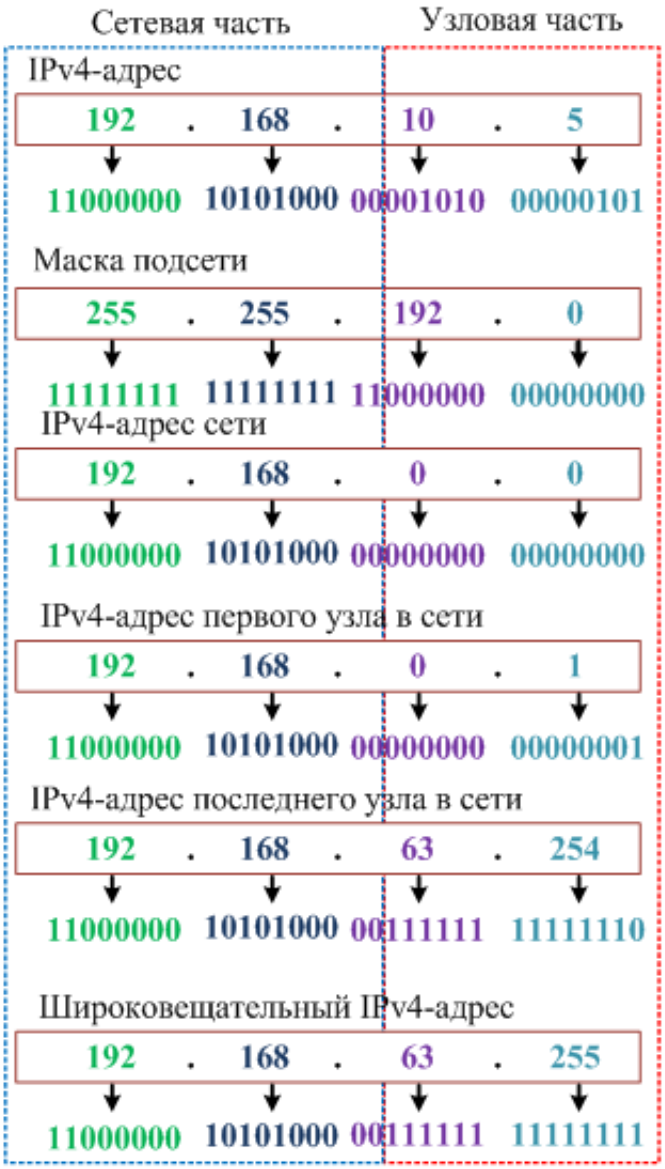

Рисунок 2.2 – Определение первого и широковещательного IPv4-адреса

Узловая часть последнего адреса узла будет содержать все единицы с нулём в крайнем справа бите. Значение этого адреса всегда на единицу меньше, чем значение широковещательного адреса. Как видно на рисунке 2.2, последним адресом узла в сети 192.168.10.0/24 является 192.168.63.254.

Если устройству назначен IPv4-адрес, то это устройство использует маску подсети, чтобы определить, к какому сетевому адресу оно принадлежит. Сетевой адрес представляет все устройства в одной и той же сети.

При отправке данных по сети устройство использует эту информацию, чтобы определить, может ли оно пересылать пакеты локально, либо оно должно отправлять пакеты на шлюз по умолчанию для удалённой отправки. Когда узел

отправляет пакет, он сравнивает сетевые части собственного IP-адреса и IP-адреса назначения, который зависит от маски подсети. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если биты не совпадают, отправляющий узел передаёт пакет на шлюз по умолчанию для отправки в другую сеть. Для определения способа отправки устройство использует операцию дискретной логики логическое умножение (операция **AND**), которая заключается в сравнение двух бит, как показано на рисунке 2.3. Например, 1 AND 1 = 1, 0 AND 1 = 0, 0 AND 0 = 0.

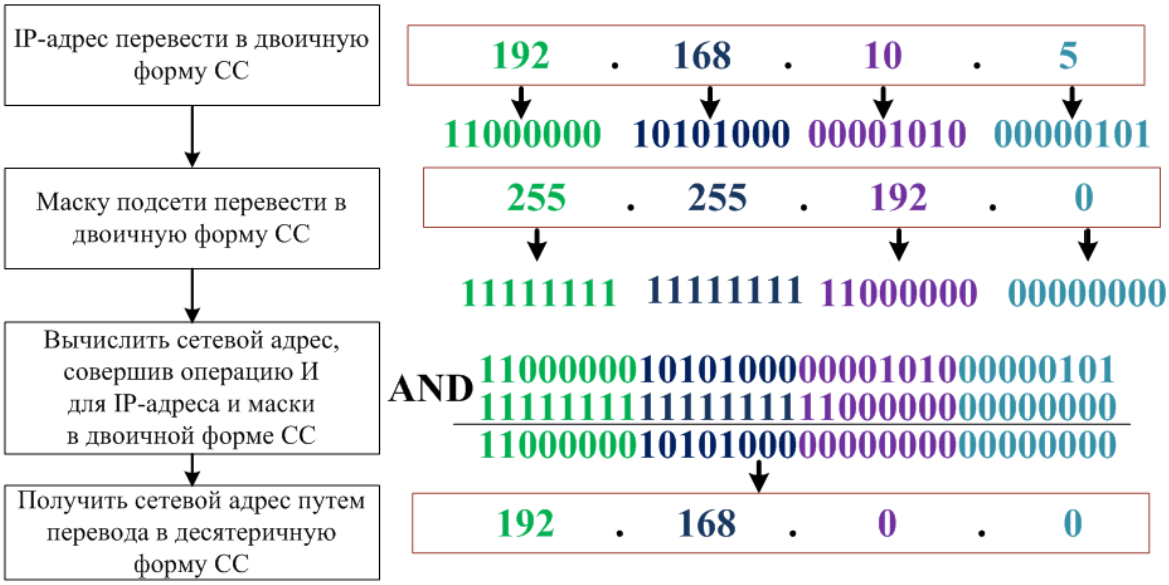

Рисунок 2.3 – Вычисление сетевого адреса

2.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. Определить первый, широковещательный адреса и адрес сети. В соответствии с шифром из таблицы 2.1 выбрать IP-адреса и маски сети и определить адрес подсети, IP-адрес первого узла, широковещательный IP-адрес. Результаты представить в виде таблицы 2.2.

Таблица 2.1 – IP-адреса для расчёта широковещательного адреса и адреса сети

Номер первой цифры шифра	IP-адреса и маски подсети
0	192.168.100.245; 255.255.248.0
	10.29.165.75; 255.128.0.0
	172.18.215.253; 255.255.255.252
1	192.168.114.224; 255.255.224.0
	10.145.156.20; 255.192.0.0
	172.20.241.86; 255.255.252.0

Продолжение таблицы 2.1

Номер первой цифры шифра	IP-адреса и маски подсети
2	192.168.127.180; 255.255.255.128
	10.250.128.15; 255.224.0.0
	172.29.228.248; 255.255.255.240
3	192.168.186.125; 255.255.224.0
	10.25.165.40; 255.128.0.0
	172.25.12.169; 255.255.254.0
4	192.168.85.200; 255.255.255.192
	10.112.220.86; 255.254.0.0
	172.31.52.175; 255.255.128.0
5	192.168.77.254; 255.255.255.254
	10.244.58.39; 255.255.128.0
	172.26.142.56; 255.255.248.0
6	192.168.52.250; 255.255.255.248
	10.185.68.145; 255.254.0.0
	172.17.150.156; 255.255.255.128
7	192.168.147.106; 255.255.255.192
	10.99.172.19; 255.248.0.0
	172.19.65.248; 255.255.255.224
8	192.168.250.93; 255.255.255.128
	10.54.92.203; 255.255.224.0
	172.30.64.193; 255.255.248.0
9	192.168.46.249; 255.255.255.252
	10.27.86.227; 255.240.0.0
	172.16.54.129; 255.255.192.0

Таблица 2.2 – Результаты расчёта IP-адресов

IP-адрес	В двоичной СС	В десятичной СС
Маска подсети		
IP-адрес с префиксом		
IP-адрес сети		
IP-адрес первого узла		
Широковещательный IP-адрес		

2. В соответствии с шифром из таблицы 2.3 выбрать IP-адреса и определить адрес подсети, IP-адрес первого узла, широковещательный IP-адрес. Результаты представить в виде таблицы 2.2.

Таблица 2.3 – IP-адреса для расчёта первого, широковещательного адреса и адреса сети

Номер третьей цифры шифра	IP-адреса
0	173.179.151.62/20, 140.147.4.238/18
1	163.45.1.121/24, 168.104.172.159/20
2	190.237.151.164/30, 179.164.136.1/19
3	145.32.213.117/18, 131.236.49.174/29
4	162.122.225.45/29, 170.121.0.247/30
5	149.67.24.168/21, 166.153.154.229/26
6	159.48.222.146/18, 161.58.20.38/28
7	143.142.244.138/21,135.8.119.158/29
8	172.42.243.160/23, 154.127.142.142/30
9	157.213.37.23/25, 137.165.250.44/16

2.3 Содержание отчёта

1. Цель работы, исходные данные из таблиц 2.1, 2.3.
2. Результаты вычислений IP-адресов (заполненная таблица 2.2 для всех заданных IP-адресов из таблиц 2.1, 2.3).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

2.4 Контрольные вопросы

1. Как определить IPv4-адрес сети по IPv4-адресу и маске подсети?
2. Что такое сетевая и узловая части IPv4-адреса?
3. В чём заключается назначение префикса IPv4-адреса?
4. Как осуществляется взаимодействие устройств в сети?
5. Какие выделяют типы адресов IPv4?
6. Что такое широковещательный адрес сети? Как он определяется?
7. Как используется операция AND для отправки пакетов в другие сети?

ПРАКТИЧЕСКАЯ РАБОТА №3
КЛАССИФИКАЦИЯ IP-АДРЕСОВ

Цель: изучить классификацию IP-адресов, научиться определять тип IPv4-адреса и его класс.

3.1 Теоретическая часть

Классовая IP-адресация – это метод IP-адресации, который не позволяет рационально использовать ограниченный ресурс уникальных IP-адресов, т. к. невозможно использование различных масок подсетей. В классовом методе адресации используется фиксированная маска подсети, поэтому класс сети всегда можно идентифицировать по первым битам.

В соответствии с документом RFC1700 все IPv4-адреса сгруппированы в диапазоны (рисунок 3.1), которые называются классами A, B, C, D (групповые), E (экспериментальные). К классам A, B и C относятся коммерческие адреса, присваиваемые узлам. Индивидуальным адресам классов A, B и C определены сети особого размера и блоки особых адресов для этих сетей. Компании или организации назначается целая сеть из блоков адресов класса A, B или C.

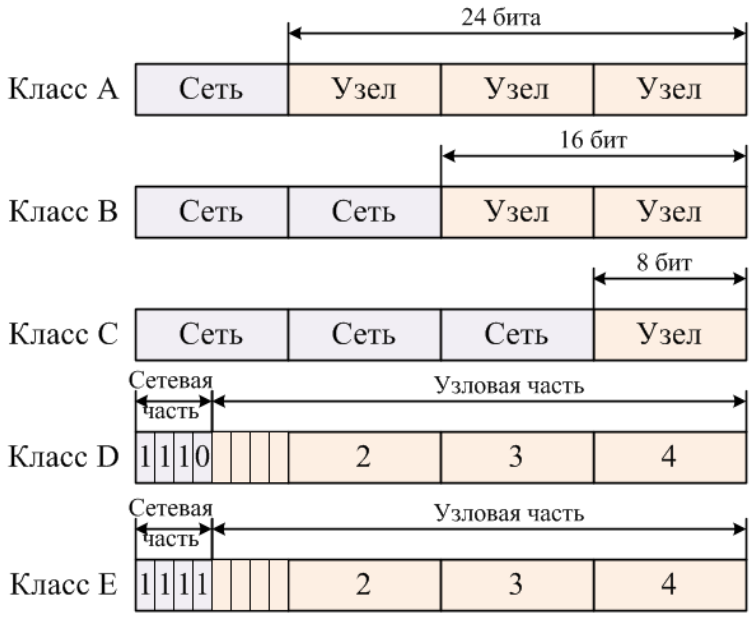

Рисунок 3.1 – Классы IPv4-адресов

Блок адресов класса A разработан для поддержки очень крупных сетей, содержащих более чем 16 миллионов адресов узлов. Для обозначения сетевого адреса IPv4-адреса класса A использовали фиксированный префикс /8 с первым октетом. Остальные три октета использовались для адресов узлов. Все адреса класса A требуют, чтобы самый старший разряд старшего октета был равен нулю. Это означает, что существовало только 128 возможных сетей класса A, от 1.0.0.0/8 до 127.0.0.0 /8 (таблица 3.1). Даже если адреса класса A

зарезервировали половину адресного пространства, в связи с их ограничением до 128 сетей они могут быть назначены только приблизительно 120 компаниям или организациям.

Адресное пространство класса B разработано для поддержки потребностей небольших и крупных сетей, содержащих приблизительно 65 000 узлов. IP-адрес класса B использовал два старших октета для обозначения сетевого адреса. Оставшиеся два октета определяли адреса узлов. Как и в случае с классом A, адресное пространство для оставшихся классов адресов должно быть зарезервированным. Для адресов класса B два самых старших разряда старшего октета равны 10. Это ограничивает блок адресов для класса B от 128.0.0.0/16 до 191.255.0.0/16 (см. таблицу 3.1). Назначение адресов класса B немного более эффективно по сравнению с классом A, поскольку 25 % его общего пространства IPv4-адресов было разделено среди примерно 16 000 сетей.

Адресное пространство класса C было доступно чаще всех остальных классов адресов. Это адресное пространство предназначено для предоставления адресов небольшим сетям с максимальным количеством узлов не более 254. Блоки адресов класса C использовали префикс /24. Это означает, что сеть класса C использовала только последний октет в качестве адресов узлов с тремя старшими октетами, используемыми для обозначения сетевых адресов. Блоки адресов класса C отделяли адресное пространство с помощью фиксированного значения 110 самых старших разрядов старшего октета. Это ограничило блок адресов класса C от 192.0.0.0/24 до 223.255.255.0/24 (см. таблицу 3.1). Хотя этот блок занял только 12,5 % от общего объёма адресного IPv4-пространства, он предоставил адреса 2 миллионам сетей.

Таблица 3.1 – Диапазон первого октета классов адресов

Класс адреса	Диапазон первого октета в десятичном формате	Маска подсети
A	1.0.0.0/8 – 127.255.255.255/8	255.0.0.0
B	128.0.0.0/16 – 191.255.255.255/16	255.255.0.0
C	192.0.0.0/24 – 223.255.255.255/24	255.255.255.0
D	224.0.0.0/4 – 239.255.255.255/4	240.0.0.0
E	240.0.0.0/4 – 255.255.255.255/4	240.0.0.0

На сегодняшний день более распространено разделение IPv4-адресов на публичные и частные. Подавляющее большинство адресов в диапазоне узлов одноадресной IPv4-рассылки являются публичными адресами. Эти адреса предназначены для использования в узлах с открытым доступом из Интернета. Даже в диапазоне этих блоков IPv4-адресов существует множество адресов, предназначенных для других особых целей.

Частные адреса определены в документе RFC 1918 «Присвоение адресов для частного Интернета». Узлы, которые не требуют доступа в Интернет, могут

использовать частные адреса. Узлы в различных сетях могут использовать одни и те же адреса частного пространства. Пакеты, использующие эти адреса в качестве источника или назначения, не должны появляться в публичном Интернете. Маршрутизатор должен блокировать или преобразовывать эти адреса. Даже если бы пакеты сами прокладывали свой путь через Интернет, у маршрутизаторов в любом случае не появилось бы маршрутов для пересылки их в соответствующую частную сеть.

В документе RFC 6598 IANA (Администрация адресного пространства Интернет) зарезервировала другую группу адресов, которая называется общим адресным пространством. Так же как и в пространстве частных адресов RFC 1918, адреса общего адресного пространства недоступны глобально. Однако эти адреса предназначены только для использования в сетях операторов связи. Блок общих адресов – 100.64.0.0/10.

Таблица 3.2 – Диапазоны адресов для частных сетей

Класс адреса	Сети	Маска под-сети	Диапазон адресов
A	10.0.0.0	255.0.0.0	10.0.0.0 –10.255.255.255
B	172.16.0.0 – 172.31.0.0	255.240.0.0	172.16.0.0 – 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 – 192.168.255.255

Также существуют особые адреса, которые не могут быть назначены узлам, такие адреса называются сетевым и широковещательным.

К таким адресам также относится IPv4-адрес логического интерфейса loopback (127.0.0.1). Loopback – это особый адрес, который используют узлы, чтобы направлять трафик самим себе. Адрес обратной связи позволяет создавать ускоренный метод взаимодействия для приложений и сервисов TCP/IP, которые работают на одном и том же устройстве. С использованием loopback-адреса вместо назначенного IPv4-адреса узла два сервиса на одном узле могут обойти нижние уровни стека протоколов TCP/IP. Для проверки настройки TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес.

Хотя используется только адрес 127.0.0.1, резервируются адреса с 127.0.0.0 до 127.255.255.255. Любой адрес из этого блока даст обратную связь с локальным узлом. Ни один адрес из этого блока не должен быть назначен устройствам в сети.

В качестве локальных адресов канала используются IPv4-адреса в блоке адресов от 169.254.0.0 до 169.254.255.255 (169.254.0.0/16). Эти адреса могут быть автоматически присвоены операционной системой локальному узлу в средах, где настройка IP-сети недоступна. Они могут использоваться в небольшой одноранговой сети или для узла, который не может автоматически получить адрес от DHCP-сервера.

Коммуникация с помощью локальных IPv4-адресов подходит только для обмена данными с другими устройствами, подключёнными к той же сети. Узел не должен отправлять пакет с локальным IPv4-адресом назначения какому-либо маршрутизатору для пересылки. Локальные адреса не предоставляют сервисы за пределами локальной сети. Однако многие приложения типа клиент-сервер и одноранговые приложения будут работать надлежащим образом с локальными IPv4-адресами.

Адреса в блоке от 240.0.0.0 до 255.255.255.254 указаны в качестве зарезервированных для использования в будущем (RFC 3330). В настоящее время эти адреса могут использоваться только в исследовательских или экспериментальных целях, но не могут использоваться в IPv4-сети. Тем не менее в соответствии с документом RFC 3330 в будущем технически они могут быть преобразованы в доступные адреса.

Блок адресов от 192.0.2.0 до 192.0.2.255 (192.0.2.0/24) предназначен для обучающих и учебных целей. В отличие от экспериментальных адресов сетевые устройства принимают эти адреса в свои конфигурации.

Если необходимо определить, относятся ли к одной сети IP-адреса узлов, то необходимо выполнить следующие действия (рисунок 3.2).

1. Перевести IP-адреса в двоичную форму.
2. Перевести маску подсети в двоичную форму.
3. Осуществить операцию AND каждого IP-адреса с маской подсети.
4. Определить сетевой адрес для каждого IP-адреса.
5. Сравнить сетевые адреса.
6. Сделать вывод о том, какие IP-адреса находятся в одной сети.

3.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. В соответствии с шифром выбрать из таблицы 3.3 IP-адреса и маску подсети и определить IP-адреса, находящиеся в одной сети. Результаты оформить виде таблицы 3.4.

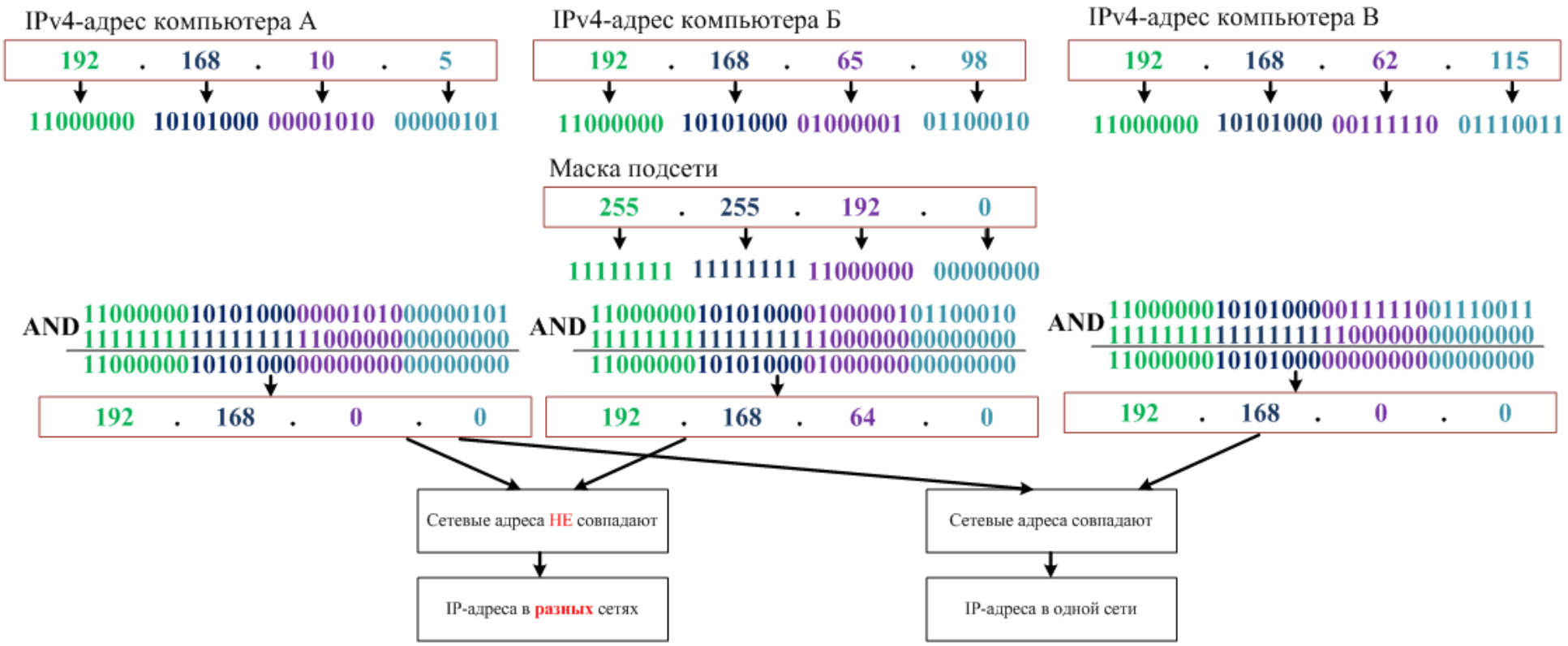

Рисунок 3.2 – Определение отношения IP-адресов к одной сети

Таблица 3.3 – IP-адреса для расчёта первого, широковещательного адреса и адреса сети

Номер третьей цифры шифра	IP-адреса	Маска подсети
0	10.145.156.20 10.192.115.20 10.177.156.20	255.192.0.0
1	172.29.228.248 172.29.228.252 172.29.288.231	255.255.255.240
2	192.168.127.180 192.168.127.192 192.168.127.225	255.255.255.224
3	10.99.172.19 10.115.127.225 10.95.245.225	255.248.0.0
4	10.112.220.45 10.112.207.245 10.112.211.244	255.255.240.0
5	192.168.186.241 192.168.192.241 192.168.160.241	255.255.224.0
6	172.30.64.193 172.30.72.105 172.30.71.180	255.255.248.0
7	172.19.65.248 172.19.65.215 172.19.65.225	255.255.255.224
8	10.27.125.45 10.33.125.45 10.31.125.51	255.240.0.0
9	192.168.85.200 192.168.85.195 192.168.85.191	255.255.255.192

Таблица 3.4 – Результаты сравнения IP-адресов

	Первый IP-адрес	Второй IP-адрес	Третий IP-адрес
В десятичном формате			
В двоичном формате			
Маска подсети в десятичном формате			
Маска подсети в двоичном формате			
Результат операции AND			
Сетевой адрес в десятичном формате			
IP-адреса в одной сети			

2. В соответствии с шифром выбрать из таблицы 3.5 IP-адреса и определить, какие из IP-адресов являются адресом сети, адресом оконечного устройства или адресом широковещательной рассылки. Результат оформить виде таблице 3.6.

Таблица 3.5 – IP-адреса для расчёта широковещательного адреса и адреса сети

Номер второй цифры шифра	IP-адреса
0	192.168.186.120/25, 172.29.228.248/28, 172.17.150.157/31
1	192.168.127.255/25, 192.168.85.31/27, 192.168.52.120/29
2	172.29.228.255/28, 172.18.215.253/30, 192.168.85.0/27
3	192.168.186.0/25, 192.168.52.127/29, 192.168.46.240/30
4	192.168.186.127/25, 172.29.228.240/28, 192.168.85.212/26
5	192.168.52.123/29, 172.19.65.25/30, 192.168.127.180/25
6	172.18.215.255/30, 172.17.150.156/31, 192.168.85.255/26
7	192.168.147.127/26, 192.168.85.26/27, 192.168.147.64/26
8	192.168.85.192/26, 192.168.46.241/30, 192.168.127.128/25
9	172.18.215.252/30, 192.168.46.243/30, 192.168.147.103/26

Таблица 3.6 – Результаты определения вида IP-адреса

Вид адреса	IP-адрес	Маска подсети
Адрес сети		
Широковещательный адрес		
Адрес узла		

3. Из таблицы 3.7 выбрать IP-адреса в соответствии с шифром и определить тип и класс IP-адреса. По результатам выполнения заполнить таблицу 3.8.

Таблица 3.7 – IP-адреса для определения типа и класса

Номер первой цифры шифра	IP-адреса
0	65.95.86.125/12, 172.15.20.45/14, 127.10.15.168/8, 168.254.15.65/16, 245.230.15.10/16
1	255.240.15.26/20, 192.0.2.25/24, 169.254.254.255/16, 127.20.254.220/8, 192.168.254.255/24
2	172.20.85.15/20, 192.168.248.255/28, 127.154.56.58/8, 169.254.156.2/16, 240.125.102.56/8
3	192.0.2.56/24, 10.25.15.56/16, 172.35.156.14/20, 127.250.56.8/16, 169.254.250.6/16
4	192.168.45.255/28, 10.125.26.12/16, 172.45.25.36/20, 127.0.1.2/8, 169.254.250.36/16
5	240.254.250.26/16, 169.254.250.2/16, 172.15.12.250/16, 192.168.10.250/30, 127.26.86.74/8
6	169.254.6.250/16, 127.25.26.250/16, 10.250.26.147/16, 240.250.26.45/8, 192.168.10.52/24
7	172.20.86.125/24, 192.0.2.250/24, 240.28.65.15/8, 169.254.0.5/16, 127.0.45.68/8
8	127.86.59.6/8, 169.254.25.63/16, 240.250.76.84/8, 192.168.10.5/16, 172.10.56.3/16
9	10.26.56.8/8, 172.16.20.46/8, 240.0.56.89/8, 169.254.0.250/16, 127.25.65.14/8

Таблица 3.8 – Результаты определения вида IP-адреса

IP-адрес	Класс	Тип

3.3 Содержание отчёта

1. Цель работы, исходные данные из таблиц 3.3, 3.5, 3.7.
2. Результаты произведённых настроек (заполненные таблицы 3.4, 3.6, 3.8).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

3.4 Контрольные вопросы

1. Какие выделяют классы IPv4-адресов?
2. В чём заключается назначение классов E и D?
3. В чём отличие частных и публичных IPv4-адресов?
4. Что такое логический интерфейс loopback?
5. Какие IPv4-адреса относятся к локальным?
6. Что такое зарезервированные IPv4-адреса и адреса для учебных целей?
7. Какая последовательность действий при проверке IPv4-адресов на принадлежность к одной сети?

ПРАКТИЧЕСКАЯ РАБОТА №4
РАЗБИЕНИЕ СЕТЕЙ IPV4 НА ПОДСЕТИ

Цель: изучить принципы разделения IPv4-сетей на подсети, овладеть навыками расчёта IPv4-адресов подсетей.

4.1 Теоретическая часть

Разбиение на подсети – это процесс сегментации сети путём разделения её на несколько более мелких сетей, которые называют подсетями. Устройства и службы в подсети можно группировать по их географическому местоположению, подразделениям или по типу устройств. Разбиение на подсети может снизить общую нагрузку на сеть и повысить её производительность.

Подсети образуют несколько логических сетей из одного блока адресов или сетевого адреса. Каждая подсеть – это отдельное сетевое пространство. Устройства в одной подсети должны использовать адрес, маску подсети и шлюз по умолчанию той подсети, которой они принадлежат. Каждый сетевой адрес содержит допустимый диапазон адресов узлов. Все устройства, подключённые к одной и той же сети, будут иметь IPv4-адрес узла этой сети, а также общую маску подсети или префикс сети. При планировании и создании IPv4-подсетей используется один или нескольких бит из узловой части в качестве бита сетевой части. Чем больше заимствовано бит из узловой части, тем больше подсетей можно создать. Для каждого заимствованного бита количество доступных подсетей удваивается. Например, если заимствовать один бит, можно создать 2 подсети, для двух бит – 4 подсети, для трёх бит – 8 подсетей и т. д. Однако с каждым заимствованным битом уменьшается количество адресов узлов в каждой подсети. Биты могут быть заимствованы только из узловой части адреса. Сетевая часть адреса выделяется оператором связи, и изменить её невозможно.

Например, необходимо разделить сеть 192.168.10.0/24, у которой 24 бита в сетевой части и 8 бит в узловой части, что обозначено маской подсети 255.255.255.0 (рисунок 4.1) или записью с префиксом /24. Без разделения на подсети эта сеть поддерживает работу только с одним интерфейсом локальной сети. Если нужна дополнительная локальная сеть, основную сеть нужно разделить на подсети. В самом старшем разряде четвертого октета заимствуется 1 бит в узловой части, тем самым маска сети расширяется до 25 бит. При этом создаются две подсети: первая определяется цифрой 0 в заимствованном бите, а вторая – цифрой 1 в заимствованном бите. Для маски подсети обеих сетей используется цифра 1 в заимствованном бите, чтобы показать, что этот бит теперь входит в сетевую часть адреса. Таким образом получается две подсети с адресами: 192.168.10.0/25 и 192.168.10.128/25. Поскольку был заимствован бит из узловой части, маска подсети для каждой подсети будет 255.255.255.128 или /25.

Рисунок 4.1 – Разбиение на подсети

Для организации разделения на подсети в локальной сети к маршрутизатору подключаются два сегмента сети. Каждому из интерфейсов маршрутизатора должен быть назначен IP-адрес в диапазоне допустимых адресов для разделенных подсетей. В качестве адреса интерфейса маршрутизатора рекомендуется использовать первый доступный адрес диапазона сети, для чего для каждой подсети необходимо рассчитать адреса, как показано в таблице 4.1. На рисунке 4.2 показан пример реализации разделения сети и конфигурация узла в одной из подсетей.

Таблица 4.1– Расчёт IP-адресов для подсетей

IP-адрес	Сеть №1	Сеть №2
Маска подсети	255.255.255.128	
IP-адрес с префиксом	192.168.10.0/25	192.168.10.128/25
IP-адрес сети	192.168.10.0	192.168.10.128
IP-адрес первого узла	192.168.10.1	192.168.10.129
IP-адрес последнего узла	192.168.10.126	192.168.10.254
Широковещательный IP-адрес	192.168.10.127	192.168.10.255

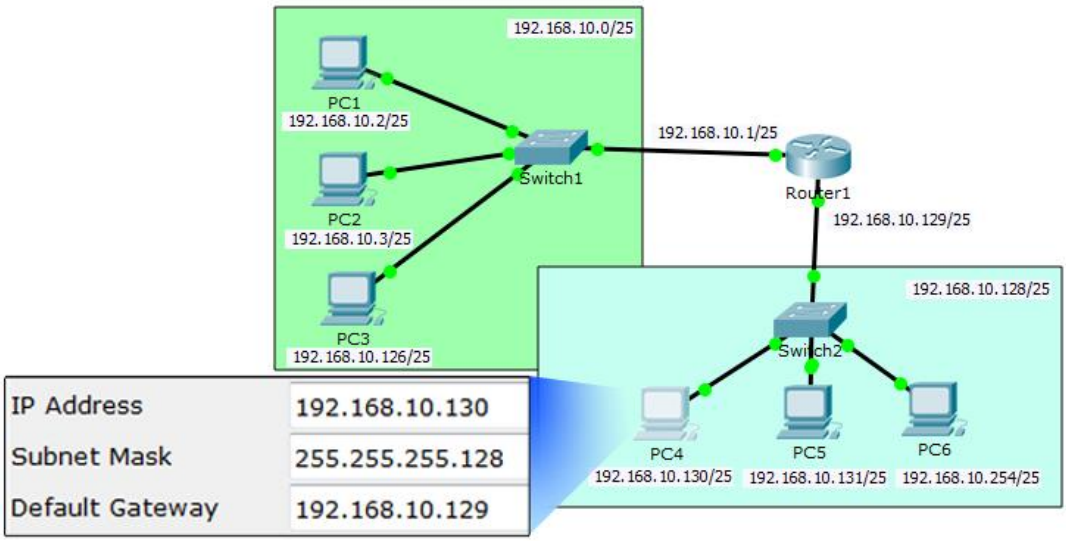

Рисунок 4.2 – Реализация разделения на подсети

При планировании подсетей необходимо определить её размер, оценить количество узлов, которым потребуются IP-адреса в каждой подсети в рамках разделённой частной сети. Для расчёта количества возможных подсетей в результате разделения используют формулу

$$K_{сетей} = 2^n, \quad (4.1)$$

где n – количество заимствованных бит в узловой части IPv4-адреса.

Для расчёта количества узлов в подсети используют формулу

$$K_{узлов} = 2^m - 2, \quad (4.2)$$

где m – количество оставшихся бит в узловой части IPv4-адреса.

В формуле (4.2) слагаемое 2^m обозначает общее количество узлов в сети. В сети присутствует адрес подсети и широковещательный адрес, которые нельзя присваивать устройствам, поэтому в формуле (4.2) от общего числа узлов необходимо вычесть 2 адреса. Таким образом, при разделение сети 192.168.10.0/24 получается 2 сети (192.168.10.0/25 и 192.168.10.128/25), т. к. берется 1 бит в узловой части, и 126 узлов для каждой подсети, т. к. 7 бит остается в узловой части. Однако при таком варианте разделения в случае появления новых подсетей необходимо будет произвести деление заново. Поэтому рекомендуется заранее учитывать будущее развитие сети, и при делении на подсети выделять дополнительно 1–2 подсети.

Рассмотрим вариант разделения сети 192.168.10.0/24 на 3 подсети. Для этого, исходя из формулы (4.1), необходимо взять 2 бита из узловой части и, таким образом, расширить маску подсети до значения 255.255.255.192. В итоге получается 4 подсети с адресами 192.168.10.0/26, 192.168.10.64/26, 192.168.10.128/26, 192.168.10.192/26. В каждой подсети, исходя из формулы (4.2), $K_{узлов} = 2^6 - 2 = 62$ узла. Расчёт IPv4-адресов для каждой подсети представлен в таблице 4.2. Такой вариант разделения сети удовлетворяет топологии сети, представленной на рисунке 4.2, и учитывает возможность расширения сети.

Таблица 4.2 – Расчёт IP-адресов для подсетей

IP-адрес	Сеть №1	Сеть №2	Сеть №3	Сеть №4
Маска подсети	255.255.255.192			
IP-адрес с префиксом	192.168.10.0/26	192.168.10.64/26	192.168.10.128/26	192.168.10.192/26
IP-адрес сети	192.168.10.0	192.168.10.64	192.168.10.128	192.168.10.192
IP-адрес первого узла	192.168.10.1	192.168.10.65	192.168.10.129	192.168.10.193
IP-адрес последнего узла	192.168.10.62	192.168.10.126	192.168.10.190	192.168.10.254
Широковещательный IP-адрес	192.168.10.63	192.168.10.127	192.168.10.191	192.168.10.255

Большинство компаний или организаций получают блоки IPv4-адресов от интернет-провайдеров. Обычно, помимо всех остальных услуг, провайдер предоставляет своим заказчикам небольшое количество доступных IPv4-адресов. По сути, провайдеры одалживают своим клиентам эти адреса. При смене интернет-провайдера новый поставщик услуг предоставляет адреса из своих адресных блоков, а предыдущий получает обратно свои адреса и выделяет их другому заказчику. Потому важно правильно распределять выделенные провайдером IP-адреса в сети, что называется планированием подсетей. При планировании подсетей следует рассмотреть два момента: количество адресов узлов, необходимых для каждой сети, и количество требуемых отдельных подсетей. Ключевым моментом является соотношение количества необходимых подсетей и количества узлов, требуемых для самой крупной подсети. Чем больше бит было заимствовано для создания дополнительных подсетей, тем меньше узлов будет доступно в каждой из подсетей.

Например, организации выделен IP-адрес 172.16.0.0/20, который нужно разделить на подсети в соответствии с топологией сети, представленной на рисунке 4.3. Для этого учитывается максимальное количество узлов в каждой сети. Порядок действий при разбиении сети на подсети представлен на рисунке 4.4.

В сети на рисунке 4.3 общее количество устройств составляет 890. В выделенном IPv4-адресе 172.16.0.0/20 для организации в узловой части 12 бит, в соответствии с формулой (4.2) такая сеть может содержать 4094 узла, что соответствует требованиям и сеть можно разделить на подсети. Выделенную сеть необходимо разделить на 5 подсетей, соответствующих сегментам локальной сети, и 4 подсети, относящиеся к соединениям между маршрутизаторами. Таким образом, требуется 9 подсетей. Наибольшее

количество узлов в сети №5 (210 узлов). Исходя из формулы (4.2), можно рассчитать, что для 210 узлов требуется выделить не менее 8 бит в узловой части, при этом в каждой сети будет 254 устройства, что будет достаточным для развитие каждой сети в будущем. Для сетевой части остается 4 бита, по формуле (4.1) можно определить, что можно создать 16 подсетей, что является достаточным для выполнения условий.

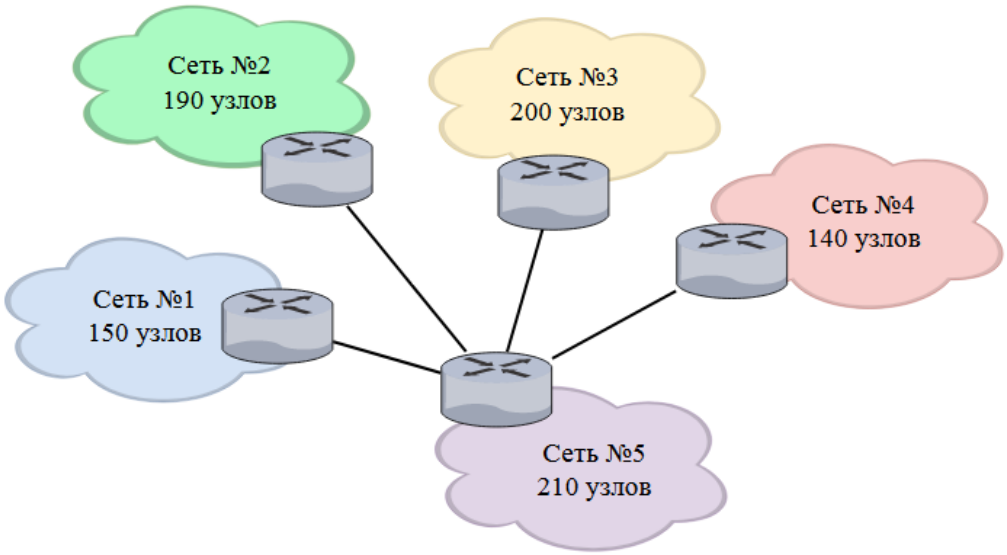

Рисунок 4.3 – Пример разделения на подсети

Таблица 4.3 – Результаты разделения на подсети

Номер подсети	Требуемое количество узлов в сети	Выделяемое количество узлов в сети	Остаток свободных адресов	IP-адрес подсети с префиксом
1	150	254	104	172.16.0.0/24
2	190	254	64	172.16.1.0/24
3	200	254	154	172.16.2.0/24
4	140	254	114	172.16.3.0/24
5	210	254	44	172.16.4.0/24
6	2	254	252	172.16.5.0/24
7	2	254	252	172.16.6.0/24
8	2	254	252	172.16.7.0/24
9	2	254	252	172.16.8.0/24
10	Резерв			172.16.9.0/24
11	Резерв			172.16.10.0/24
12	Резерв			172.16.11.0/24
13	Резерв			172.16.12.0/24
14	Резерв			172.16.13.0/24
15	Резерв			172.16.14.0/24
16	Резерв			172.16.15.0/24

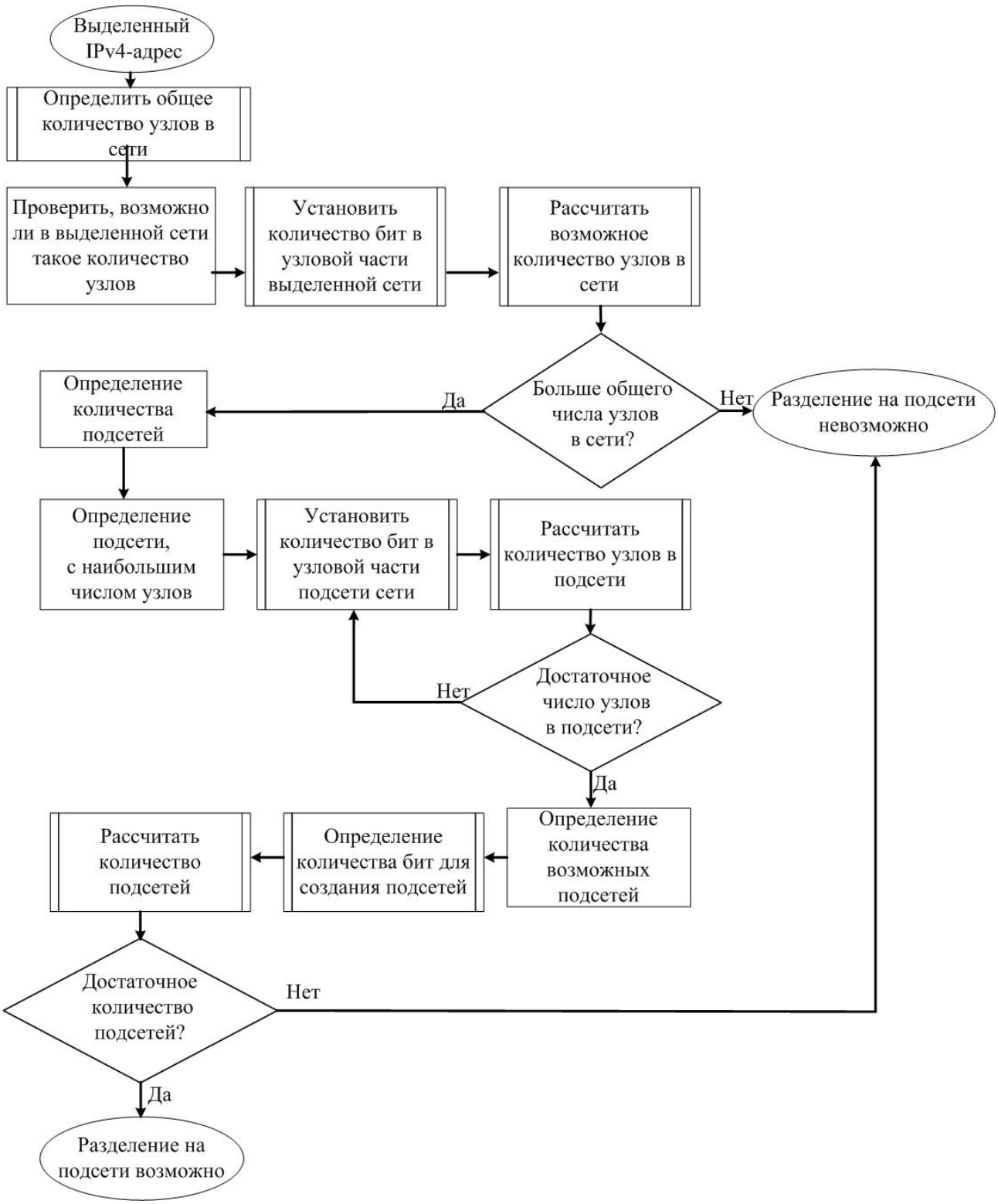

Рисунок 4.4 – Последовательность действий при разделении на подсети

4.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. В соответствии с шифром выбрать из таблицы 4.4 выделенный IP-адрес для сети на рисунке 4.5. Разделить заданную сеть на рисунке 4.5 на необходимое количество подсетей и заполнить таблицу 4.5.

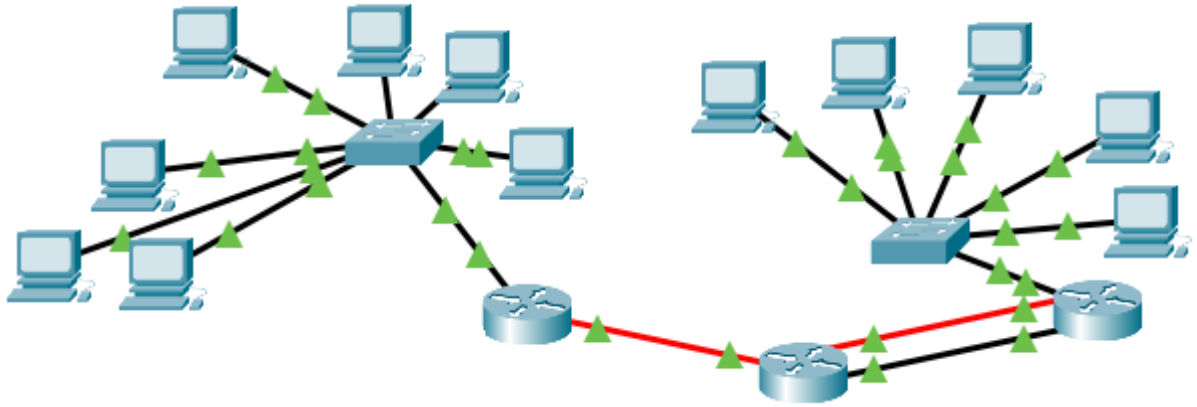

Рисунок 4.5 – Вариант сети для разделения на подсети

Таблица 4.4 – Варианты задания для разделения сети, представленной на рисунке 4.5, на подсети

Номер второй цифры шифра	Выделенный IPv4-адрес
0	192.168.164.0/23
1	192.168.44.0/22
2	192.168.224.0/20
3	192.168.176.0/21
4	192.168.169.0/24
5	192.168.245.128/25
6	192.168.112.0/21
7	192.168.59.128/26
8	192.168.86.0/25
9	192.168.76.0/22

Таблица 4.5 – Результаты разделения на подсети

Номер подсети	Требуемое количество узлов в сети	Выделяемое количество узлов в сети	Остаток свободных адресов	IP-адрес подсети с префиксом	Маска подсети	Диапазон адресов	Широковещательный адрес

2. В соответствии с шифром выбрать из таблицы 4.6 выделенный IP-адрес для сети на рисунке 4.6. Разделить заданную сеть на рисунке 4.6 на необходимое количество подсетей и заполнить таблицу 4.5.

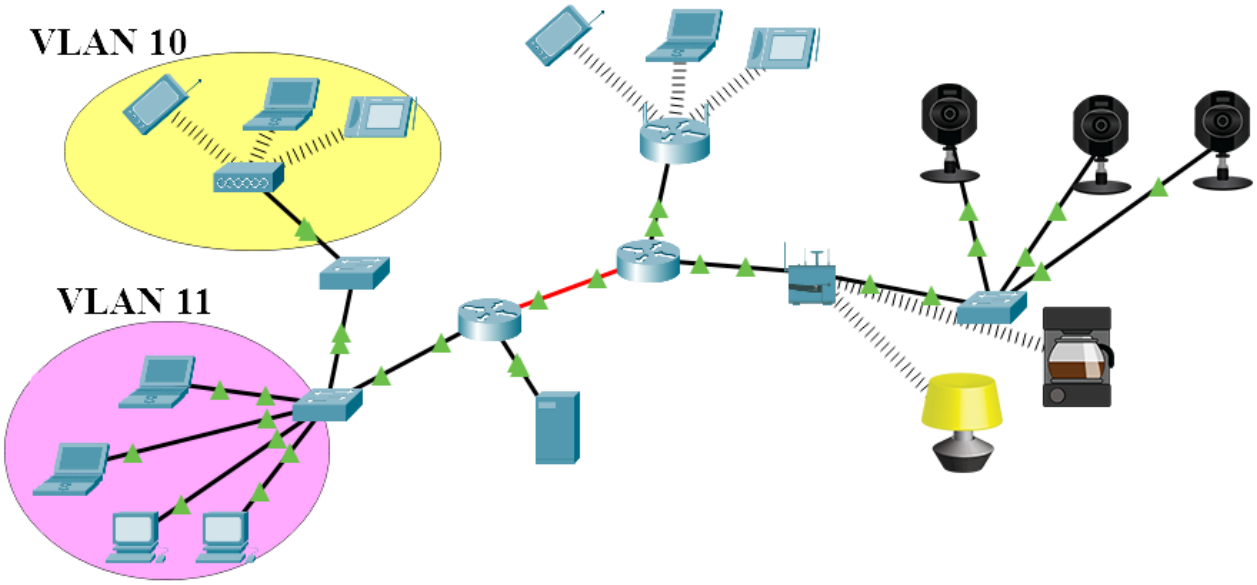

Рисунок 4.6 – Вариант сети для разделения на подсети

Таблица 4.6 – Варианты задания для разделения сети, представленной на рисунке 4.6, на подсети

Номер первой цифры шифра	Выделенный IPv4-адрес
0	172.24.0.0/13
1	172.28.0.0/14
2	172.30.0.0/15
3	172.31.0.0/16
4	172.18.128.0/17
5	172.26.192.0/18
6	172.29.160.0/19
7	172.25.96.0/20
8	172.22.128.0/17
9	172.25.0.0/16

2. В соответствии с шифром выбрать из таблицы 4.7 выделенный IP-адрес для сети на рисунке 4.7 и количество устройств. Разделить заданную сеть на рисунке 4.7 на необходимое количество подсетей и заполнить таблицу 4.5.

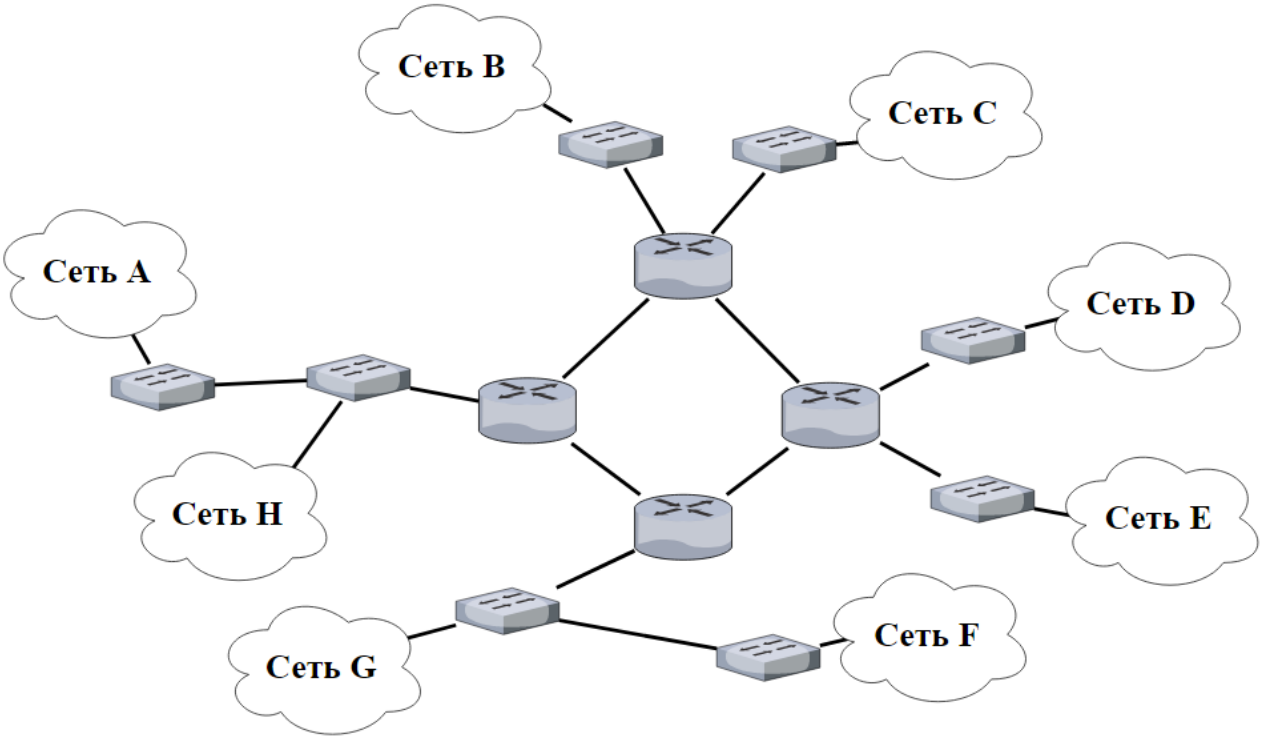

Рисунок 4.7 – Вариант сети для разделения на подсети

Таблица 4.7 – Варианты задания для разделения сети, представленной на рисунке 4.7, на подсети

Номер первой цифры шифра	Выделенный IPv4-адрес	Количество устройств							
		A	B	C	D	E	F	G	H
0	10.248.0.0/16	3000	3500	2500	4000	500	2000	1000	200
1	10.240.0.0/17	2000	2000	1000	2000	200	1000	10	20
2	10.249.192.0/18	1010	1000	1000	1000	800	400	600	10
3	10.114.128.0/18	500	900	800	800	700	200	800	500
4	10.184.0.0/15	5000	7000	6000	5000	6000	4000	4000	3000
5	10.188.0.0/14	9000	7000	8000	6000	9000	8000	8000	5000
6	10.168.0.0/15	3000	5000	5000	5000	5000	6000	2000	5000
7	10.104.0.0/13	9000	9000	9000	9000	9000	9000	9000	9000
8	10.152.0.0/14	9000	8500	8500	8500	8500	8000	8000	7000
9	10.70.0.0/15	4000	5000	5000	6000	7000	3000	5000	4000

4.3 Содержание отчёта

1. Цель работы, исходные данные из таблиц 4.4, 4.6, 4.7.
2. Результаты произведённых расчётов, выполненных для разных сетей, в виде заполненной таблицы 4.5.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

4.4 Контрольные вопросы

1. В чём заключается назначение разбиения на подсети?
2. Что такое подсеть?
3. Как осуществляется планирование IPv4-подсетей?
4. Какие выделяют принципы определения размера подсети?
5. В чём отличие разделения сети на 2 и на 4 подсети?
6. Какая последовательность действий при разделение на подсети?
7. Как реализуется разделение на подсети при настройке сетевых устройств?

ПРАКТИЧЕСКАЯ РАБОТА №5
АДРЕСАЦИЯ VLSM

Цель: овладеть навыками разделения на подсети с использованием маски подсети переменной длины в бесклассовом методе адресации.

5.1 Теоретическая часть

Бесклассовая IP-адресация (Classless Inter-Domain Routing, CIDR) – это метод IP-адресации, который позволяет рационально управлять пространством IP-адресов. В бесклассовом методе адресации используются маски подсети переменной длины (Variable Length Subnet Mask, VLSM).

Классовое назначение IPv4-адресов является неэффективным, если в каждой подсети после разделения остается много неиспользуемых IPv4-адресов. Как видно из таблицы 4.3, для сети, разделенной на 9 подсетей (см. рисунок 4.3) с использованием традиционного способа разделения, в четырех сетях свободными остаются 252 IPv4-адреса, что является весьма нерациональным. При этом данное разбиение на подсети соответствует требованиям самой крупной сети и делит адресное пространство на достаточное количество подсетей, однако образуется значительный объём неиспользуемых адресов.

VLSM-маска позволяет разделить сетевое пространство на неравные части. VLSM-маска подсети может варьироваться в зависимости от количества бит, которые были заимствованы для конкретной подсети. Отличия бесклассовой адресации от классовой состоит в том, что разбиение на подсети выполняется в несколько этапов. При использовании VLSM сеть сначала разбивается на подсети, а затем подсети снова делятся на подсети. Этот процесс может повторяться много раз для создания подсетей различного размера.

В сети на рисунке 5.1 общее количество устройств составляет 813. В выделенном IPv4-адресе 172.20.160.0/20 в узловой части 12 бит, в соответствии с формулой (4.2) такая сеть может содержать 4094 IPv4-адреса. Таким образом, изначально есть блок IPv4-адресов (рисунок 5.2), который можно разделить на 2 блока по 2046 адресов, или на три блока (2046, 1022, 1022 адреса в каждом), или на 4 блока (2046, 1022, 510, 510 адресов в каждом) и т. д. Не все блоки могут быть использованы, а только те, которые удовлетворяют условию подсети по количеству узлов, остальные могут использоваться как резервные. Таким образом, для сети, представленной на рисунке 5.1, разделить блок адресов из 4094 адресов можно, как показано на рисунке 5.3. На данном рисунке используемые блоки выделены серым цветом, и в блоке указано общее количество доступных IPv4-адресов и требуемых. Остальные блоки не будут использоваться, они могут быть учтены при дальнейшем развитии сети.

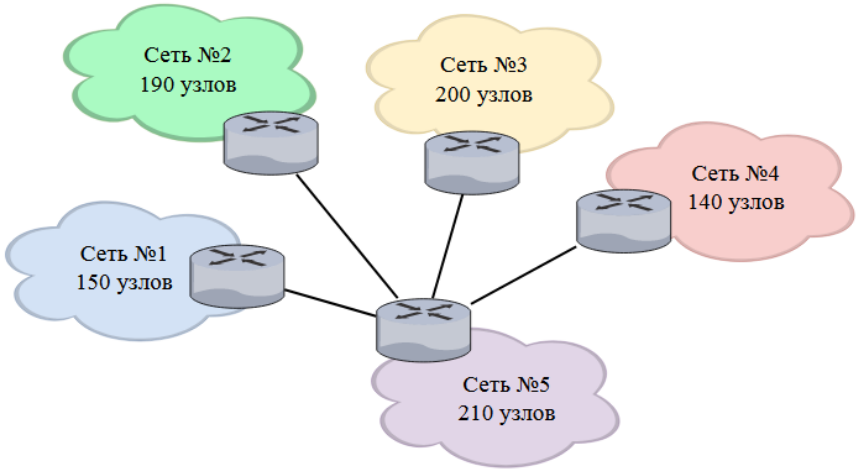

Рисунок 5.1 – Пример разделения на подсети

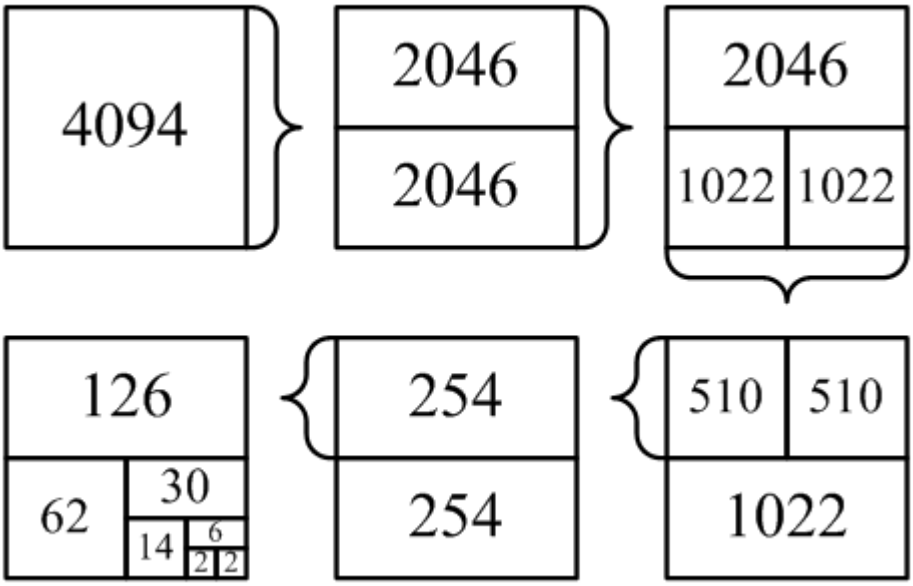

Рисунок 5.2 – Разделение блока из 4094 IPv4-адресов

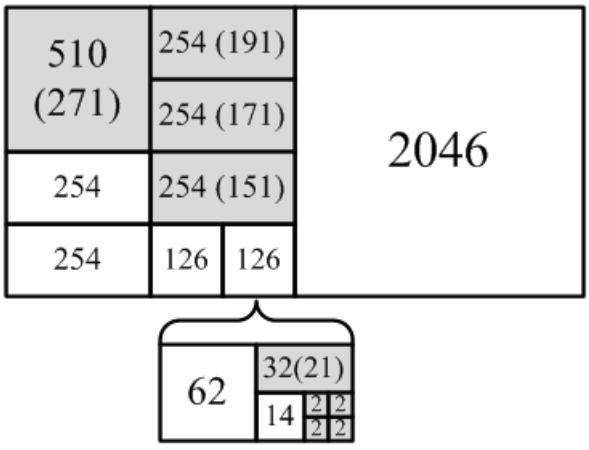

Рисунок 5.3 – Разделение блока из 4094 IPv4-адресов для сети на рисунке 5.1

Далее необходимо определить IPv4-адреса подсетей и диапазоны адресов в каждой из них. Сначала необходимо определить маску подсети для выделенного IPv4-адреса 172.20.160.0/20, которой является 255.255.240.0. Как уже было отмечено, в узловой части 12 бит, которые можно использовать для создания подсетей. Если взять 1 бит из узловой части, то можно получить 2 подсети с 2046 IPv4-адресами в каждой (формулы (4.1), (4.2)). У первой подсети будет IPv4-адрес 172.20.160.0/21, у второй – 172.20.168.0/21. Исходя из рисунка 5.3 одна из представленных сетей не будет использоваться (172.20.168.0/21), а вторая будет подразделяться далее (172.20.160.0/21).

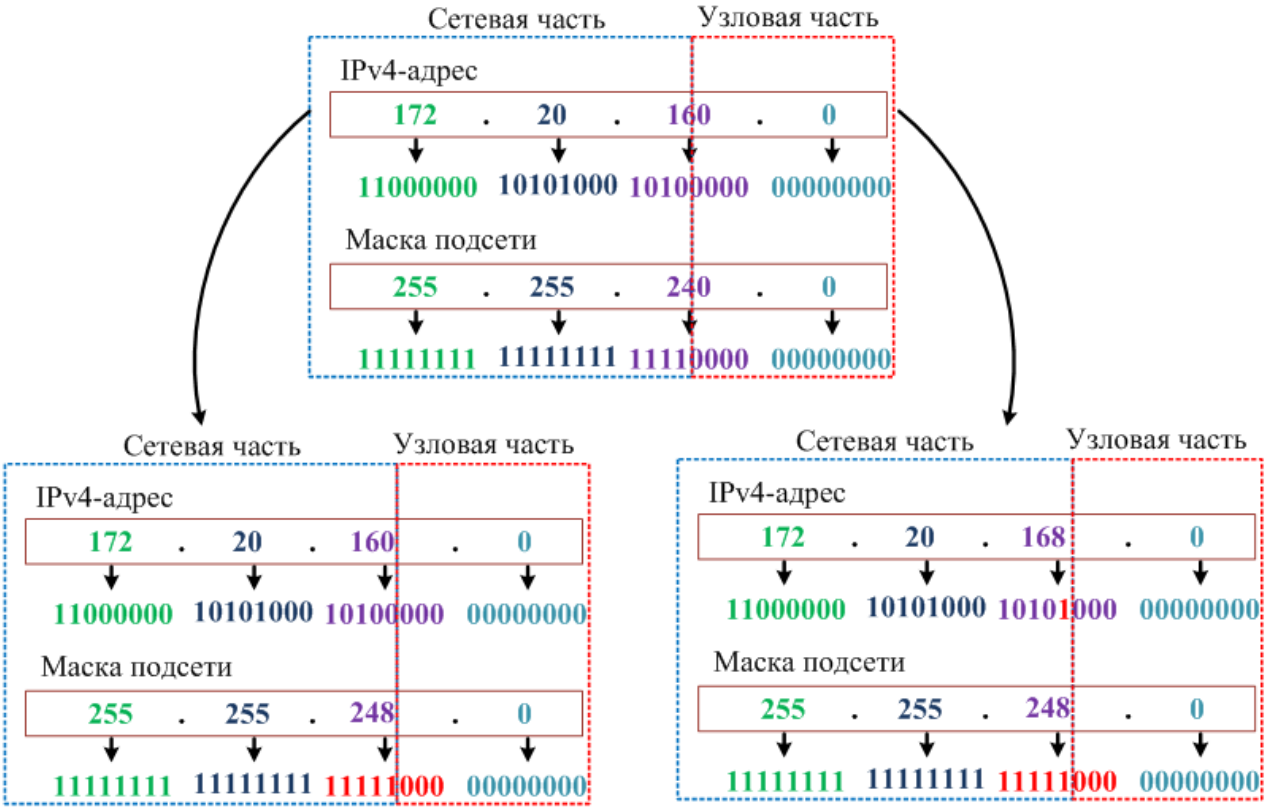

Рисунок 5.4 – Подразделение на подсети сети 172.20.160.0/20

Основное правило при разделении с использованием VLSM заключается в том, что необходимо начинать с наибольшей сети. Самая большая сеть №4 (рисунок 5.1), в которой 271 устройство. По формуле (4.2) для 271 адреса необходимо 9 бит, для сетевой части останется 2 бита, что позволит создать 4 подсети по 510 IPv4-адресов в каждой. Таким образом, получаем 4 подсети (рисунок 5.5) с адресами 172.20.160.0/23, 172.20.162.0/23, 172.20.164.0/23, 172.20.166.0/23. На рисунке 5.5 не показаны подсети с адресами 172.20.162.0/23, 172.20.164.0/23. IPv4-адрес 172.20.160.0/23 будет использован для сети №4 с 271 устройством.

Следующая по величине сеть №2 с 191 устройством. Исходя из формулы (4.2) для 191 адреса необходимо 8 бит, для сетевой части останется 1 бит, что позволит создать 2 подсети по 254 IPv4-адресов. Разделим сеть 172.20.162.0/23

на сети 172.20.162.0/24 и 172.20.163.0/24 (рисунок 5.6). Получается, что в каждой сети в узловой части 8 бит, что достаточно для сетей №2 и №3.

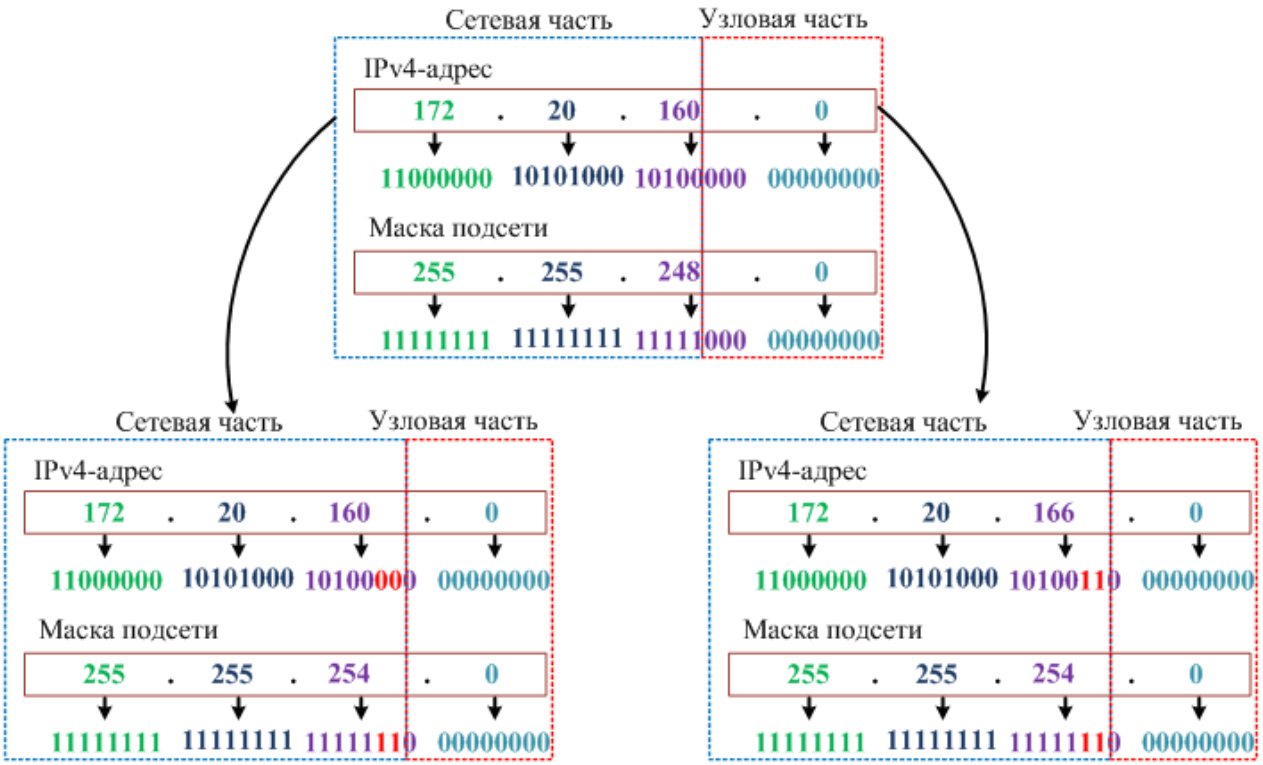

Рисунок 5.5 – Разделение на подсети сети 172.20.160.0/21

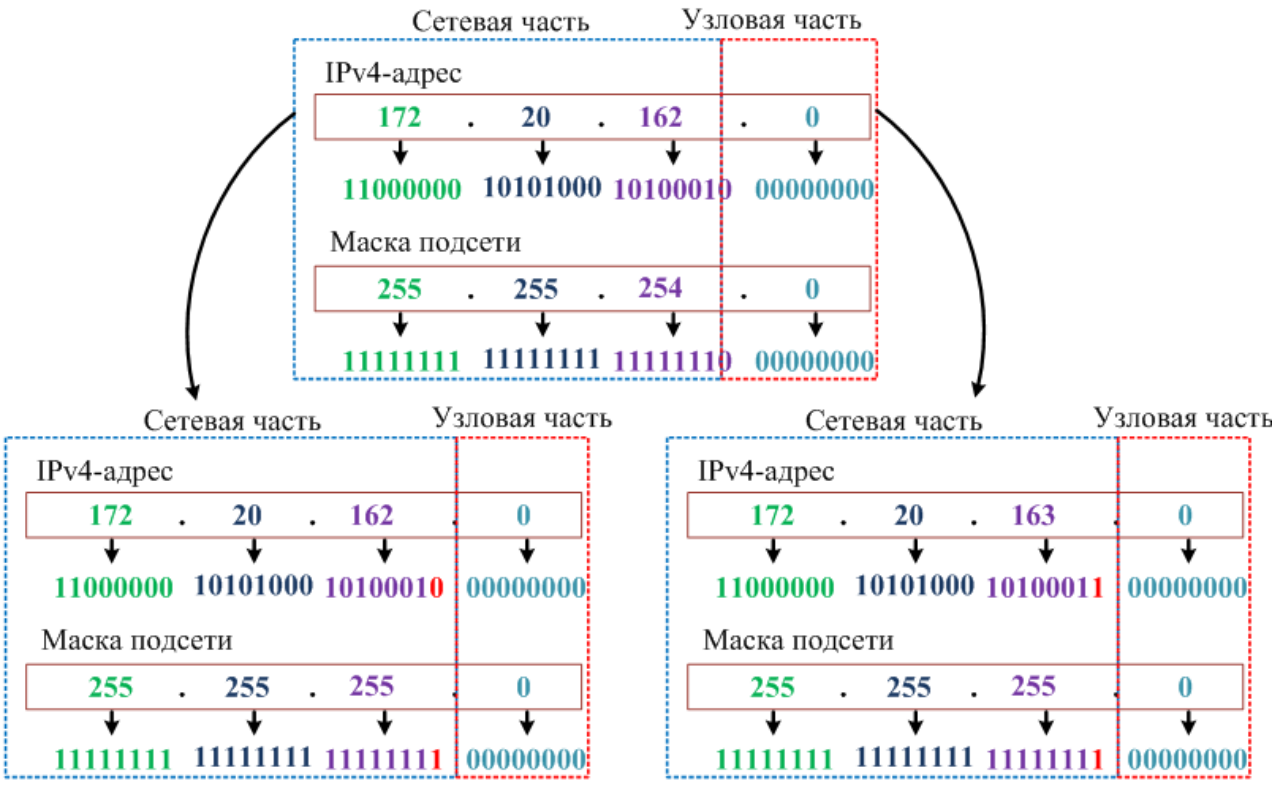

Рисунок 5.6 – Разделение на подсети сети 172.20.162.0/23

Для сети №3 необходимо также 8 бит, т. к. количество устройств 171. Поэтому для сети №2 можно использовать IPv4-адрес 172.20.162.0/24, а для сети №3 172.20.163.0/24. Необходимо отметить, что для создания сети №1 также достаточно 8 бит в узловой части, поэтому можно взять следующую неиспользуемую сеть 172.20.164.0/23 и разделить её на 2 подсети по аналогии с предыдущей. Таким образом получим 2 подсети с IPv4-адресами 172.20.164.0/24 и 172.20.165.0/24, в каждой из которых возможно по 254 IPv4-адресов. Используем IPv4-адрес 172.20.164.0/24 для сети №1.

Для сети №5 необходимо 20 IPv4-адресов, т. е. в узловой части достаточно согласно формуле (4.2) 5 бит, в сетевой части останется 3 бита для создания согласно формуле (4.1) восьми подсетей. Разделим сеть 172.20.165.0/24 (рисунок 5.7) и получим следующие сети: 172.20.165.0/27; 172.20.165.32/27; 172.20.165.64/27; 172.20.165.96/27; 172.20.165.128/27; 172.20.165.160/27; 172.20.165.192/27; 172.20.165.224/27.

Сеть 172.20.165.0/27 содержит 32 IPv4-адреса, что удовлетворяет требованиям сети №5.

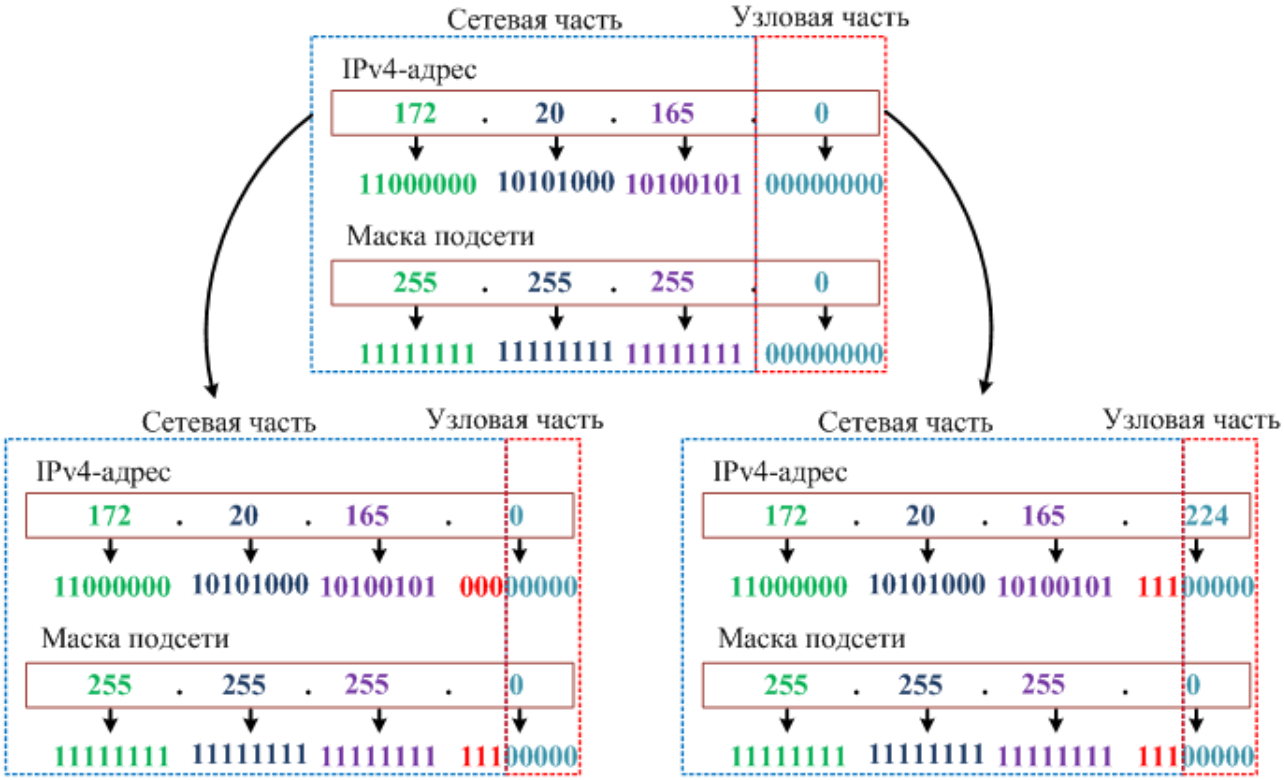

Рисунок 5.7 – Разделение на подсети сети 172.20.165.0/24

Для обеспечения соединений между маршрутизаторами необходимо 4 сети по 2 IPv4-адреса в каждой, для чего по формуле (4.2) необходимо 2 бита в узловой части и 2 бита в сетевой части. Для разделения используем следующий свободный IPv4-адрес 172.20.165.32/27, в узловой части которого 5 бит, т. к. для узловой части достаточно 2 бита, то для сетевой части используем 3 бита, что позволит создать дополнительные небольшие сети для дальнейшего

развития сети при добавлении новых маршрутизаторов. По результатам разбиения сети 172.20.165.32/27 получаем следующие подсети: 172.20.165.32/30; 172.20.165.36/30; 172.20.165.40/30; 172.20.165.44/30; 172.20.165.48/30; 172.20.165.52/30; 172.20.165.56/30; 172.20.165.60/30.

Каждая из полученных подсетей содержит по 2 IPv4-адреса, что является достаточным для сетей между маршрутизаторами. В таблице 5.1 представлена итоговая таблица расчёта подсетей для сети на рисунке 5.1. Диапазон доступных IPv4-адресов, широковещательный адрес рассчитывается по аналогии с расчётом в классовых IPv4-сетях.

Таблица 5.1 – Результаты разделения на подсети

Номер подсети	Требуемое количество узлов в сети	Выделяемое количество узлов в сети	Остаток свободных адресов	IP-адрес подсети с префиксом
4	271	510	239	172.20.160.0/23
2	191	254	63	172.20.162.0/24
3	171	254	83	172.20.163.0/24
1	151	254	103	172.20.164.0/24
5	21	30	9	172.20.165.0/27
6	2	2	0	172.20.165.32/30
7	2	2	0	172.20.165.36/30
8	2	2	0	172.20.165.40/30
9	2	2	0	172.20.165.44/30
Резерв	0	2046	0	172.20.168.0/21
Резерв	0	510	0	172.20.166.0/23
Резерв	0	30	0	172.20.165.64/27
Резерв	0	30	0	172.20.165.96/27
Резерв	0	30	0	172.20.165.128/27
Резерв	0	30	0	172.20.165.160/27
Резерв	0	30	0	172.20.165.192/27
Резерв	0	30	0	172.20.165.224/27
Резерв	0	2	0	172.20.165.48/30
Резерв	0	2	0	172.20.165.52/30
Резерв	0	2	0	172.20.165.56/30
Резерв	0	2	0	172.20.165.60/30

5.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. В соответствии с шифром выбрать из таблицы 5.2 выделенный для сети на рисунке 5.8 IP-адрес и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть на рисунке 5.8 на необходимое количество подсетей с использованием VLSM и заполнить таблицу 5.3.

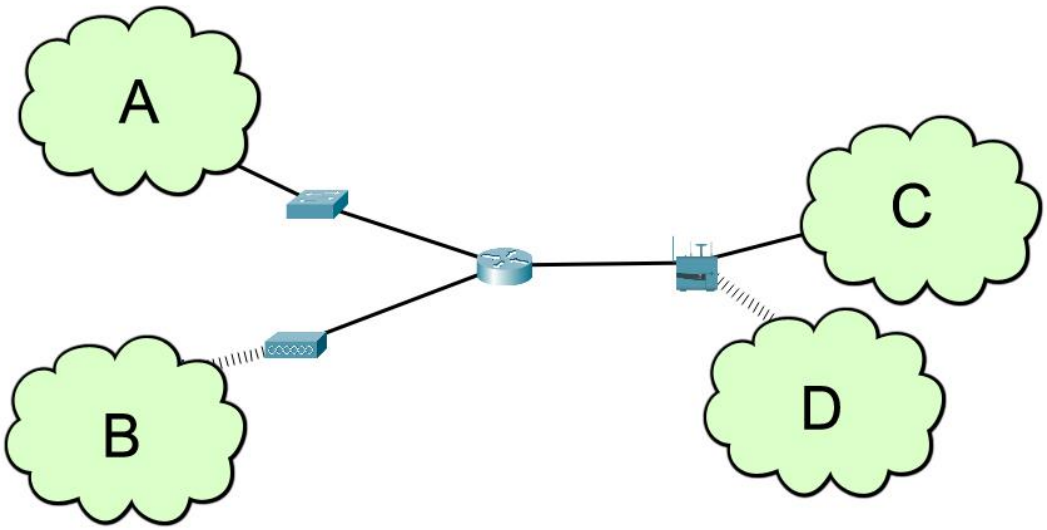

Рисунок 5.8 – Вариант сети для разделения на подсети

Таблица 5.2 – Варианты задания для разделения сети, представленной на рисунке 5.8, на подсети

Номер первой цифры шифра	Выделенный IPv4-адрес	Количество устройств			
		A	B	C	D
0	192.168.96.0/27	1	3	6	6
1	192.168.58.192/26	2	27	5	8
2	192.168.109.128/25	5	24	28	31
3	192.168.129.0/24	8	51	33	34
4	192.168.169.224/27	1	3	5	5
5	192.168.169.64/26	7	3	10	7
6	192.168.52.0/24	57	13	44	45
7	192.168.103.128/25	4	27	28	29
8	192.168.193.160/27	1	1	8	4
9	192.168.37.64/26	4	10	10	10

Таблица 5.3 – Результаты разделения на подсети

Номер подсети	Требуемое количество узлов в сети	Выделяемое количество узлов в сети	Остаток свободных адресов	IP-адрес подсети с префиксом	Маска подсети	Диапазон адресов	Широковещательный адрес

2. В соответствии с шифром выбрать из таблицы 5.4 выделенный IP-адрес для сети на рисунке 5.9 и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть на рисунке 5.9 на необходимое количество подсетей с использованием VLSM и заполнить таблицу 5.3.

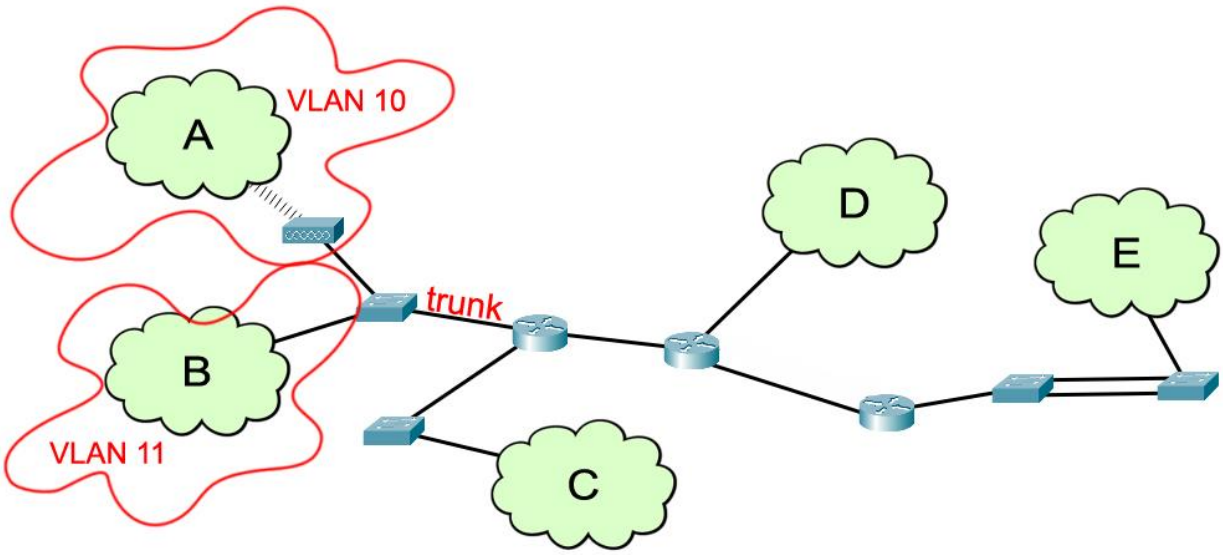

Рисунок 5.9 – Вариант сети для разделения на подсети

Таблица 5.4 – Варианты задания для разделения сети, представленной на рисунке 5.9, на подсети

Номер первой цифры шифра	Выделенный IPv4-адрес	Количество устройств				
		A	B	C	D	E
0	172.30.176.0/20	1100	90	10	200	40
1	172.21.136.0/21	400	131	700	16	50
2	172.16.124.0/23	100	60	90	30	15
3	172.19.140.0/22	60	5	20	150	400

Продолжение таблицы 5.4

Номер первой цифры шифра	Выделенный IPv4-адрес	Количество устройств				
		A	B	C	D	E
4	172.29.106.0/23	20	70	10	110	20
5	172.25.192.0/20	30	80	900	6	100
6	172.18.76.0/22	80	10	30	100	300
7	172.17.224.0/21	26	140	500	60	800
8	172.28.44.0/22	20	400	16	200	100
9	172.26.152.0/21	36	100	80	500	50

3. В соответствии с шифром выбрать из таблицы 5.5 выделенный для сети на рисунке 5.10 IP-адрес и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть на рисунке 5.10 на необходимое количество подсетей с использованием VLSM и заполнить таблицу 5.3.

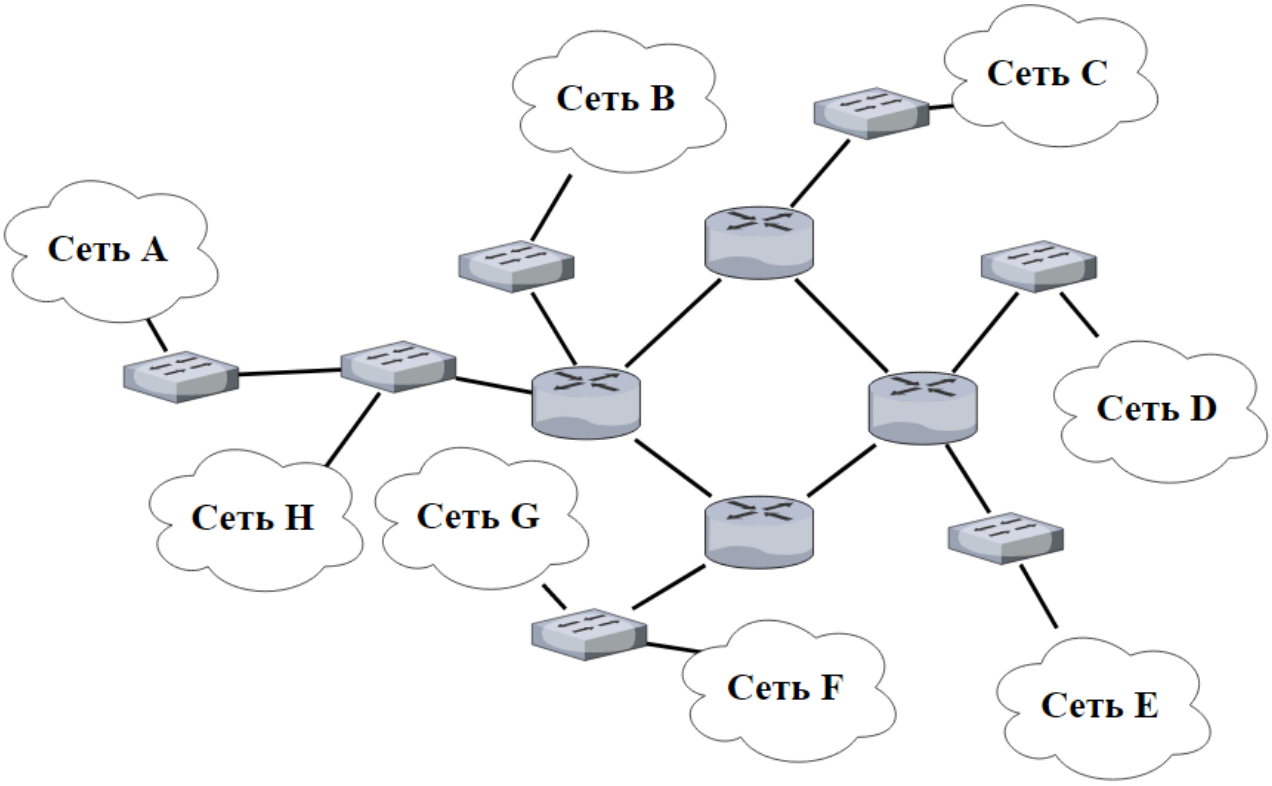

Рисунок 5.10 – Вариант сети для разделения на подсети

Таблица 5.5 – Варианты задания для разделения сети, представленной на рисунке 5.10, на подсети

Номер первой цифры шифра	Выделенный IPv4-адрес	Количество устройств							
		A	B	C	D	E	F	G	H
0	10.89.96.0/19	1500	4	40	200	1000	50	50	1500
1	10.252.0.0/16	250	200	70	10	4000	4000	4000	250
2	10.248.0.0/17	4000	1000	100	500	90	6000	6000	4000
3	10.145.0.0/16	4500	300	80	30	800	2500	2500	4500
4	10.89.224.0/19	800	70	200	800	1500	1000	1000	800
5	10.59.0.0/16	450	50	90	6000	9000	50	50	450
6	10.245.192.0/18	100	100	300	80	50	950	950	100
7	10.213.128.0/17	1500	500	200	100	50	2000	2000	1500
8	10.92.32.0/19	100	10	40	70	80	1000	1000	100
9	10.76.64.0/18	1000	80	70	10	40	1500	1500	1000

5.3 Содержание отчёта

1. Цель работы, исходные данные в соответствии с заданным шифром из таблиц 5.2, 5.4, 5.5.
2. Результаты произведённых расчётов, выполненных для разных сетей, в виде заполненной таблицы 5.3.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

5.4 Контрольные вопросы

1. Что такое CIDR?
2. В чём различие классовой и бесклассовой IP-адресации,
3. Какие выделяют достоинства использования VLSM?
4. Какая последовательность действий при разбиении на подсети в бесклассовой IP-адресации?

ПРАКТИЧЕСКАЯ РАБОТА №6
ПРЕДСТАВЛЕНИЕ IPV6-АДРЕСОВ

Цель: изучить формат IPv6-адреса и его типы, научиться использовать процесс EUI-64 для создания локальных и глобальных IPv6-адресов.

6.1 Теоретическая часть

Протокол IPv6 использует для адресации 128 бит вместо 32 бит в IPv4. В стандарте IPv6 используется шестнадцатеричная запись числа для представления 128-битных адресов. В отличие от IPv4-адресов, которые выражены в десятичном формате с разделительными точками, IPv6-адреса представлены с помощью шестнадцатеричных значений.

Если в десятичной системе основанием является 10, в двоичной системе основанием является 2, то основание шестнадцатеричной системы счисления – 16. Система с основанием 16 использует цифры от 0 до 9 и буквы от A до F, где $A_{16} \rightarrow 1010_2 \rightarrow 10_{10}$, $F_{16} \rightarrow 1111_2 \rightarrow 15_{10}$. Шестнадцатеричное значение обычно представлено в тексте значением с подстрочным индексом 16, как показано выше. Однако, поскольку подстрочный текст не распознаётся в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой X), для представленных выше примеров 0x0A, 0x0F. Также возможен вариант обозначения шестнадцатеричной СС с помощью буквы H (например, 0AH). Это необходимо для отличия шестнадцатеричной СС от десятичной. Если есть значение 75 без обозначений, скорее всего имеется в виду десятичное выражение, если 0x75 или 75H, то данные значения представлены в шестнадцатеричной СС. Перевод из шестнадцатеричной СС в десятичную или двоичную осуществляется на основе знания таблицы 6.1. Например, значения $0xBC \rightarrow 10111100_2 \rightarrow 188_{10}$.

Таблица 6.1 – Представление шестнадцатеричных значений в десятичной и двоичной системах счисления

Шестнадцатеричное представление	Десятичное представление	Двоичное представление
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001

Продолжение таблицы 6.1

Шестнадцатеричное	Десятичное	Двоичное
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Шестнадцатеричная система счисления очень удобна в использовании, поскольку любые четыре бита могут быть представлены одним шестнадцатеричным значением. Например, если 8 бит или 1 байт представить в виде двоичного кода 11111111, то в шестнадцатеричной системе счисления данный код будет равен 0xFF. Для завершения 8-битного представления значения 1010 дополняют нули (00001010), которое в шестнадцатеричной системе представляется как 0x0A.

Протокол IPv6 позволяет использовать $3{,}4 \cdot 10^{38}$ IPv6-адресов. Эта версия протокола IP должна обеспечить необходимое количество адресов как на текущий момент, так и в будущем. Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причём общее количество шестнадцатеричных значений равно 32.

Формат для записи IPv6-адреса представлен на рисунке 6.1 и выражается в записи шестнадцатеричных чисел через двоеточия, которые ограничивают сегменты из 16 бит или четырёх шестнадцатеричных значений (гекстеты).

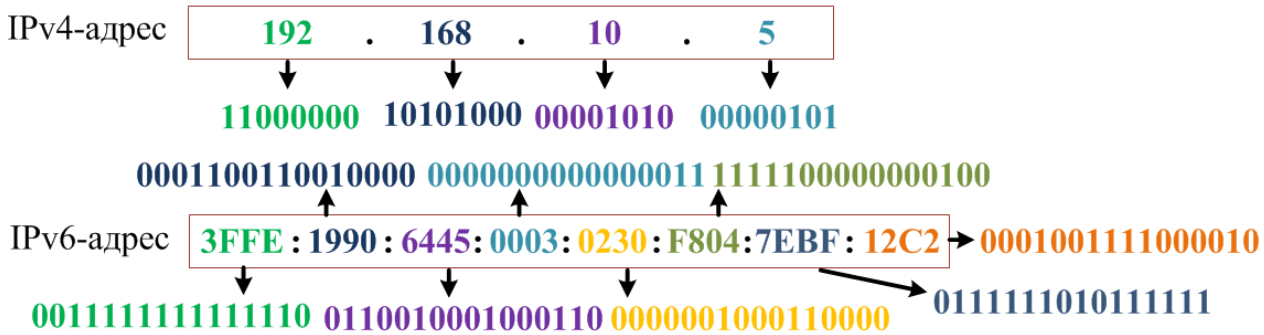

Рисунок 6.1 – Представление IPv4- и IPv6-адресов

Для сокращения записи IPv6-адреса используются следующие правила:

1) сокращение ведущих нулей – в IPv6-адресе не учитываются первые нули, например, значение 0x0200 можно записать в виде 0x200 (рисунок 6.2);

2) пропуск нулевых блоков – использование двойного двоеточия «::» позволяет сокращать гекстеты, состоящие из нулей; может использоваться в адресе только один раз (рисунок 6.2).

Рисунок 6.2 – Пример применения правил для представления сжатого формата IPv6-адреса

Выделяют три типа IPv6-адресов:

– индивидуальный служит для определения интерфейса на устройстве под управлением протокола IPv6, т. е. IPv6-адрес источника должен быть индивидуальным;

– групповой используется для отправки IPv6-пакетов по нескольким адресам назначения; – произвольный – любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам.

В отличие от протокола IPv4, IPv6 не использует адрес широковещательной рассылки. Однако есть групповой IPv6-адрес для всех узлов, который даёт аналогичный результат.

Протокол IPv6 использует префикс для обозначения части префикса адреса. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Диапазон длины префикса может составлять от 0 до 128. Традиционной длиной IPv6-префикса для локальных и других типов сетей является /64 (рисунок 6.3). Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для узловой части адреса.

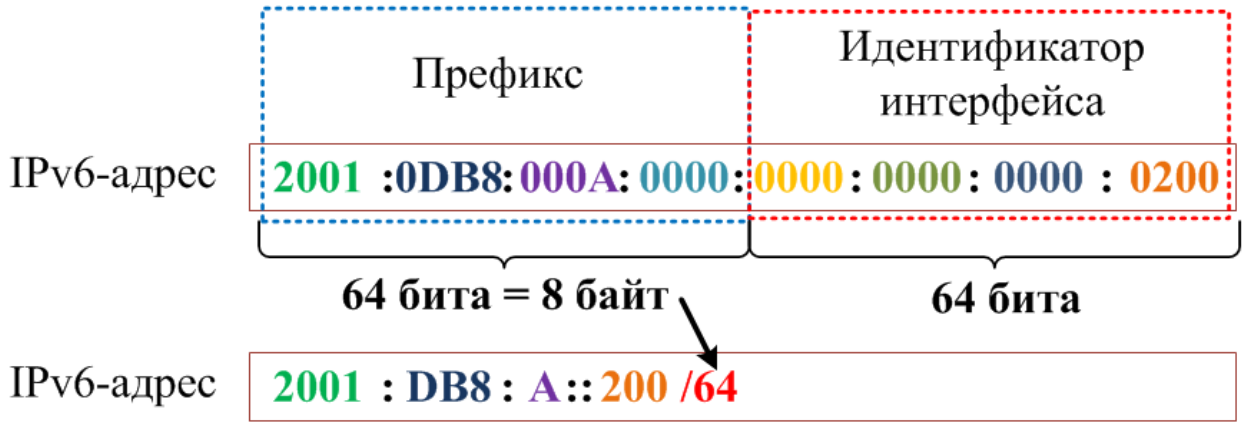

Рисунок 6.3 – Запись IPv6-адреса с префиксом

Существуют следующие типы индивидуальных IPv6-адресов:

– глобальный индивидуальный адрес;

– локальный адрес канала;

– логический интерфейс loopback;

– неопределённый адрес;
– уникальный локальный адрес.

Глобальный индивидуальный адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. В динамическом назначении IPv6-адреса устройством имеются некоторые важные отличия по сравнению с динамическим назначением IPv4-адреса. Глобальные индивидуальные адреса обозначаются первыми тремя битами 001 или 2000::/3. Адрес 2001:0DB8::/32 был зарезервирован для документации, в том числе для использования в примерах. На рисунке 6.4 представлено, что у IPv6-адреса префикс глобальной маршрутизации представлен в виде первых трех гекстетов (2001:0DB8:ACAD), четвертый гекстет обозначает адрес подсети. Так как префикс глобальной маршрутизации /48, префикс подсети /16, то общий префикс составляет /64.

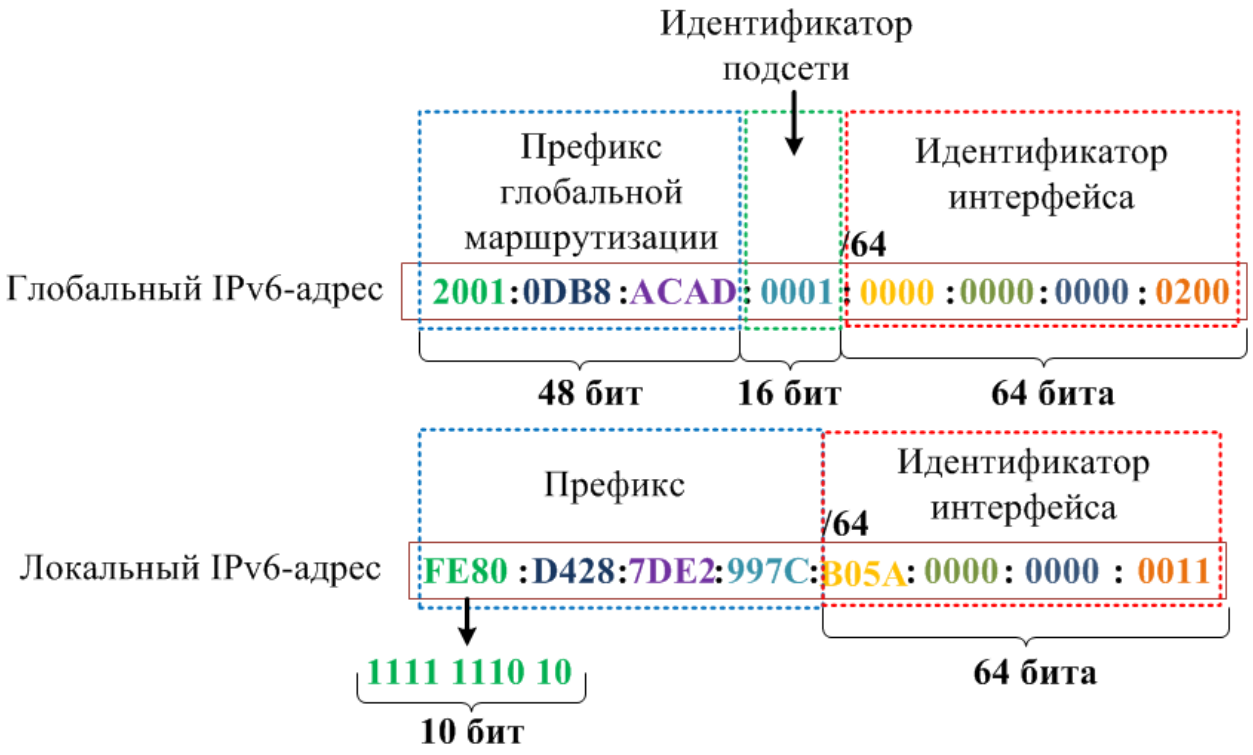

Рисунок 6.4 – Представление глобальных и локальных IPv6-адресов

Локальные адреса канала используются для обмена данными с другими устройствами по одному локальному каналу. В протоколе IPv6 термин «канал» означает подсеть. Локальные адреса каналов ограничены одним каналом. Они должны быть уникальны только в рамках этого канала, поскольку вне канала к ним нельзя проложить маршрут. Другими словами, маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения.

Узлы под управлением IPv6 создают локальный IPv6-адрес канала даже в том случае, если устройству не был назначен глобальный IPv6-адрес. Это

позволяет устройствам под управлением IPv6 обмениваться данными с другими устройствами под управлением IPv6 в одной подсети, в том числе со шлюзом по умолчанию (маршрутизатором). Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10 указывает на то, что первые 10 бит – 1111 1110 10. Первый гекстет имеет диапазон от 1111 1110 1000 0000 (FE80) до 1111 1110 1011 1111 (FEBF).

Логический интерфейс (loopback-адрес) используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

Неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128. Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFF::/7.

Последними из рассматриваемых типов индивидуальных адресов являются встроенные IPv4-адреса. Использование этих адресов способствует переходу с протокола IPv4 на IPv6.

Процесс EUI-64 – процесс, использующий 48-битный MAC-адрес клиента и в середине этого адреса размещается 16 бит для создания 64-битного идентификатора интерфейса в IPv6-адресе. MAC-адрес представляется в шестнадцатеричном формате и состоит из двух частей:

– уникальный идентификатор организации (OUI) – 24-битный код поставщика, назначенный IEEE;

– идентификатор устройства – уникальное 24-битное значение с общим уникальным идентификатором организации (OUI).

Идентификатор интерфейса в формате EUI-64 представлен в двоичном формате и состоит из трёх частей:

– 24-битный OUI на основе MAC-адреса, в котором седьмой бит является обратным, т. е. если седьмой бит имеет значение 0, то он становится 1, и наоборот;

– 16-битное значение FFFE;

– 24-битный идентификатор устройства на основе MAC-адреса клиента.

Процесс EUI-64 состоит из следующих шагов (рисунок 6.4).

1. Разделение MAC-адреса на часть OUI и идентификатор устройства.

2. Вставка шестнадцатеричного значения FFFE в двоичном формате.

3. Преобразование седьмого бита OUI в обратное значение.
4. Добавление префикса локального адреса.

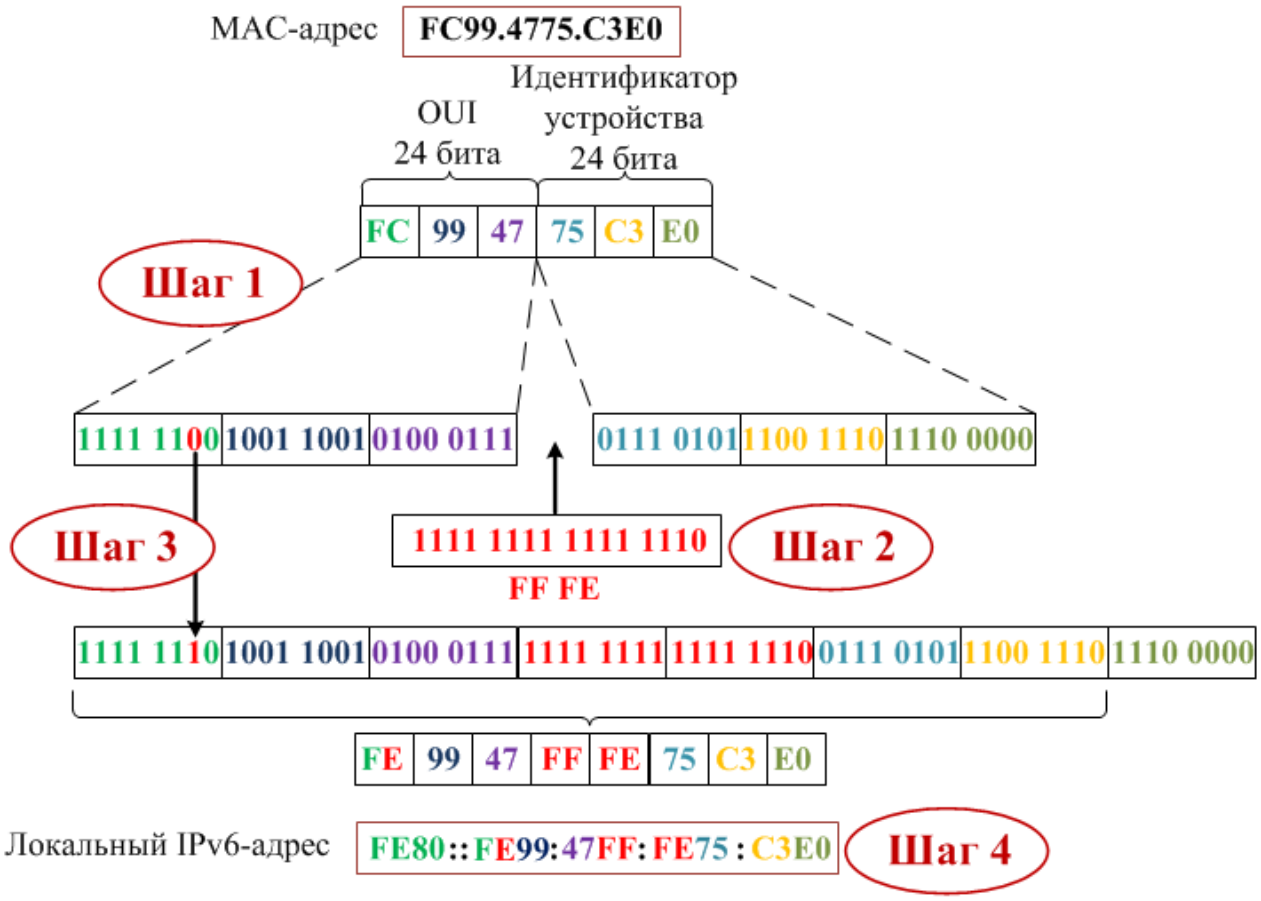

Рисунок 6.5 – Процесс EUI-64

Групповой адрес используется для отправки одного пакета по одному или нескольким назначениям (группе мультивещания). Групповые IPv6-адреса имеют префикс FF00::/8. Групповые адреса могут быть только адресами назначения, а не адресами источника.

Существует два типа групповых IPv6-адресов:

– присвоенный групповой адрес;

– групповой адрес запрошенного узла.

Присвоенный групповой адрес – это один адрес, используемый для осуществления связи с группой устройств, работающих на одном протоколе или сервисе. Присвоенные групповые адреса зарезервированы для заданных групп устройств.

Существует две распространённые группы присвоенных групповых IPv6-адресов:

– группа мультивещания для всех узлов;

– группа мультивещания для всех маршрутизаторов.

Группа мультивещания для всех узлов FF02::1. Это группа мультивещания, к которой подключены все устройства под управлением

протокола IPv6. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-интерфейсами в канале или сети. Эта группа адресов работает так же, как широковещательный адрес в протоколе IPv4.

Группа мультивещания для всех маршрутизаторов FF02::2. Это группа мультивещания, к которой подключены все IPv6-маршрутизаторы. Маршрутизатор становится частью этой группы, когда переходит под управление протоколом IPv6 с помощью команды глобальной конфигурации `ipv6 unicast-routing`. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-маршрутизаторами в канале или сети.

Устройства под управлением протокола IPv6 отправляют сообщения с запросом маршрутизатора групповому адресу для всех маршрутизаторов. Такие сообщения запрашивают у IPv6-маршрутизатора объявление маршрутизатора, чтобы помочь устройству в процессе адресной конфигурации.

Групповой адрес запрашиваемого узла – это адрес, который соответствует только 24 битам глобального индивидуального IPv6-адреса устройства. Обрабатывать эти пакеты должны только те устройства, которые имеют аналогичные 24 бита в наименее значащей, крайней правой части идентификатора интерфейса.

Групповой IPv6-адрес запрашиваемого узла создаётся автоматически при назначении глобального индивидуального адреса или локального адреса канала. Групповой IPv6-адрес запрашиваемого узла создаётся посредством объединения специального префикса FF02:0:0:0:0:1:FF00::/104 с крайними правыми 24 битами его индивидуального адреса (рисунок 6.6).

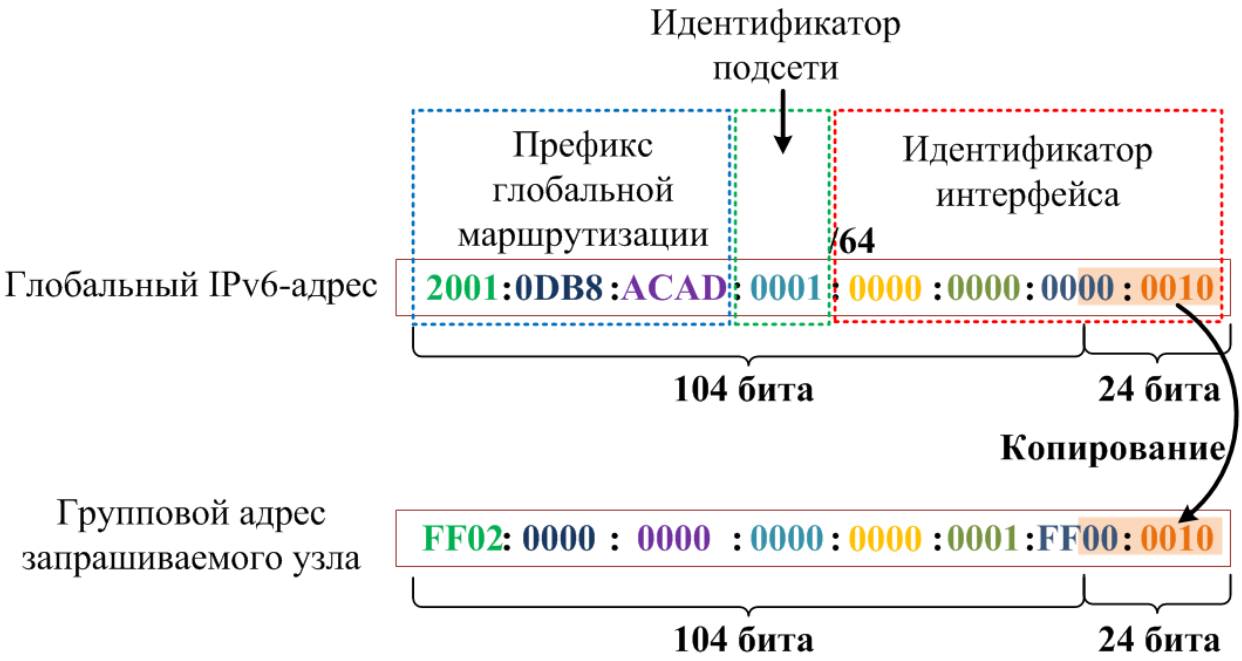

Рисунок 6.6 – Преобразование глобального IPv6-адреса в групповой адрес запрашиваемого узла

Групповой адрес запрашиваемого узла состоит из двух частей:

– групповой префикс FF02:0:0:0:0:1:FF00::/104: – первые 104 бита группового адреса запрашиваемого узла;

– 24 бита группового адреса запрашиваемого узла – копия 24 бит из крайних правых бит глобального индивидуального адреса или локального адреса канала устройства.

6.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. Осуществить преобразование десятичных чисел в шестнадцатеричные и шестнадцатеричных в двоичные. В соответствии с шифром из таблицы 6.2 выбрать десятичные числа и осуществить их преобразование в двоичную СС. Результаты перевода представить в виде таблицы 6.3.

Таблица 6.2 – Шестнадцатеричные числа для перевода в двоичную СС

Номер первой цифры шифра	Шестнадцатеричные числа для перевода в двоичную СС
0	8BA3, A2CB, C1EA, 3AF8
1	E188, 324E, 87D4, AC2F
2	4EC8, 97AD, 91B5, F82B
3	2F8A, CA7D, C9B6, 4E14
4	52FC, A19B, 7CD4, BFB8
5	E274, 7E94, D5F8, A437
6	41F6, 7C4B, FC4D, A8E3
7	53BA, EF9A, 5D8C, F721
8	A9D3, 24DE, B789, 3CB4
9	6F49, 2CDB, F7EC, 236E

Таблица 6.3 – Представление результатов перевода из одной СС в другую

Шестнадцатеричное число	Результат перевода в двоичную СС

2. Осуществить преобразование двоичных чисел в шестнадцатеричные. В соответствии с шифром из таблицы 6.4 выбрать двоичные числа и осуществить их преобразование в шестнадцатеричную СС. Результаты перевода представить в виде таблицы 6.3.

Таблица 6.4 – Двоичные числа для перевода в шестнадцатеричную СС

Номер второй цифры шифра	Двоичные числа для перевода в шестнадцатеричную СС
0	100100010111100, 111110111101010 10101010011111, 1111001101011011
1	0101000011111010, 0001100110001110 110110011011001, 1011111100100111
2	0110001110101110, 101101111001000 0000100001111101, 1111101010010010
3	0101000111001101, 1111011101101110 0100101010110111, 1001000011101010
4	1100111100110101, 0011100010100110 1110011001011101,1011010000011001
5	1010001110001111, 1101010101001110 1111001011001001, 1100000000110111
6	1111100111100101, 1110000110111000 1100010000111101, 0111001000001010
7	1011001100101100, 1101000010110111 0100100110101111, 1110111001110011
8	1110111101010011, 0111110111011001 1100111110100110, 1010001000011011
9	1111111001000011, 1101001100011100 1001000100001010, 1011111010010101

3. Определение типа IPv6-адреса. В соответствии с шифром из таблицы 6.5 выбрать IPv6-адреса и определить их тип. В таблице 6.6 записать IPv6-адреса в сокращённом формате в ячейку, соответствующую типу.

Таблица 6.5 – IPv6-адреса для определения типа

Номер третьей цифры шифра	IPv6-адреса
0	2090:03F0:0000:0584:00E3:F700:004B:9200/48 FE80:0000:0000:0000:E9E3:F7FF:FE4B:9295/10 FD03:0000:0500:0030:0000:0000:00DF:0001/7 FF02:0000:0000:0000:0000:0000:0000:0001/8
1	24F8:00E4:5000:0D20:0000:D7FF:0000:0E9A/48 FF02:0000:0000:0000:0000:0000:0000:0002/8 FCFF:0560:0000:0000:1100:FF00:00DF:0045/7 FE80:0000:0000:0000:D7B7:A3FF:FED5:1CA2/10

Продолжение таблицы 6.5

Номер третьей цифры шифра	IPv6-адреса
2	FE80:0000:0000:0000:1EF9:7CFF:FEA7:1B5E/10 FF02:0000:0000:0000:0000:0000:0000:0001/8 2086:0AC0:FB58:0000:2800:00FF:0000:0000/64 0000:0000:0000:0000:0000:0000:0000:0000/128
3	2011:0500:0077:0000:3D27:0000:0000:6EDC/48 0000:0000:0000:0000:0000:0000:0000:0001/128 FCFF:0020:0CD4:0000:1100:0000:0000:0010/7 FE80:0000:0000:0000:A1E3:BDFF:FED2:B87E/10
4	20AA:00FD:0010:01F0:A1E3:BDFF:FED2:B87E/48 FDDE:0200:0000:0000:0100:0000:0020:0D10/7 FF02:0000:0000:0000:0000:0000:0000:0002/8 FE80:0000:0000:0000:FF71:D7FF:FEC8:3E9A/10
5	0000:0000:0000:0000:0000:0000:0000:0001/128 20F0:0A00:0000:01A2:00DE:0000:FEE7:0000/64 FCA5:00DE:0000:0130:0100:00B0:0059:0000/7 FE80:0000:0000:0000:ACDE:D8FF:FEE7:F4CB/10
6	20F0:0B00:F800:0F30:00B4:0000:FE2F:000A/64 FF02:0000:0000:0000:0000:0000:0000:0001/8 0000:0000:0000:0000:0000:0000:0000:0000/128 FE80:0000:0000:0000:28F7:4DFF:FEB2:252C/10
7	0000:0000:0000:0000:0000:0000:0000:0001/128 25D0:00A3:E3B0:0000:5DE6:0000:00F0:6A58/64 FD00:0096:0100:0101:0DF0:2030:0AC0:0000/7 FE80:0000:0000:0000:FBB4:F7FF:FE2F:12EA/10
8	204D:0003:00FD:07CE:1EF9:0000:FEA7:0000/48 FF02:0000:0000:0000:0000:0000:0000:0002/8 FDDF:0A51:0000:0001:0160:2030:0070:0000/7 FE80:0000:0000:0000:3D27:B7FF:FE59:6EDC/10
9	FF02:0000:0000:0000:0000:0000:0000:0001/8 20BA:00CD:2100:80D0:0000:A3FF:0000:1CA2/64 FE80:0000:0000:0000:5DE6:6BFF:FE9C:6A58/10 0000:0000:0000:0000:0000:0000:0000:0000/128

Таблица 6.6 – Результаты определения типа IPv6-адреса

IPv6-адрес	Тип адреса

4. Определить IPv6-адрес посредством процесса EUI-64. Из таблица 6.7 выбрать MAC-адреса в соответствии с шифром и рассчитать для них глобальные и локальные IPv6-адреса. Для полученных IPv6-адресов рассчитать групповой адрес запрашиваемого узла. Результаты расчёта представить в виде таблицы 6.8.

Таблица 6.7 – MAC-адреса для расчёта IPv6-адреса

Номер второй цифры шифра	MAC-адреса	Префикс глобальной маршрутизации	Идентификатор подсети
0	574D.F482.83B7	2050:00DF:AC95::/48	194D
1	1E6C.E747.7AEE	2FA0:0450:0020::/48	2076
2	51D3.87E7.AE57	2630:0FA0:BC00::/48	0AF9
3	FF35.5C39.AC46	2BD0:0003:AC00::/48	06BB
4	ED55.EBF8.869C	2300:004F:58F0::/48	A9E8
5	E495.5D13.360D	2BA1:0AE0:FD80::/48	2DDF
6	FD71.D5B7.3F27	2039:00D4:0BA2::/48	7091
7	D9B2.E864.A41B	2070:05B0:004D::/48	F8F8
8	D282.6E4C.E331	2EB4:AD00:FE00::/48	2135
9	B793.21B7.3D74	2FE1:0500:6070::/48	7A85

Таблица 6.8 – Результаты расчёта IPv6-адреса посредством процесса EUI-64

MAC-адрес	
Глобальный IPv6-адрес	
Локальный IPv6-адрес	
Групповой адрес запрашиваемого узла	

6.3 Содержание отчёта

1. Цель работы, исходные данные из таблиц 6.2, 6.4, 6.5, 6.7.
2. Результаты произведённых расчётов (заполненные таблицы 6.3, 6.6, 6.8).
3. Вывод по работе.
4. Ответы на контрольные вопросы.

6.4 Контрольные вопросы

1. В чём заключаются отличия структуры IPv4- и IPv6-адреса.
2. Что такое шестнадцатеричная система счисления?
3. Какие правила нужно использовать при сокращении IPv6-адреса?
4. Какие выделяют IPv6-адреса?
5. Что такое префикс IPv6-адресов?

6. Какие выделяют типы индивидуальных IPv6-адресов?

7. В чём заключаются отличия локального и глобального IPv6-адресов?

8. Какая последовательность действий при генерации IPv6-адреса с помощью процесса EUI-64?

9. Какие выделяют типы групповых IPv6-адресов?

10. Что такое присвоенные групповые IPv6-адреса?

ПРАКТИЧЕСКАЯ РАБОТА №7
РАЗБИЕНИЕ IPV6-СЕТИ НА ПОДСЕТИ

Цель: овладеть навыками разделения IPv6-сетей на подсети с использованием идентификатора подсети и идентификатора интерфейса.

7.1 Теоретическая часть

Идентификатор подсети IPv6-адреса содержит 16 бит (рисунок 6.4). Разбиение на подсети с использованием 16 бит идентификатора подсети даёт 65 536 возможных подсетей с префиксом /64. Поэтому нет необходимости заимствовать биты из идентификатора интерфейса. Каждая такая IPv6-подсеть содержит примерно 18 квинтиллионов адресов.

Если создавать подсети из идентификатора подсети, достаточно рассчитать шестнадцатеричное число. Например, если выдан IPv6-адрес 2001:0DB8:ACAD::/48, то изменяя шестнадцатеричное значение в четвертом гестете, можно создавать сети с адресом от 2001:0DB8:ACAD:0000::/64 до 2001:0DB8:ACAD:FFFF::/64. Так для сети, представленной на рисунке 7.1, можно выделить следующие сети:

– для сети №1 – 2001:0DB8:ACAD:0000::/64;
– для сети №2 – 2001:0DB8:ACAD:0001::/64;
– для сети №3 – 2001:0DB8:ACAD:0002::/64;
– для сети №4 – 2001:0DB8:ACAD:0003::/64;
– для сети №5 – 2001:0DB8:ACAD:0004::/64.

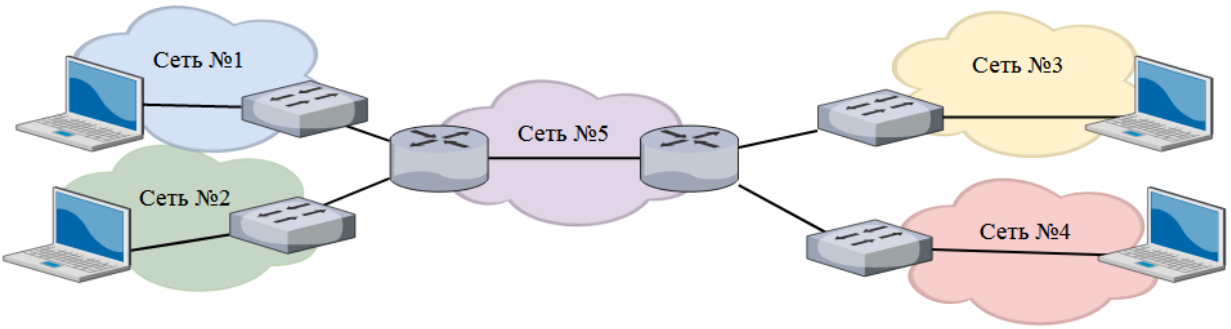

Рисунок 7.1 – Пример сети с IPv6-адресацией для разделения на подсети

Разбиение на подсети с использованием идентификатора интерфейса делается по соображениям безопасности, чтобы уменьшить число узлов в подсети и создавать дополнительные подсети. При расширении идентификатора подсети путём заимствования бит из идентификатора интерфейса рекомендуется создавать подсеть на границе полубайта. Полубайт – это 4 бита или одна шестнадцатеричная цифра. Префикс подсети /64 расширяется на четыре бита или один полубайт до подсети /68. Это позволяет уменьшить размер идентификатора на 4 бита (рисунок 7.2).

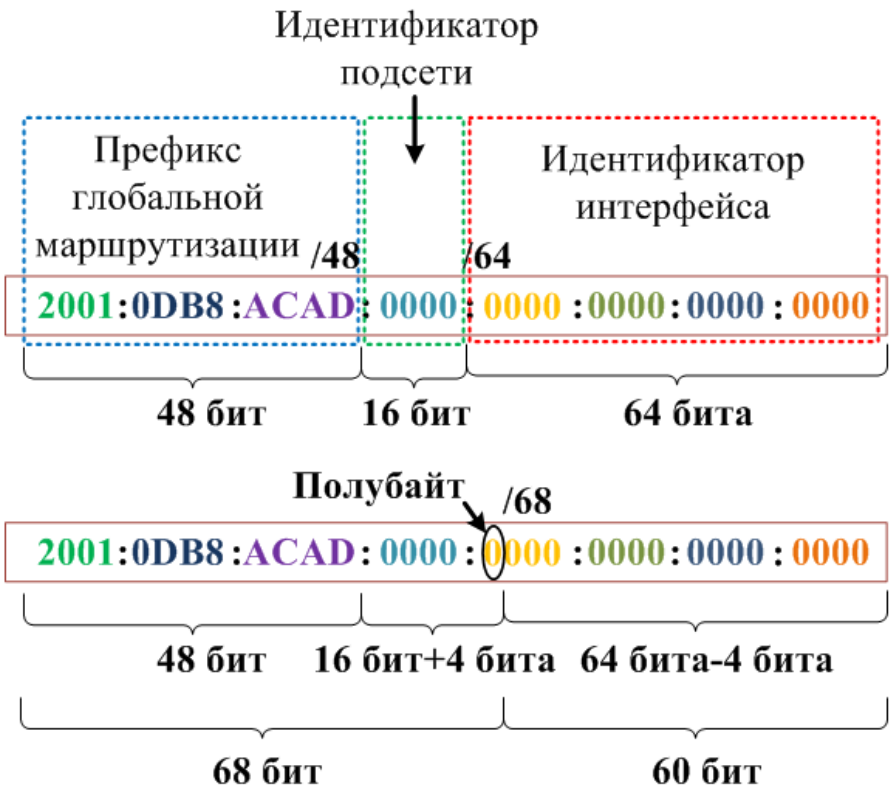

Рисунок 7.2 – Разбиение на подсети с использованием идентификатора интерфейса

Разбиение на подсети по границе полубайта имеет значение только для масок подсетей, выровненных по полубайту. Начиная с /64, масками подсети, выровненными по полубайту, будут являться маски /68, /72, /76, /80 и т. д. Разбиение на подсети по границе полубайта позволяет создать подсети с использованием дополнительного шестнадцатеричного значения. Разбиение на подсети в пределах полубайта снижает вероятность быстрого определения префикса из идентификатора интерфейса. Для примера на рисунке 6.2 в результате разбиения на подсети с использованием полубайта получены следующие IPv6-адреса подсетей:

– 2001:0DB8:ACAD:0000:0000::/68;

– 2001:0DB8:ACAD:0000:1000::/68;

– 2001:0DB8:ACAD:0000:2000::/68 и др.

У последней и предпоследней подсети адреса будут 2001:0DB8:ACAD:0:E000::/68 и 2001:0DB8:ACAD:0:F000::/68 соответственно.

7.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. В соответствии с шифром выбрать из таблицы 7.1 выделенный для сети на рисунке 7.3 IPv6-адрес и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть, начиная с заданного IPv6-адреса, на

подсети **с использованием идентификатора подсети** на необходимое количество подсетей и заполнить таблицу 7.2.

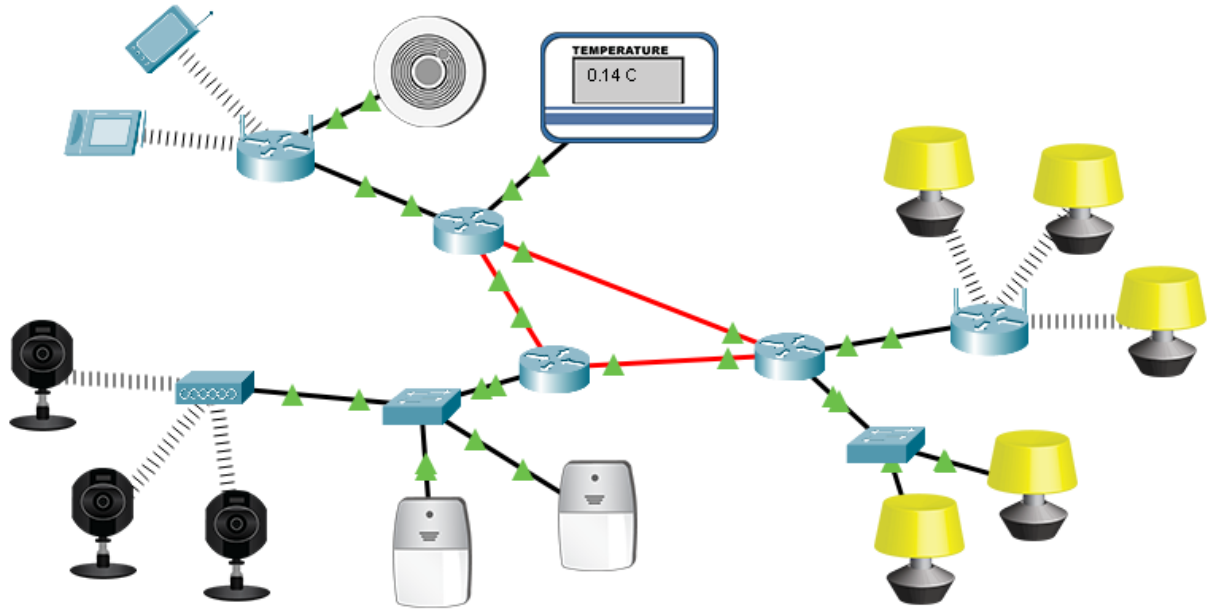

Рисунок 7.3 – Вариант сети для разделения на подсети

Таблица 7.1 – Варианты задания для разделения сети на подсети

Номер второй цифры шифра	Выделенный IPv6-адрес
0	2ABD:9A40:80::/48
1	2900:1:3490::/48
2	2A00:20::/48
3	2CC0::/48
4	2001: DB8:ACAD::/48
5	2490:580:213::/48
6	2C0F:FC89:54::/48
7	28D0:DC:CA10::/48
8	2FEC::170::/48
9	2A06::/48

Таблица 7.2 – Результаты разделения на подсети

Номер подсети	IPv6-адрес подсети с префиксом	IPv6-адрес последнего узла в сети

2. В соответствии с шифром выбрать из таблицы 7.3 выделенный для сети на рисунке 7.4 IPv6-адрес и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть, начиная с заданного IPv6-адреса, на подсети **с использованием полубайта** на необходимое количество подсетей и заполнить таблицу 6.2.

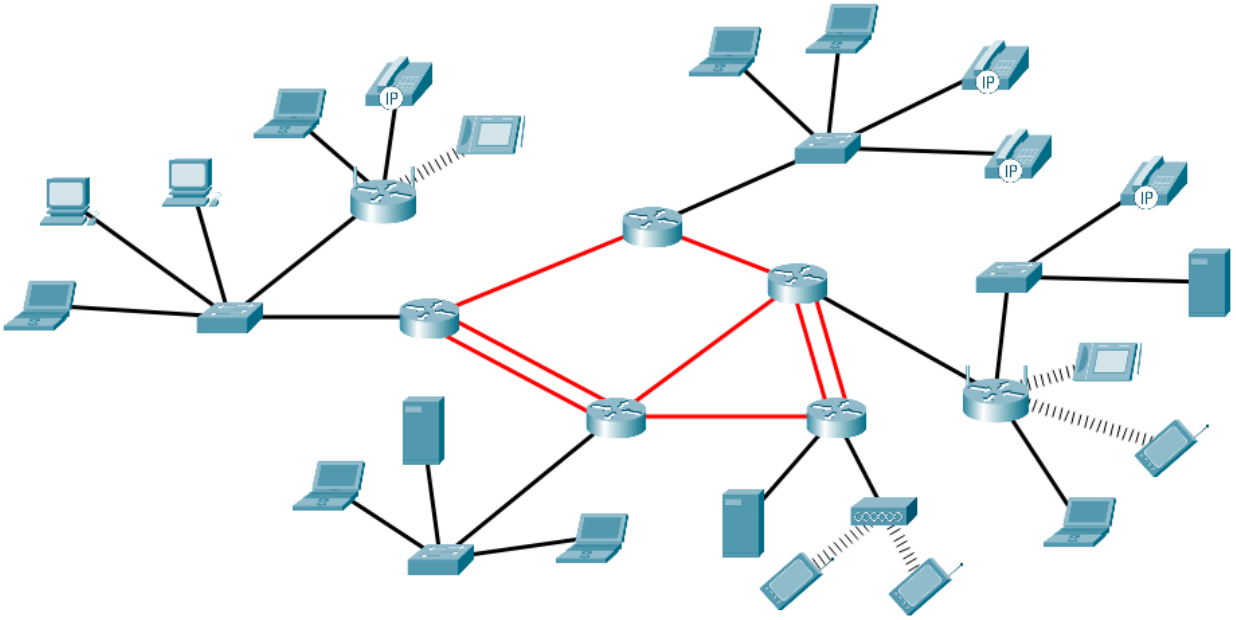

Рисунок 7.4 – Вариант сети для разделения на подсети

Таблица 7.3 – Варианты задания для разделения сети на подсети

Номер второй цифры шифра	Выделенный IPv6-адрес
0	2110:5::1205:900:0:0:0/72
1	2340:3:42:1C::1200:0:0/88
2	2AE9:5::2:1073:80:0:0/92
3	2AD9:123::5000:0:0/84
4	231F:FF::3000:0:0:0/68
5	200D::EA00:0:0:0/72
6	200D:6::500:0:0:0/76
7	2029:AE00::1500:0:0:0/80
8	2ad9::8:0:0:0/84
9	2c60:C:B2:73::3200:0:0/92

3. В соответствии с шифром выбрать из таблицы 7.4 выделенный для сети на рисунке 7.5 IPv6-адрес и количество устройств, находящихся в каждой из подсетей. Разделить заданную сеть, начиная с заданного IPv6-адреса, на подсети **с использованием полубайта** на необходимое количество подсетей и заполнить таблицу 7.2.

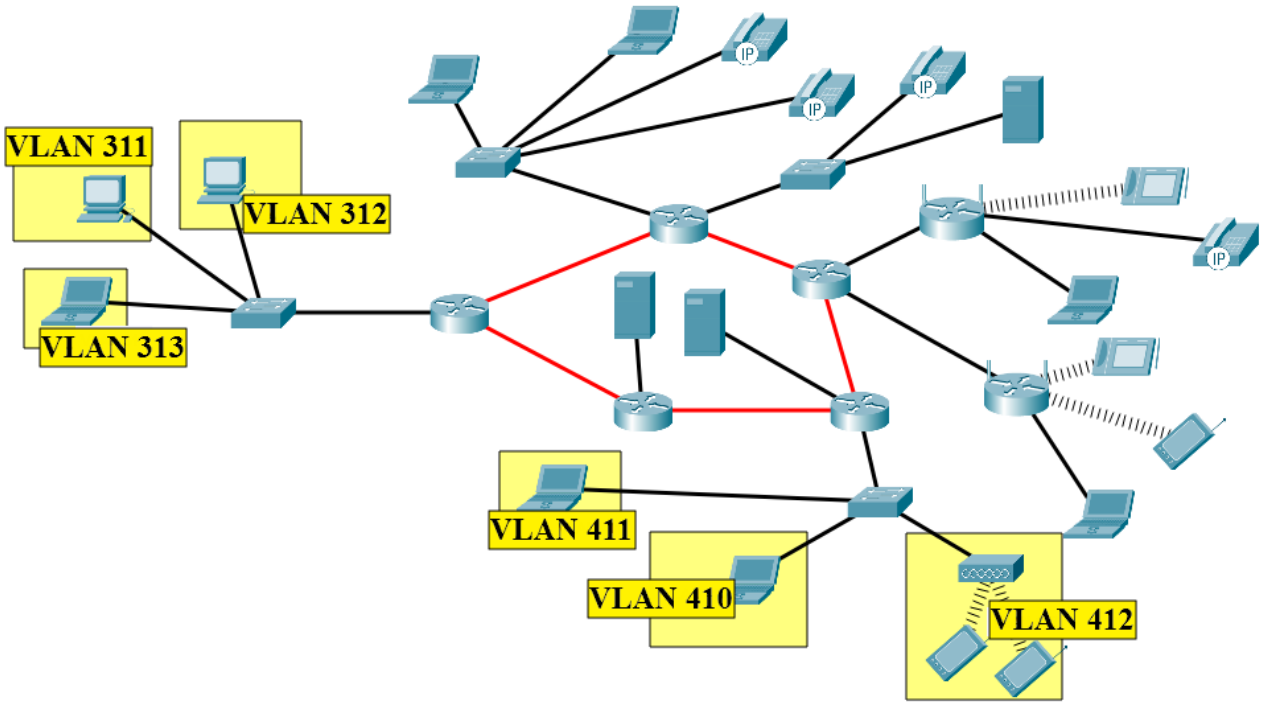

Рисунок 7.5 – Вариант сети для разделения на подсети

Таблица 7.4 – Варианты задания для разделения сети на подсети

Номер второй цифры шифра	Выделенный IPv6-адрес
0	25E6:AD::8000:0/100
1	2606:4700::6800:0/104
2	2A03:2880:F234::B000:0:0/84
3	2460:55:4900:4541:60::/76
4	2001::485:0/112
5	2491:9::5:20:0:0:0/76
6	2E50:9:8::5:0:0/96
7	2331:E::C:D0:50:F0:0/108
8	2300:6:F::60:0:0/92
9	2000:6::C:40:35F:3200:0/104

4. В соответствии с шифром выбрать из таблицы 7.5 IPv6-адреса и длины префиксов, определить IPv6-адреса подсетей и заполнить таблицу 7.6.

Таблица 7.5 – Варианты задания для разделения сети на подсети

Номер второй цифры шифра	IPv6-адрес
0	2305:9:A5:1::8600/60, 2003:C5:A::1BA:F3:120/92, 2017:AA::5:ED:59F:17FF:40/104, 2EED:12:8:2008::34:E:12C0/52

Продолжение таблицы 7.5

Номер второй цифры шифра	IPv6-адрес
1	2590:A:EE:93::AC0F:58:1/92, 2490::848:10:2:9:175/56, 2010:8:C0:10::20DE:9:27/88, 2450::58EC:8:10:AC:123D:CA/40
2	26EC:7:40:AC::130C:E8:1284/88, 25F0:F2::A1:C3:4:19:128/60, 21FC:7::12:A085:81:5:4387/92, 2420:2:40:848::2:9:175/44
3	2ED0:230E::61:A:3:F00:F500/60, 2600:1406:4400::170B:D5C5/104 2110:5:4920:4541:65::F340:1220/44, 2EDB:5::C:11:46:E3:1280/76
4	2253:2DA0:F004:6:F67E:A00C::167/72, 20E0:10::ED29:BB31/100, 23DE:FAC5:1CAD::A56:1129/44, 2340:47AC:45::6816:3A64/116
5	2EDC:4731::6002:A162/104, 2DDA:2:29:1::16F/56, 2301:B340::89:D:A:158:103/76,2E61:B:A0A::31:200:31/44
6	28AD:2670:FACA::A00A:4591:AD/84, 210C:3D60:EE0::FFE1:450/52, 2600:1406:4400::6872:4D2A/100, 2A04:4E42:A129:ABC1::323/44
7	2AB1:AA71::AB89:0:0:112:323/56, 2AA1:BA0A::31:E:F:200:31/104, 2233::109:1005:EB00:1000/120, 2460:55:4900:4541:65::F340:1220/76
8	23EE:AC40:E00D:1606::700C/52, 20C3::AC5:14B9/112, 2284::A9:C130:40:9100/76, 2208:12CA:CC00::100/36
9	225C:CC10:410::200C/40, 2F20:10:A::9:D:2C50/96, 2200:D::1E04:170:C0:ACD0:6630/72, 2267:6::D:60:10:D5:EA00/108

Таблица 7.6 – Результаты расчёта адресов подсетей по заданному IPv6-адресу

Заданный IPv6-адрес	IPv6-адрес подсети	IPv6-адрес последнего узла в сети

7.3 Содержание отчёта

1. Цель работы, исходные данные в соответствии с заданным вариантом из таблиц 7.1 и 7.2.

2. Результаты произведённых расчётов (заполненная таблица 7.2 для всех заданий).

3. Вывод по работе.

4. Ответы на контрольные вопросы.

7.4 Контрольные вопросы

1. Как используется идентификатор подсети для разбиения на IPv6-сети?
2. Как используется идентификатор интерфейса для разбиения на IPv6-сети?
3. В чём заключаются отличительные особенности разбиения на IPv4-сети и IPv6-сети?
4. В чём отличие принципов деления IPv6-сетей на подсети по сравнению с IPv4-сетями?
5. Что такое полубайт? Как он используется в IPv6?

ПРАКТИЧЕСКАЯ РАБОТА №8
РАСЧЁТ СУММАРНЫХ IPV4- И IPV6-МАРШРУТОВ

Цель: научиться определять адреса для настройки суммарных маршрутов в IPv4- и IPv6-сетях.

8.1 Теоретическая часть

Для уменьшения числа записей в таблице маршрутизации можно объединить несколько статических маршрутов в один статический маршрут, который называют суммарным. Это возможно при следующих условиях:

– сети назначения являются смежными и могут быть объединены в один сетевой адрес;

– все статические маршруты используют один и тот же выходной интерфейс или один IP-адрес следующего перехода.

Как видно из рисунка 8.1, маршрутизатору 1 требуется четыре отдельных статических маршрута для подключения к сетям в диапазоне 172.20.0.0/16–172.23.0.0/16. Вместо этого можно настроить один суммарный статический маршрут, который будет обеспечивать подключение к этим сетям.

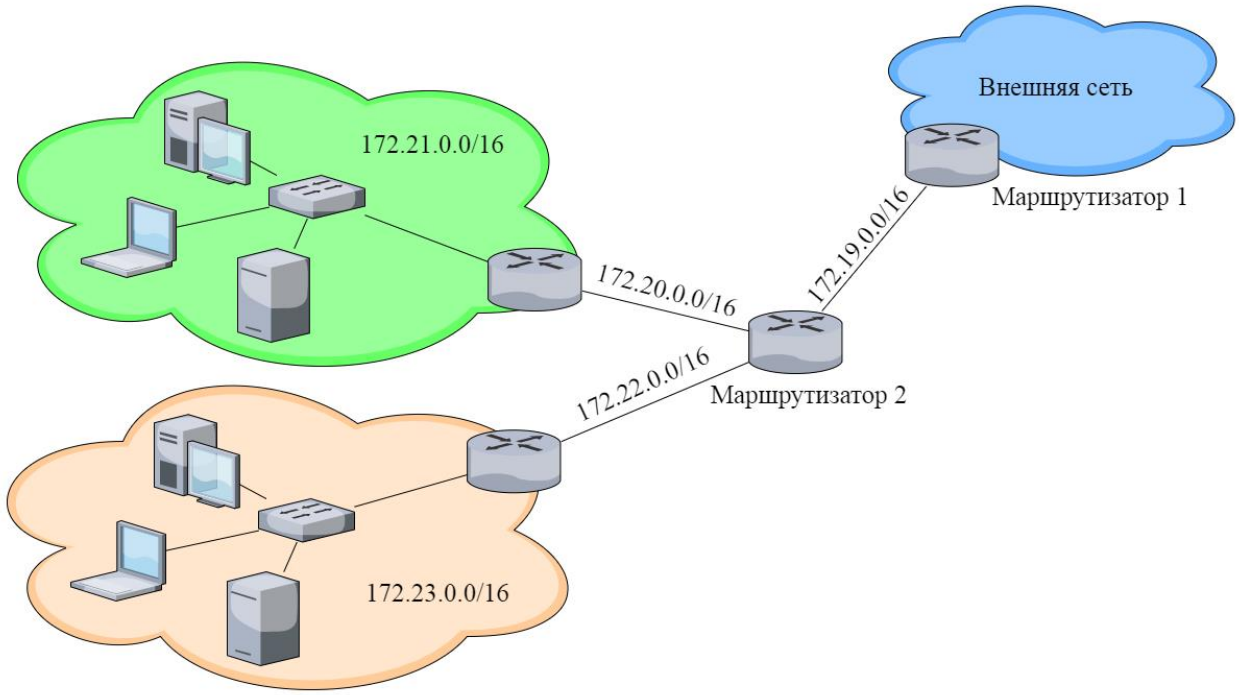

Рисунок 8.1 – Пример сети с суммарным статическим маршрутом

Объединение сетей в один адрес и маску выполняется в три этапа.

1. Запись сетей в двоичном формате. На рисунке 8.2 перечислены сети в диапазоне от 172.20.0.0/16 до 172.23.0.0/16 в двоичном формате.

2. Подсчёт количества крайних слева совпадающих бит для определения маски суммарного маршрута. На рисунке 8.2 приведены 14 крайних слева совпадающих бит. Они составляют префикс /14 и маску подсети 255.252.0.0 для суммарного маршрута.

3. Копирование совпадающих бит и добавление нулевых бит для определения суммарного сетевого адреса. На рисунке 8.2 показано, что совпадающие биты с конечными нулями образуют сетевой адрес 172.20.0.0. Четыре сети (172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16 и 172.23.0.0/16) можно объединять в один сетевой адрес 172.20.0.0/14.

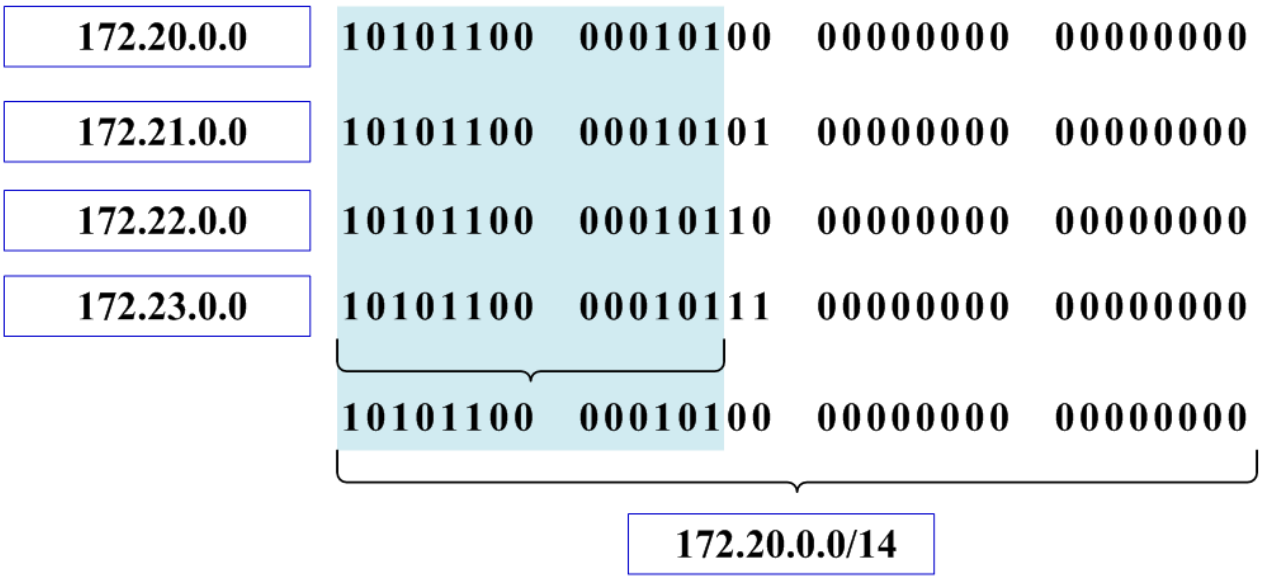

Рисунок 8.2 – Пример расчёта суммарного статического маршрута

Объединение IPv6-адресов схоже с объединением адресов IPv4, за исключением того, что адреса IPv6 составляют 128 бит и написаны в шестнадцатеричном коде. Для объединения требуется несколько дополнительных шагов в связи с сокращённой формой адресов IPv6 и преобразованием в шестнадцатеричный код.

Объединение сетей IPv6 в один префикс и длину префикса IPv6 выполняется в шесть этапов, как показано на рисунке 8.3.

1. Создание списка сетевых адресов (префиксов) для определение части IPv6-адреса.

2. Расширение записи IPv6, в случае если он записан в сокращённом виде.

3. Преобразование различающихся частей из шестнадцатеричного в двоичный код.

4. Подсчёт количества крайних слева совпадающих бит для определения длины префикса суммарного маршрута.

5. Выделение совпадающих бит и добавление нулевых бит для определения суммарного сетевого адреса (префикса).

6. Преобразование части в двоичном коде обратно в шестнадцатеричный, присоединение префикса суммарного маршрута

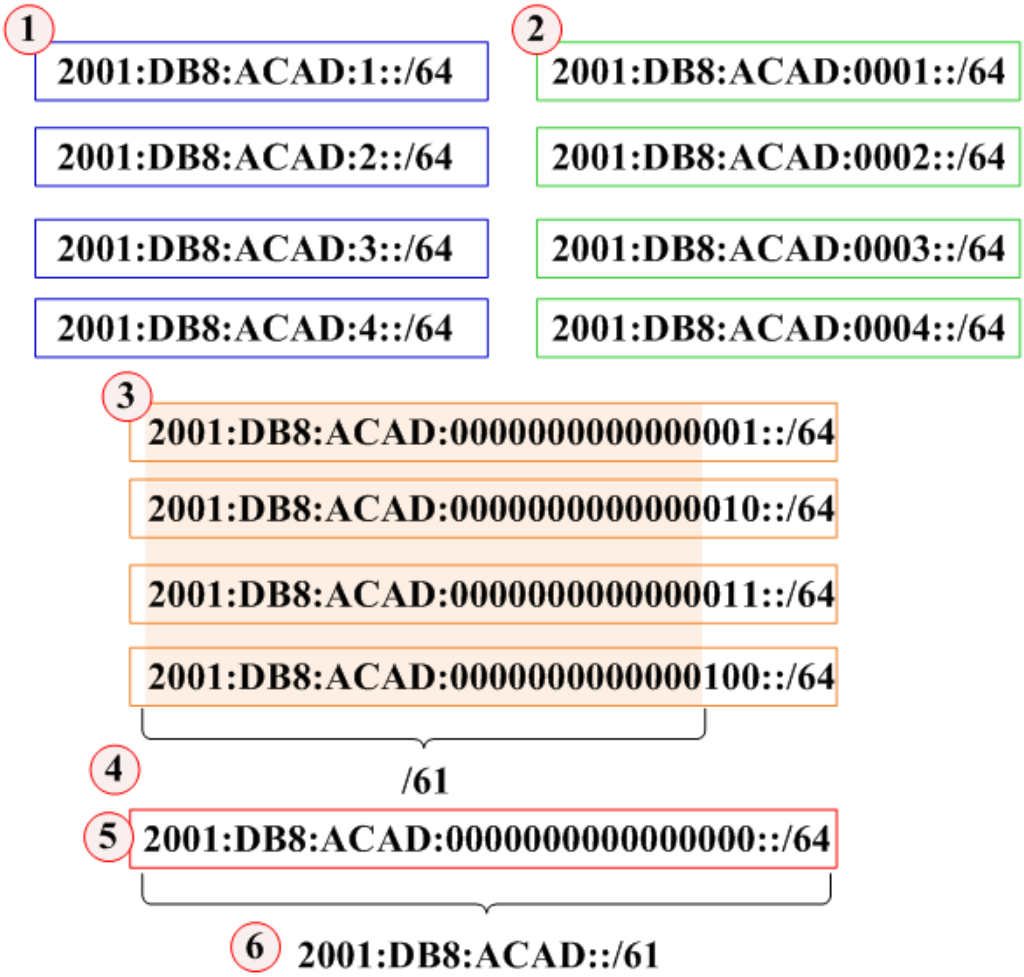

Рисунок 8.3 – Расчёт суммарного IPv6-маршрута

8.2 Практическое задание

В данной практической работе необходимо выполнить представленные ниже задания.

1. В соответствии с шифром выбрать из таблицы 8.1 IPv4-адреса устройств и определить IPv4-адреса сетей, к которым они относятся. Рассчитать суммарный IPv4-адрес для настройки на заданном в таблице 8.1 маршрутизаторе и записать команду для его настройки на заданном маршрутизаторе. Результаты расчёта представить в форме таблицы 8.2.

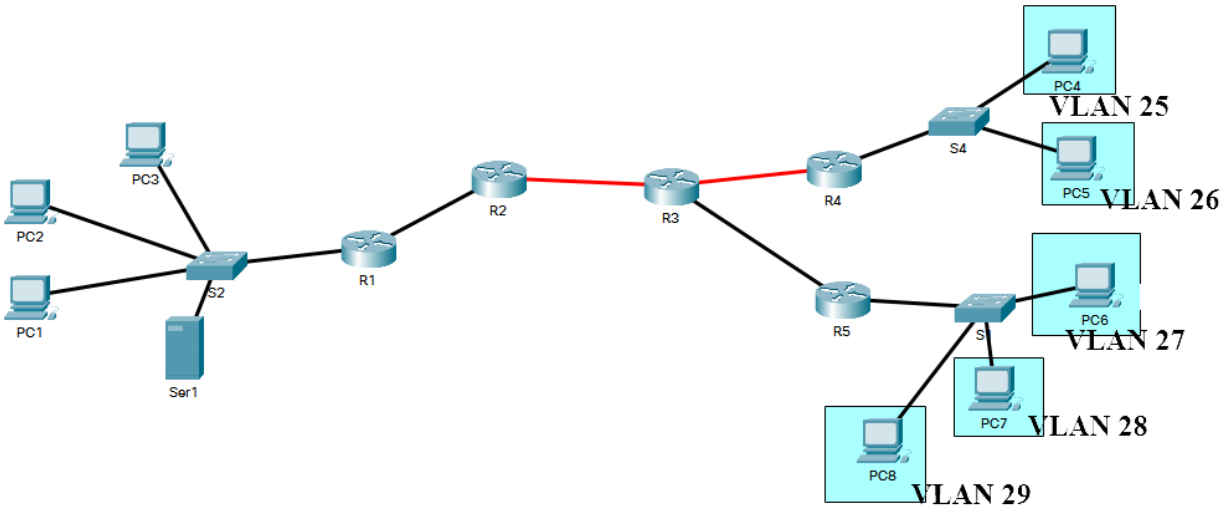

Рисунок 8.4 – Вариант сети для расчёта суммарного маршрута

Таблица 8.1 – Варианты задания для расчёта суммарного IPv4-маршрута

Номер первой цифры шифра	IPv4-адрес устройства				Номер маршрутизатора
	R1	R3	PC4–PC8		
0	192.168.192.109/30 192.168.192.44/28	192.168.192.98/30 192.168.192.101/30 192.168.192.106/30	PC4 PC5 PC6 PC7 PC8	192.168.192.28/28 192.168.192.90/28 192.168.192.72/28 192.168.192.58/28 192.168.192.12/28	R1
1	192.168.64.50/26 192.168.65.6/30	192.168.65.2/30 192.168.64.254/30 192.168.64.249/30	PC4 PC5 PC6 PC7 PC8	192.168.64.237/28 192.168.64.243/29 192.168.64.200/27 192.168.64.150/26 192.168.64.100/26	R5
2	192.168.201.109/30 192.168.201.82/28	192.168.201.98/30 192.168.201.102/30 192.168.201.105/30	PC4 PC5 PC6 PC7 PC8	192.168.201.11/28 192.168.201.19/28 192.168.201.76/28 192.168.201.62/28 192.168.201.38/28	R3
3	192.168.59.110/30 192.168.59.88/28	192.168.59.97/30 192.168.59.101/30 192.168.59.105/30	PC4 PC5 PC6 PC7 PC8	192.168.59.20/28 192.168.59.10/28 192.168.59.66/28 192.168.59.60/28 192.168.59.40/28	R4
4	192.168.41.137/30 192.168.41.35/26	192.168.41.134/30 192.168.41.141/30 192.168.41.146/30	PC4 PC5 PC6 PC7 PC8	192.168.41.84/27 192.168.41.100/28 192.168.41.114/29 192.168.41.124/29 192.168.41.129/30	R1

Продолжение таблицы 8.1

Номер первой цифры шифра	IPv4-адрес устройства				Номер маршрутизатора
	R1	R3	PC4–PC8		
5	192.168.128.60/26 192.168.129.6/30	192.168.129.2/30 192.168.128.254/30 192.168.128.249/30	PC4 PC5 PC6 PC7 PC8	192.168.128.235/28 192.168.128.245/29 192.168.128.220/27 192.168.128.130/26 192.168.128.120/26	R5
6	172.20.140.97/30 192.168.91.12/28	172.20.140.110/30 172.20.140.101/30 172.20.140.105/30	PC4 PC5 PC6 PC7 PC8	192.168.91.18/28 192.168.91.38/28 192.168.91.90/28 192.168.91.74/28 192.168.91.54/28	R4
7	192.168.72.109/30 192.168.72.90/28	192.168.72.98/30 192.168.72.102/30 192.168.72.105/30	PC4 PC5 PC6 PC7 PC8	192.168.72.27/28 192.168.72.8/28 192.168.72.71/28 192.168.72.56/28 192.168.72.38/28	R2
8	192.168.92.138/30 192.168.92.46/26	192.168.92.133/30 192.168.92.142/30 192.168.92.146/30	PC4 PC5 PC6 PC7 PC8	192.168.92.94/27 192.168.92.109/28 192.168.92.115/29 192.168.92.125/29 192.168.92.130/30	R1
9	172.20.211.98/30 192.168.211.83/28	172.20.211.109/30 172.20.211.102/30 172.20.211.106/30	PC4 PC5 PC6 PC7 PC8	192.168.211.73/28 192.168.211.13/28 192.168.211.23/28 192.168.211.53/28 192.168.211.35/28	R1

Таблица 8.2 – Расчёт суммарного IPv4-адреса

IPv4-адреса сетей в десятичной СС	IPv4-адреса сетей в двоичной СС
Суммарный сетевой адрес в двоичной СС	
Суммарный сетевой адрес в десятичной СС	

2. В соответствии с шифром выбрать из таблиц 8.3, 8.4 IPv4-адреса устройств и определить IPv4-адреса сетей, к которым они относятся. Рассчитать суммарный IPv4-адрес для настройки на заданном в таблице 8.3 маршрутизаторе и записать команду для его настройки на заданном маршрутизаторе. Результаты расчёта представить в форме таблицы 8.2.

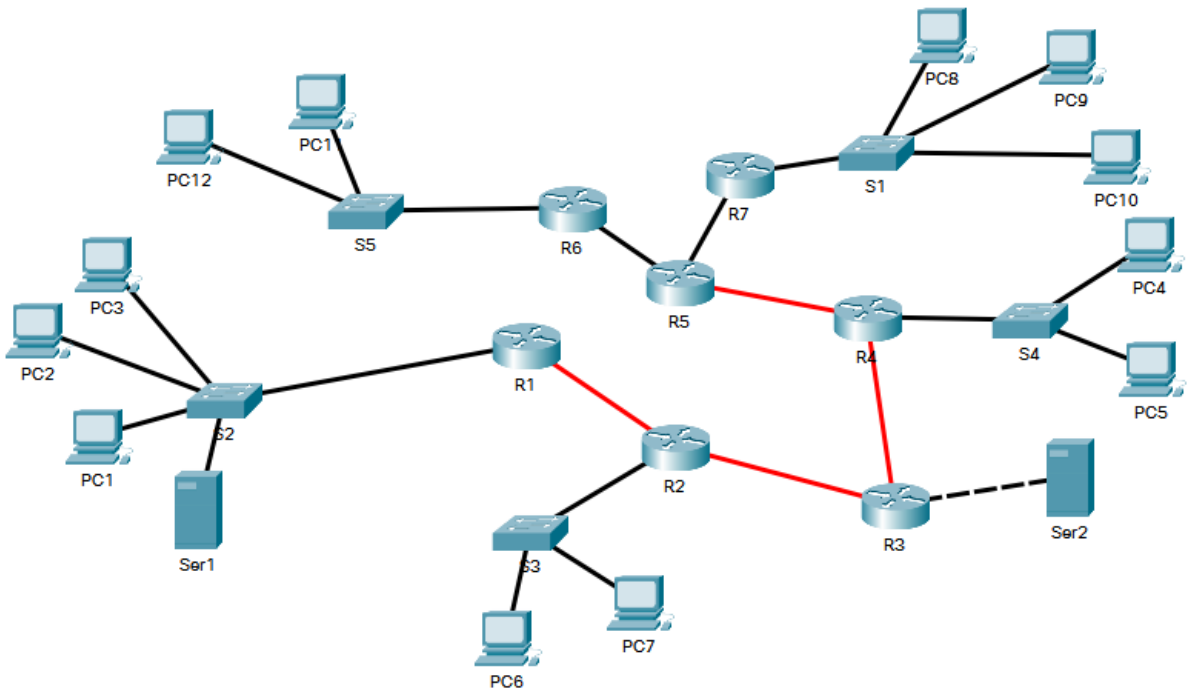

Рисунок 8.5 – Вариант сети для разделения на подсети

Таблица 8.3 – Варианты задания для расчёта суммарного IPv4-маршрута

Номер третьей цифры шифра	IPv4-адреса устройств		Номер маршру-тизатора
	R2	R4	
0	172.20.135.118/30 172.20.135.122/30 172.20.135.100/28	172.20.135.130/30 172.20.135.126/30 172.20.134.250/24	R5
1	172.21.71.125/30 172.21.71.130/30 172.21.71.90/27	172.21.71.118/30 172.21.71.122/30 172.21.70.58/24	R4
2	172.22.103.126/30 172.22.103.122/30 172.22.103.11028	172.22.103.134/30 172.22.103.130/30 172.22.102.140/24	R3
3	172.24.39.142/30 172.24.39.133/30 172.24.39.70/27	172.24.39.125/30 172.24.39.130/30 172.24.39.50/26	R1
4	172.25.24.54/30 172.25.24.50/30 172.25.19.65/23	172.25.24.62/30 172.25.24.42/30 172.25.21.251/23	R6
5	172.26.215.38/30 172.26.215.49/30 172.26.211.25/23	172.26.215.42/30 172.26.215.46/30 172.26.205.57/22	R1
6	172.30.165.38/30 172.30.165.62/30 172.30.148.77/28	172.30.165.65/30 172.30.165.54/30 172.30.145.27/23	R6

Продолжение таблицы 8.3

Номер третьей цифры шифра	IPv4-адреса устройств		Номер маршру-тизатора
	R2	R4	
7	172.39.13.42/30 172.39.13.46/30 172.39.7.142/28	172.39.13.53/30 172.39.13.50/30 172.39.7.150/28	R7
8	172.17.24.53/30 172.17.24.49/30 172.17.19.52/23	172.17.24.61/30 172.17.24.41/30 172.17.21.201/23	R7
9	172.23.55.100/28 172.23.55.121/30 172.23.55.125/30	172.23.54.52/24 172.23.55.133/30 172.23.55.129/30	R2

Таблица 8.4 – Варианты задания для расчёта суммарного IPv4-маршрута

Номер третьей цифры шифра	IPv4-адрес устройств			
	R6	R7	Ser2	PC1
0	172.20.130.200/22 172.20.135.134/30	172.20.133.100/23 172.20.135.138/30	172.20.135.114/30	172.20.135.90/27
1	172.21.71.133/30 172.21.69.15/23	172.21.71.138/30 172.21.65.140/22	172.21.71.114/30	172.21.71.40/26
2	172.22.103.138/30 172.22.98.24/22	172.22.101.45/23 172.22.103.142/30	172.22.103.118/30	172.22.103.90/27
3	172.24.38.10/24 172.24.39.118/30	172.24.37.54/23 172.24.39.121/30	172.24.39.113/30	172.24.34.38/22
4	172.25.24.34/30 172.25.32.145/27	172.25.24.37/30 172.25.22.83/24	172.25.24.70/30	172.25.17.241/23
5	172.26.215.62/30 172.26.202.203/22	172.26.215.66/30 172.26.209.62/23	172.26.215.34/30	172.26.198.25/21
6	172.30.147.120/25 172.30.165.33/30	172.30.146.59/24 172.30.165.50/30	172.30.148.82/30	172.30.148.62/26
7	172.39.6.57/24 172.39.13.58/30	172.39.7.120/25 172.39.13.62/30	172.39.7.162/30	172.39.5.149 /23
8	172.17.24.33/30 172.17.22.49/24	172.17.24.38/30 172.17.32.104/27	172.17.24.69/30	172.17.17.128/23
9	172.23.50.163/22 172.23.55.137/30	172.23.53.48/23 172.23.55.141/30	172.23.55.117/30	172.23.55.90/27

3. В соответствии с первой цифрой шифра выбрать из таблиц 8.5, 8.6 IPv6-адреса устройств и определить IPv6-адреса сетей, к которым они относятся. Рассчитать суммарный IPv6-адрес для настройки на заданном маршрутизаторе на рисунке 8.6. Результаты расчёта представить в форме, показанной на рисунке 8.3.

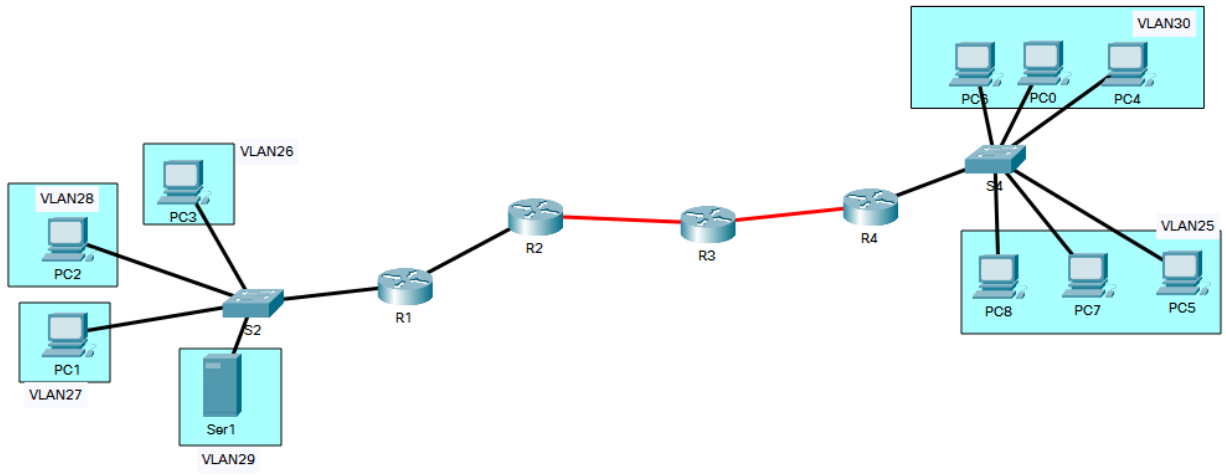

Рисунок 8.6 – Вариант сети для расчёта суммарного маршрута

Таблица 8.5 – Варианты задания для расчёта суммарного IPv6-маршрута для сети, представленной на рисунке 8.6

Номер второй цифры шифра	IPv6-адреса устройства	
	R2	R4
0	28AD:2670::7529:D300:ADBC/84	28AD:2670::4545:4059:159/84
1	2284::1045:CDAE:45:138/76	2284::49:C1DA:A6:193/76
2	2200:D::1E01:125:250:67: F397/72	2200:D::1E02:6170:10:5:6630/72
3	2301:B340::5: D:158: D22/80	2301:B340::FF:0:30: D69F: F74/80
4	2253:2DA0:F004:F:FAC0:4::C87/72	2253:2DA0:F004:1:F230:2::CD86/72
5	2EDB:5::C:7F56:46:E3:ABA9/76	2EDB:5::C:FF3:45:5:EE6E/76
6	2010:8:C0::14: 2C4: AD:38/88	2010:8:C0::1D:20DE: E3:8D/88
7	2460:5::FD06:6: BE94: A6A3/76	2460:5::4:52:D427:EE6E/76
8	26EC:7:40::A0:4545: D6:DB/88	26EC:7:40::AF:4570: B5:68/88
9	2284::AED9:C130: 94:B1/76	2284::BDC:C130: C2:40/76

Таблица 8.6 – Варианты задания для расчёта суммарного IPv6-маршрута

Номер второй цифры шифра	R3	IPv6-адреса устройства		Номер марш-рутизатора
0	28AD:2670::FFD5:1093:DB56 /84	PC1 PC2 PC3 Ser1 PC5 PC4	28AD:2670::AB18:DF51:1087/84 28AD:2670::CD25: 1:D130/84 28AD:2670::454D:157/84 28AD:2670::D6DE:1836:AD/84 28AD:2670::5ADF:4441:3/84 28AD:2670::65E6:FEA1:D084	R1

Продолжение таблицы 8.6

Номер второй цифры шифра	R3	IPv6-адреса устройства		Номер марш-рутизатора
1	2284::A349:C130:40:9100/76	PC1 PC2 PC3 Ser1 PC5 PC4	2284::5C19:C130:40:1F23/76 2284::8C49:C130:40:15C8/76 2284::9A19:C130:40:CC13/76 2284::7A19:C130:40:86D6/76 2284::B210:1280:196:91/76 2284::A3D3:1530:1D:10/76	R3
2	2200:D::1EFF:6170:150:5:EE4 /72	PC1 PC2 PC3 Ser1 PC5 PC4	2200:D::1E04:9170:10:5: D49E/72 2200:D::1E06:8170:10:5: A465/72 2200:D::1E03:D170:10:5: DA29/72 2200:D::1E07:E170:10:5: C57F/72 2200:D::1E0D:1020:20:D0: CE7572 2200:D::1E0E:D530:20:D0: F397/72	R2
3	2301:B340::E:7:158: D49/80	PC1 PC2 PC3 Ser1 PC5 PC4	2301:B340::5E: D:158: D2E/76 2301:B340::4A: D:158: E4A/76 2301:B340::6D: D:158: C7B/76 2301:B340::7C: D:158: A45/76 2301:B340::FF:6:30: 9AE: DEC/80 2301:B340::FF:5:30: A65: C11/80	R4
4	2253:2DA0:F004:3:F120:5::D /72	PC1 PC2 PC3 Ser1 PC5 PC4	2253:2DA0:F004:0:4DE8:7::D761/72 2253:2DA0:F004:0:5F51:8::A4CC/72 2253:2DA0:F004:0:3CC5:F:: BA3/72 2253:2DA0:F004:0:7593:C::ABA9/72 2253:2DA0:F004:6:D552:8:: 9B88/72 2253:2DA0:F004:6:F510:D2::D0C1/72	R1
5	2EDB:5::C:FD6:45:5:EB47/76	PC1 PC2 PC3 Ser1 PC5 PC4	2EDB:5::C:AF51:46:E3:A965/76 2EDB:5::C:8F52:46:E3:CAA9/76 2EDB:5::C:9F53:46:E3:D761/76 2EDB:5::C:BF51:46:E3:CD86/76 2EDB:5::C:F51:45:5: A4CC/76 2EDB:5::C:F42:45:5: D0CA/76	R2
6	2010:8:C0::15: 2C4: E1:3F/88	PC1 PC2 PC3 Ser1 PC5 PC4	2010:8:C0::1A:2C4: A0:A7/88 2010:8:C0::1B: 2C4: E0:6F/88 2010:8:C0::1F: 2C4: D4:27/88 2010:8:C0::1E: 2C4: D6:DB/88 2010:8:C0::12:F152: D4:27/88 2010:8:C0::13:E153: A2:86/88	R3
7	2460:5::DD56:56:98C4:B926 /76	PC1 PC2 PC3 Ser1 PC5 PC4	2460:5::5:B685: 9D:B6: E687/76 2460:5::AD25:5: AF23: B568/76 2460:5::8AC0:F: A484: 8DBC/76 2460:5::9D05:5: C77F: EEDB/76 2460:5::F45:B:7A4:B96F/76 2460:5::705:56: F5:EE/76	R4

Продолжение таблицы 8.6

Номер второй цифры шифра	R3	IPv6-адреса устройства		Номер марш-рутизатора
8	26EC:7:40::AE:4515:A4:84/88	PC1 PC2 PC3 Ser1 PC5 PC4	26EC:7:40::AA:45DA: A2:86/88 26EC:7:40::A9:45C4: E3:8D/88 26EC:7:40::AB:45A8: A0:A7/88 26EC:7:40::A8:4520: E0:6F/88 26EC:7:40::A2:45F5: E1:3F/88 26EC:7:40::A3:4560: 9D:B6/88	R2
9	2284::AFF5:C130: E1:C0/76	PC1 PC2 PC3 Ser1 PC5 PC4	2284::A4A9:C130: AE:99/76 2284::A0A9:C130: BF:9D/76 2284::A7A9:C130: EB:52/76 2284::A1A9:C130: FF:A0/76 2284::ACd5:C130: B5:A1/76 2284::ACD6:C130: 98:DF/76	R4

8.3 Содержание отчёта

1. Цель работы, исходные данные в соответствии с заданным вариантом из таблиц 8.1, 8.3–8.6.
2. Результаты произведённых расчётов в таблице 8.2.
3. Вывод по работе.
4. Ответы на контрольные вопросы.

8.4 Контрольные вопросы

1. Что такое объединение IPv4-сетей в один адрес?
2. Как осуществляется расчёт суммарного статического IPv4-маршрута?
3. Как вычислить суммарный IPv6-маршрут?

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Каменев, Д. Проектируем систему IP-видеонаблюдения / Д. Каменев [Электронный ресурс]. – 2020. – Режим доступа : https://www.iksmedia.ru/articles/3754049-Proektiruem-sistemu-IPvideonablyude.html.

2. Чернобровцев, А. Какие сети нужны для систем видеонаблюдения предприятий? / А. Чернобровцев [Электронный ресурс]. – 2020. – Режим доступа : https://www.osp.ru/nets/2012/04/13017491.

3. Новиков, С. Передача данных видеонаблюдения по IP-сетям / С. Новиков [Электронный ресурс]. – 2020. – Режим доступа : http://citforum.ru/nets/digest/video.

4. Яницкая, Т. С. Глобальные и территориальные инфокоммуникационные сети / Т. С. Яницкая, А. Б. Кузьмичёв. – Тольятти : Изд-во ПВГУС, 2016. – 256 с.

5. Инфокоммуникационные системы и сети. Практикум : учеб. пособие / И. Г. Карпов [и др.]. – Тамбов : Изд-во ФГБОУ ВО «ТГТУ», 2016. – 236 с.

6. Материалы CISCO CCNA (маршрутизация) [Электронный ресурс]. – 2020. – Режим доступа : https://arny.ru/education/ccna-rs/materialyi-cisco-ccna-chasti-1-i-2-kursa-marshrutizatsiya.

7. Ловшук, А. П. Исследование способов обеспечения отказоустойчивой маршрутизации в сетях пакетной коммутации / А. П. Ловшук, Е. А. Шеленок // Учёные заметки ТОГУ. – 2016. – Т. 7, №2. – С. 223 – 230.

8. Инфокоммуникационные сети: энциклопедия. Т. 1 : Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / С. П. Воробьёв [и др.]. – СПб. : Наукоёмкие технологии, 2019. – 739 с.

9. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – СПб. : Питер, 2012. – 960 с.

10. Рубашенков, А. М. Протокол OSPF / А. М. Рубашенков, Д. А. Семёнов // Научный журнал. – №10 (33). – 2018. – С. 20–21.

11. Бирюков, А. Безопасность протокола OSPF / А. Бирюков // Системный администратор. – №7–8. – 2012.

12. Королькова, А. В. Сетевые технологии. Лабораторные работы / А. В. Королькова, Д. С. Кулябов. – М. : РУДН, 2014. – 106 с.

13. Ловшук, А. П. Исследование способов обеспечения отказоустойчивой маршрутизации в сетях пакетной коммутации / А. П. Ловшук, Е. А. Шеленок // Учёные заметки ТОГУ. – 2016. – Т. 7, №2. – С. 223–230.

14. Бабаян, Р. Г. Промышленное видеонаблюдение / Р. Г. Бабаян // Вестник науки – Т. 1, №6 (15). – 2019. – С. 35–37.

15. Ракчеев, А. Ю. Настройка динамической маршрутизации OSPF / А. Ю. Ракчеев // Colloquium-journal. – №5 (57). – 2020. – С. 106–110.

16. Васин, Н. Н. Основы сетевых технологий на базе коммутаторов и маршрутизаторов / Н. Н. Васин. – Интернет-университет информационных технологий, 2011. – 270 с.

17. Королькова, А. В. Сетевые технологии. Лабораторные работы / А. В. Королькова, Д. С. Кулябов. – М. : РУДН, 2014. – 106 с.

18. Телекоммуникационные системы и сети. В 3 т. Т. 3 : Мультисервисные сети : учеб. пособие / В. В. Величко [и др.]. – 2-е изд., стереотип. – М. : Горячая линия. – Телеком, 2015. – 592 с.

19. Гребешков, А. Ю. Вычислительная техника, сети и телекоммуникации : учеб. пособие для вузов / А. Ю. Гребешков. – М. : Горячая линия – Телеком, 2015. – 190 с.

20. Ганжа, В. А. Компьютерные сети. Введение : учеб.-метод. пособие / В. А. Ганжа, В. В. Шиманский. – Минск : БГУИР, 2015. – 155 с.

21. Лэммл, Т. CCNP. Маршрутизация: учебное руководство / Т. Лэммл, Ш. Одом, К. Уоллес ; пер. с англ. В. Пучков. – М. : Лори, 2015. – 485 с.

22. Амато, В. Основы организации сетей Cisco. Т. 1 / В. Амато; пер. с англ. – М. : Изд. дом «Вильямс», 2002. – 512 с.

23. Елисеев, А. И. Технологии маршрутизации : учеб. пособие / А. И. Елисеев, Д. В. Поляков. – Тамбов : Изд-во ФГБОУ ВО «ТГТУ», 2016. – 79 с.

24. Семёнов, Ю. А. Алгоритмы телекоммуникационных сетей. В 3 ч. Ч. 2 : Протоколы и алгоритмы маршрутизации в Internet / Ю. А. Семёнов. – М. : НОУ «ИНТУИТ», 2007. – 1004 с.

25. Цветков, В. Ю. Протоколы внутренней маршрутизации: OSPF и EIGRP : учеб.-метод. пособие / В. Ю. Цветков, К. А. Волков. – Минск : БГУИР, 2017. – 72 с.

Св. план 2022, поз. 24

Учебное издание

Белоусова Елена Сергеевна

АДРЕСАЦИЯ В IPV4- И IPV6-СЕТЯХ. ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать 18.10.2022. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 4,77. Уч.-изд. л. 4,8. Тираж 40 экз. Заказ 189.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск