Северо-Кавказский филиал

Московского технического университета связи и информатики

Кафедра Сетей связи и систем коммутации

Методические указания

к практическим занятиям по теме:

ИЗУЧЕНИЕ ПРИНЦИПОВ АДРЕСОВАНИЯ В IP-СЕТЯХ

Дисциплина: Мультисервисные сети связи.

Ростов-на-Дону

2010

УМР на 2009/2010 учебный год

Методические указания к практическим занятиям

по теме:

ИЗУЧЕНИЕ ПРИНЦИПОВ АДРЕСОВАНИЯ В IP-СЕТЯХ

Дисциплина: Мультисервисные сети связи.

Разработал: профессор кафедры Сети связи и системы коммутации, д.т.н. Нерсесянц Альфред Аванесович

Рассмотрено и одобрено на заседании кафедры Сети связи и системы коммутации 05.05.06.

Протокол №8. Зав. кафедры СССК, доцент - Спасский Б.Г.

ИЗУЧЕНИЕ ПРИНЦИПОВ АДРЕСОВАНИЯ В IP-СЕТЯХ

1. Цель работы: Изучить основные принципы адресования в IP-сетях в протоколах IPv4, включая адресование к сетям, подсетям и отдельным устройствам (хостам).

2. Основные положения системы адресования версии IPv4

Протоколы адресации в версии IPv4 изложена в рекомендациях: RFC 791, RFC 950, RFC 1518.

2.1. IP-адреса.

У каждого хоста и маршрутизатора в Internet есть IP-адрес, состоящий из номера сети и номера хоста (строго говоря, IP-адрес присваивается не всему маршрутизатору, а каждому его порту).

Таблица 1. Структура адресов различных классов

Кл	1-й байт	2-й байт	3-й байт	4-й байт	Диапазон адресов хоста
A	0 № сети	№ хоста			От 1.0.0.0 до 127.255.255.255
B	10 № сети		№ хоста		От 128.0.0.0 до 191.255.255.255
C	110 № сети			№ хоста	От 192.0.0.0 до 223.255.255.255
D	1110 Адрес группы широковещания				От 224.0.0.0 до 239.255.255.255
E	11110 Зарезервировано				От 240.0.0.0 до 247.255.255.255

Все IP-адреса имеют длину 32 бита и используются в полях *Адрес отправителя* и *Адрес получателя* IP-пакетов. Используемые для IP-адреса форматы показаны в табл. 1.

Формат класса D предназначен для многоадресной рассылки. Адреса, начинающиеся с 11110, зарезервированы для будущего применения. В настоящее время с Internet соединены сотни тысяч сетей, и это число удваивается каждый год. Номера сетям во избежание конфликтов назначаются сетевым информационным центром (NIC, Network Information Center).

Численности сетей и хостов в классах A, B и C представлены в табл. 2.

Таблица 2. Числа сетей и хостов в классах

Класс сети	Число сетей	Число хостов
A	126	≈ 16 млн.
B	16382	≈ 65 тыс.
C	≈ 2 млн.	254

Сетевые адреса, являющиеся 32-разрядными числами, записываются в виде четырёх десятичных чисел, соответствующих отдельным байтам, разделённых точками. Например, шестнадцатеричный адрес C0290614 записывается как 192.41.6.20. Наименьший IP-адрес выглядит как 0.0.0.0 (32 нулевых разряда), а наибольший – 255.255.255.255 (32 единичных разряда).

IP-адрес 0.0.0.0 используется хостом только при загрузке. IP-адреса с нулевым номером сети обозначают текущую сеть. Такой адрес позволяет машинам обращаться к хостам собственной сети, не зная её номера (но они должны знать её класс и сколько нулей использовать). Адрес, состоящий изо всех единиц, обеспечивает широковещание в пределах текущей (обычно локальной) сети. Адреса, в которых указана сеть, но со всеми единицами в поле номера хоста, обеспечивают широковещание в пределах любой удалённой локальной сети, соединённой с Internet.

Адрес 192.168.0.0 (адрес класса B) используется только внутри локальных сетей. При выдаче пакета в Internet этот адрес (адрес отправителя) заменяется на IP-адрес выходного маршрутизатора. Аналогично, при входе пакета в ЛВС IP-адрес входного маршрутизатора заменяется на адрес вида 192.168.0.0. Процедуру замены адресов выполняет специальный сервер-посредник (прокси-сервер).

Наконец, все адреса вида 127.xx.yy.zz зарезервированы для тестирования сетевого программного обеспечения методом шлейфа. Отправляемые по этому адресу пакеты не попадают в линию, а обрабатываются локально как входные пакеты.

2.2. Подсети

Как было показано, у всех хостов данной сети должен быть один и тот же номер сети. Это свойство IP-адресации может вызвать проблемы при росте сети. Например, представьте предприятие, начавшее подключение к Internet с сети класса C. Со временем число компьютеров предприятия может превысить 254 и потребуется вторая сеть класса C или даже класса B. В каждой из новых сетей должен быть свой сетевой адрес и свой маршрутизатор. Всё это существенно усложняет управление сетями предприятия, особенно в части актуальности внутренних адресов сетей предприятия для Internet (Обязательный контакт с Сетевым информационным центром – NIC).

Решение этих проблем состоит в разбиении сети на несколько частей для внутреннего использования, но так, чтобы для внешнего мира эта сеть продолжала действовать как единая сеть. Эти части сети принято называть «подсетями».

Например, в табл. 3 представлен адрес сети класса В предприятия, в котором из 16-и разрядов 3-го и 4-го байтов адреса 6 разрядов выделены для обозначения адресов подсетей.

Таблица 3. Иерархическая структура адреса: Сеть-Подсеть-Хост

Адрес сети		Адрес подсети	Адрес хоста
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		1 1 1 1 1 1	1 1 1 1 1 1 1 1 1 1
1 0	0 0 0 0 1 0 0 0 1 1 0 0 1 0	0 0 1 0 0 0	0 0 0 0 1 0 0 1 0 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		0 0 0 0 0 0 0 0 0 0	
130	50	8	36

IP-адрес представлен в двоичной (3-я строка) и десятичной (5-я строка) формах. В четвёртой строке приведена маска подсети, с помощью которой можно отделить номер подсети от номера хоста. В таблице представлен 4-х байтный IP-адрес 130.50.8.36. С помощью маски 3-й байт адреса разделяется на части: 6 разрядов относятся к адресу подсети (подсеть № 8), а два разряда вместе с двумя разрядами 4-го байта определяют адрес хоста (№ 36). Данная маска содержит 22 единицы и 10 нулей. В четырёхбайтном представлении это 255.255.252.0. Более компактно адрес с маской представляется в виде адреса с сетевым префиксом: 130.50.32.36/22. Таким образом, одна и та же маска может быть представлена в трёх вариантах:

- в двоичном коде – 11111111111111111111110000000000;
- в десятичном коде – 255.255.252.0;
- в виде сетевого префикса /22 (число левых единиц).

Чтобы понять, как функционируют подсети, следует рассмотреть процесс обработки IP-пакетов маршрутизатором. У каждого маршрутизатора есть таблица маршрутизации (ТМ), содержащая IP-адреса сетей и IP-адреса хостов. Адреса сетей позволяют получать доступ к удалённым сетям, а адреса хостов – обращаться к локальным хостам. С каждым адресом связан сетевой интерфейс данного маршрутизатора (например, адрес порта), применяющийся для получения доступа к пункту назначения и другая служебная информация.

Когда IP-пакет поступает на маршрутизатор, адрес получателя, указанный в пакете, ищется в ТМ. Если пакет отправляется в удалённую сеть, он пересылается следующему маршрутизатору по интерфейсу, указанному в ТМ. Если пакет предназначен локальному хосту (т.е. в локальной сети маршрутизатора), он посылается напрямую адресату. Если номер сети, в которую посылается пакет, в ТМ не содержится, пакет пересылается маршрутизатору по умолчанию, с более

подробными таблицами. Такой алгоритм означает, что каждый маршрутизатор должен учитывать только другие сети и локальные хосты, а не пары «сеть, хост», что значительно сокращает размер ТМ.

При разбиении сети на подсети ТМ изменяются. При этом к ним добавляются новые строки вида «эта сеть, подсеть, 0» и «эта сеть, эта подсеть, хост». Таким образом, маршрутизатор в каждой подсети знает, как получить доступ ко всем остальным подсетям и ко всем хостам своей подсети. Подробности о хостах других подсетей ему знать не нужно. Всё что нужно маршрутизатору – это, определив класс сети, наложить маску подсети на IP-адрес пакета, чтобы, удалив номер хоста, получить номер подсети, который затем ищется в ТМ. Например, пакет, направляющийся по адресу 130.50.15.6, прибывает на маршрутизатор подсети 5. После наложения маски 22 его адрес превращается в 130.50.12.0, что означает подсеть 3. Адрес этой подсети находится в ТМ и маршрутизатор подсети 5 избавлен от необходимости знать хосты подсети 3. Этими хостами займётся маршрутизатор 3-й подсети (именно в его ТМ содержатся адреса этих хостов).

Для задания многоуровневой структуры подсетей используются маски переменной длины. Например, адрес с префиксом 130.50.15.6/16 на верхнем (базовом) уровне сети, на 1-м уровне подсетей изменяется на адрес 130.50.15.6/20, т.е. для выбора одной из 16-и подсетей выделены 4 разряда (с 16-го по 19-й). В данном примере это подсеть № 0. Если на втором уровне подсетей необходимо организовать до 32-х подсетей, то маска изменится – 130.50.15.6/25, т.е. выделяется 5 разрядов (с 20-го по 24-й). В данном примере это подсеть № 30.

2.3. Выводы

Протокол IP решает задачу доставки сообщений между узлами составной сети. Поскольку он является дейтаграммным, то не дает никаких гарантий надежной доставки сообщений.

Важной особенностью протокола IP, отличающей его от других сетевых протоколов, например от сетевого протокола IPX, является его способность выполнять динамическую фрагментацию пакетов при передаче их между сетями с различными, максимально допустимыми значениями длины поля данных кадров (MTU).

Максимальная длина IP-пакета составляет 65 535 байт. Заголовок обычно имеет длину 20 байт и содержит информацию о сетевых адресах отправителя и получателя, параметры фрагментации, время жизни пакета, контрольную сумму и некоторые другие параметры.

Вид таблицы IP-маршрутизации зависит от конкретной реализации маршрутизатора. Несмотря на значительные внешние различия выводимых на экран таблиц, все они включают два обязательных поля, без которых невозможно выполнять маршрутизацию, — это поля адресов назначения и следующего маршрутизатора.

Записи в таблицу маршрутизации могут поступать из разных источников. Во-первых, в результате конфигурирования программное обеспечение стека TCP/IP заносит в таблицу записи о непосредственно подключенных сетях и маршрутизаторах по умолчанию, а также записи об особых адресах. Во-вторых, администратор вручную заносит записи о специфических маршрутах и о маршруте по умолчанию. В-третьих, протоколы маршрутизации автоматически заносят в таблицу динамические записи об имеющихся маршрутах.

Эффективным средством структуризации IP-сетей являются маски. Маски позволяют разделить одну сеть на несколько подсетей или объединить несколько сетей в одну более крупную сеть.

Значительная роль в будущем IP-сетей отводится технологии бесклассовой междоменной маршрутизации (CIDR), которая решает две основные задачи. Первая состоит в более экономном расходование адресного пространства, вторая — в уменьшении числа записей в таблицах (одна запись может представлять множество сетей, объединенных общим префиксом).

В начале 90-х годов стек протоколов TCP/IP столкнулся с серьезными проблемами, которые нельзя было решить без изменения формата IP-пакета и логики обработки полей заголовка IP-пакетов. В результате сообщество Интернета решило создать новую версию протокола IP (IPv6), выбрав в качестве основных целей модернизации создание масштабируемой схемы адресации; повышение пропускной способности сети за счет сокращения работ, выполняемых маршрутизаторами; предоставление гарантий качества транспортных услуг; обеспечение защиты данных, передаваемых по сети. Краткие сведения о протоколе IPv6 представлены в приложении.

Ниже рассмотрено несколько примеров использования IP-адресации.

3. Примеры назначения адресов подсетям и устройствам

Пример 1. 512 подсетей (IP-адрес класса B)

Предположим, что организации для ее корпоративной сети назначен сетевой номер 140.25.0.0/16. При этом организация планирует разделить сеть на несколько подсетей, каждая из которых должна поддерживать до 60 устройств.

Определение маски подсети и расширенного сетевого префикса

На первом шаге необходимо определить число битов, требуемых для идентификации 60 устройств в подсети. Ранее мы показали, что адрес конкретного устройства имеет определенное двоичное представление и верхняя граница адресного пространства для устройств одной подсети представляется степенью двойки. Это, в частности, означает, что невозможно выделить адресное прост-

ранство ровно для 60 устройств, так как 60 — не степень двойки. Ближайшая сверху степень — это 64=2 . На самом деле, к числу устройств нужно прибавить 2, так как адреса, содержащие только нули или только единицы, не используются для адресации отдельных устройств. Здесь мы видим, что необходимый задел есть: 60+2=62<64. Однако, удовлетворяя существующие на сегодня потребности по числу рабочих мест, такой выбор не оставляет адресного пространства для возможного роста подсети (в наличии имеется всего 2 свободных адреса). И хотя следующая степень двойки равна 128 (2) и число адресов устройств будет равно 2-2=126, то есть намного больше требуемого в настоящий момент, сетевой администратор выбирает именно это адресное пространство и получает 66 (126-60) дополнительных адресов для каждой подсети. Такой выбор означает, что поле адреса устройства займет 7 бит.

На втором шаге определяется маска подсети и длина расширенного сетевого префикса. Так как для идентификации устройств из 32-разрядного IP-адреса решено выделить 7 бит, то получаем расширенный сетевой префикс равный /25 (32-7=25). Такой 25-разрядный расширенный сетевой префикс может быть выражен в десятично-точечном представлении маской подсети 255.255.255.128. На рис. 1 показана запись маски подсети и расширенного сетевого префикса. См. также аналогичные рисунки в части II «Стек протоколов TCP/IP».

	Сетевой префикс		Номер подсети	Номер устройства
140.25.0.0/16	10001100.	00011001.	00000000.0	140.25.0.0/16
255.255.255.128	11111111.	11111111.	11111111.1	255.255.255.128
или эквивалентная запись				
	25-битовый расширенный сетевой префикс			Номер устройства
140.25.0.0/25	10001100.	100011001.	00000000.0	140.25.0.0/25

Рис. 1. Определение маски подсети и расширенного сетевого префикса

Мы видим, что 25-разрядный расширенный префикс предполагает выделение 9 бит для идентификации подсетей. Теперь можно вычислить количество идентифицируемых подсетей: 2^9=512, то есть девять битов позволяют назначить адреса 512 подсетям. Понятно, что сетевой администратор имеет некоторую свободу действий при определении соотношения числа идентифицируемых устройств и числа подсетей. Выделяя большее число бит в поле идентификации устройств, администратор может включать в подсеть больше устройств. С другой стороны, чем меньше бит выделено для идентификации устройств, тем больше подсетей может создать администратор. Все зависит от текущих требований организации.

Определение номеров подсетей

Выделенные 512 подсетей пронумеруем от 0 до 511. Если выделить 9 разрядов для двоичного представления десятичных чисел от 0 до 511, то получим: 0

$(000000000)_2$, 1 $(000000001)_2$, 2 $(000000010)_2$, 3 $(000000011)_2$,..., 511 $(111111111)_2$. Например, для определения подсети номер 3 (#3) сетевой администратор размещает двоичное представление числа 3 $(000000011)_2$ в 9 битах номера подсети. Номера подсетей для рассматриваемого примера приводятся ниже. В каждом адресе курсивом выделен расширенный сетевой префикс всего адреса, в то время как 9-битовое представление поля номера подсети выделено полужирным шрифтом.

Базовая сеть: *10001100.00011001*.**00000000.0**0000000 = 140.25.0.0/16
Подсеть #0: *10001100.00011001*.**00000000.0**0000000 = 140.25.0.0/25
Подсеть #1: *10001100.00011001*.**00000000.1**0000000 = 140.25.0.128/25
Подсеть #2: *10001100.00011001*.**00000001.0**0000000 = 140.25.1.0/25
Подсеть #3: *10001100.00011001*.**00000001.1**0000000 = 140.25.1.128/25
Подсеть #4: *10001100.00011001*.**00000010.0**0000000 = 140.25.2.0/25
Подсеть #5: *10001100.00011001*.**00000010.1**0000000 = 140.25.2.128/25
Подсеть #6: *10001100.00011001*.**00000011.0**0000000 = 140.25.3.0/25
Подсеть #7: *10001100.00011001*.**00000011.1**0000000 = 140.25.3.128/25
Подсеть #8: *10001100.00011001*.**00000100.0**0000000 = 140.25.4.0/25
Подсеть #9: *10001100.00011001*.**00000100.1**0000000 = 140.25.4.128/25
…
Подсеть #510: *10001100.00011001*.**11111111.0**0000000 = 140.25.255.0/25
Подсеть #511: *10001100.00011001*.**11111111.1**0000000 = 140.25.255.128/25

Определение адресов устройств

Итак, администратор выделил 7 битов для идентификации устройств в каждой подсети. Это означает, что каждая подсеть имеет 126 адресов для идентификации устройств. Устройства в подсети нумеруются от 1 до 126. Приведем перечень адресов устройств для подсети #3. При этом курсивом выделен расширенный сетевой префикс, в то время как полужирным шрифтом показано 7-разрядное поле номера устройства.

Подсеть #3: *10001100.00011001.00000001.1***0000000** = 140.25.1.128/25
Устройство #1 *10001100.00011001.00000001.1***0000001** = 140.25.1.129/25
Устройство #2 *10001100.00011001.00000001.1***0000010** = 140.25.1.130/25
Устройство #3 *10001100.00011001.00000001.1***0000011** = 140.25.1.131/25
Устройство #4 *10001100.00011001.00000001.1***0000100** = 140.25.1.132/25
Устройство #5 *10001100.00011001.00000001.1***0000101** = 140.25.1.133/25
Устройство #6 *10001100.00011001.00000001.1***0000110** = 140.25.1.134/25
…
Устройство #62 *10001100.00011001.00000001.1***0111110** = 140.25.1.190/25

Устройство #63 *10001100.00011001.00000001.1***0111111** = 140.25.1.191/25
Устройство #64 *10001100.00011001.00000001.1***1000000** = 140.25.1.192/25
Устройство #65 *10001100.00011001.00000001.1***1000001** = 140.25.1.193/25
…
Устройство #62 *10001100.00011001.00000001.1***0111110** = 140.25.1.190/25
Устройство #63 *10001100.00011001.00000001.1***0111111** = 140.25.1.191/25
Устройство #64 *10001100.00011001.00000001.1***1000000** = 140.25.1.192/25
Устройство #65 *10001100.00011001.00000001.1***1000001** = 140.25.1.193/25

Определение широковещательного адреса

Для подсети #3 широковещательным адресом будет адрес, в котором все биты поля номера устройства установлены в единицу:

*10001100.00011001.00000001.1***1111111** = 140.25.1.255.

Следует отметить, что широковещательный адрес для подсети #3 ровно на единицу меньше базового адреса подсети #4 (140.25.2.0).

Пример 2. 8 подсетей (IP-адрес класса B)

Изменим ситуацию. Пусть организации назначен сетевой адрес 132.45.0.0/16. Администратору поручено сформировать 8 подсетей. Для идентификации такого количества подсетей требуется 3 бита. В этом случае расширенный сетевой префикс будет равен /19 (маска подсети 255.255.224.0). Приведем адреса этих подсетей в двоичном и десятичном представлениях:

Подсеть #0: *10000100.00101101.***000**00000.00000000 = 132.45.0.0/19
Подсеть #1: *10000100.00101101.***001**00000.00000000 = 132.45.32.0/19
Подсеть #2: *10000100.00101101.***010**00000.00000000 = 132.45.64.0/19
Подсеть #3: *10000100.00101101.***011**00000.00000000 = 132.45.96.0/19
Подсеть #4: *10000100.00101101.***100**00000.00000000 = 132.45.128.0/19
Подсеть #5: *10000100.00101101.***101**00000.00000000 = 132.45.160.0/19
Подсеть #6: *10000100.00101101.***110**00000.00000000 = 132.45.192.0/19
Подсеть #7: *10000100.00101101.***111**00000.00000000 = 132.45.224.0/19

Теперь определим адреса устройств для подсети #3 (132.45.96.0/19 – *10000100.00101101.011*00000.00000000):

Подсеть #3: *10000100.00101101.***011**00000.00000000 = 132.45.96.0/19
Устройство #1: *10000100.00101101.*011**00000.00000001** = 132.45.96.1/19
Устройство #2: *10000100.00101101.*011**00000.00000010** = 132.45.96.2/19
Устройство #3: *10000100.00101101.*011**00000.00000011** = 132.45.96.3/19
…
Устройство #8190: *10000100.00101101.*011**00000.11111110** = 132.45.96.254/19

Определим широковещательный адрес для подсети #3 (132.45.96.0/19):

10000100.00101101.011**11111.11111111** = 132.45.127.255/19.

Пример 3. 8 подсетей (IP-адрес класса С)

Проделаем те же операции для сетевого адреса 200.35.1.0/24. Пусть также в каждой подсети необходимо предусмотреть адресное пространство для 20 устройств. Требуется определить расширенный сетевой префикс. Для их идентификации требуется минимум пять бит. Поэтому расширенный сетевой префикс будет равен /27 (32-5=27).

Ответим на следующие вопросы:

- Каково максимальное количество устройств, которые могут существовать в каждой подсети?

Максимальное количество устройств в каждой подсети равно 30 ($2^5 - 2 = 32 - 2 = 30$).

- Каково максимальное число подсетей, которые могут быть сформированы сетевым администратором?

Максимальное число подсетей равно 8 (2^3).

Приведем номера получающихся подсетей в двоичном и десятичном представлениях:

Подсеть #0: *11001000.00100011.00000001*.**000**00000 = 200.35.1.0/27
Подсеть #1: *11001000.00100011.00000001*.**001**00000 = 200.35.1.35/27
Подсеть #2: *11001000.00100011.00000001*.**010**00000 = 200.35.1.64/27
Подсеть #3: *11001000.00100011.00000001*.**011**00000 = 200.35.1.96/27
Подсеть #4: *11001000.00100011.00000001*.**100**00000 = 200.35.1.128/27
Подсеть #5: *11001000.00100011.00000001*.**101**00000 = 200.35.1.160/27
Подсеть #6: *11001000.00100011.00000001*.**110**00000 = 200.35.1.192/27
Подсеть #7: *11001000.00100011.00000001*.**111**00000 = 200.35.1.224/27

Приведем список адресов устройств, которые могут быть определены в подсети #6 (200.35.1.192/27):

Подсеть #6: *11001000.00100011.00000001*.110**00000** = 200.35.1.192/27
Устройство #1: *11001000.00100011.00000001*.110**00001** = 200.35.1.193/27
Устройство #2: *11001000.00100011.00000001*.110**00010** = 200.35.1.194/27
Устройство #3: *11001000.00100011.00000001*.110**00011** = 200.35.1.195/27
…
Устройство #29: *11001000.00100011.00000001*.110**11101** = 200.35.1.221/27
Устройство #30: *11001000.00100011.00000001*.110**11110** = 200.35.1.222/27

Широковещательный адрес для подсети 200.35.1.192/27 равен *11001000.00100011.00000001*.110**11111** = 200.35.1.223/27

Пример 4. Использование маски подсети переменной длины

Предположим, что организации был выделен адрес сети 140.25.0.0/16 (IP-адрес класса B), и она планирует использовать маски подсети переменной длины. На рис.2 показана схема выделения адресов для подсетей этой организации.

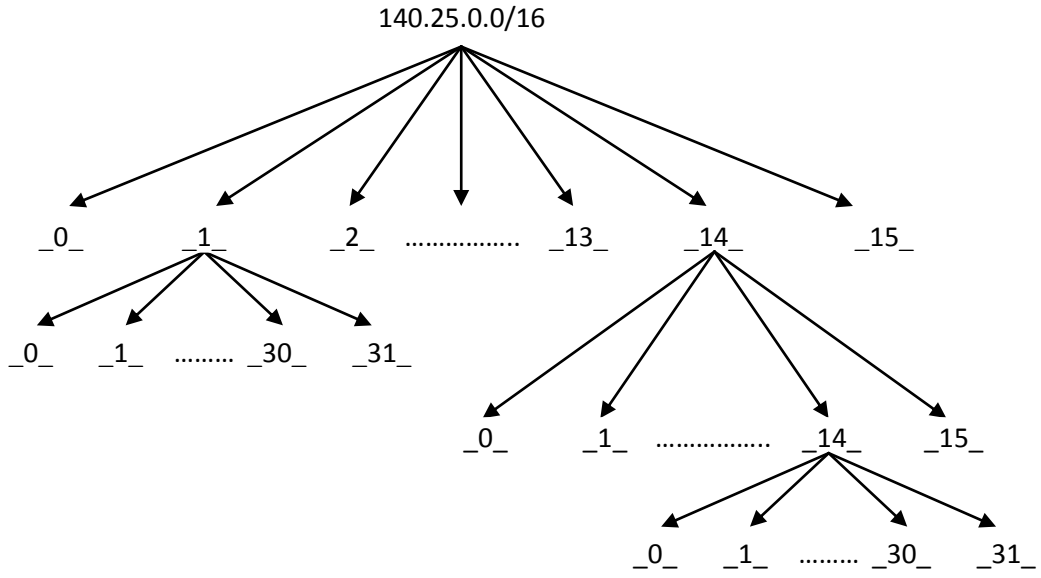

Рис. 2. Стратегия выделения подсетей

Первый шаг в процессе выделения подсетей состоит в делении основного сетевого адреса (140.25.0.0/16) на 16 адресных блоков (подсетей) равного размера. Затем подсеть #1 делится на 32 адресных блока равного размера, а подсеть #14 делится на 16 адресных блоков равного размера (подсетей нижнего уровня). Промежуточные сети #2—13 не делятся. Полученная подсеть нижнего уровня, например, 14-я подсеть в 14-й подсети (обозначим ее как #14-14) делится на 8 адресных блоков (подсетей) равного размера, которые образуют подсети следующего уровня. Таким образом в сети организации планируется использовать 74 подсети, каждая из которых будет поддерживать необходимое количество устройств.

Этот процесс подробно рассматривается ниже.

Определение 16 подсетей

Первым шагом в процессе выделения подсетей является деление сетевого адресного пространства на 16 адресных блоков равного размера (рис. 3).

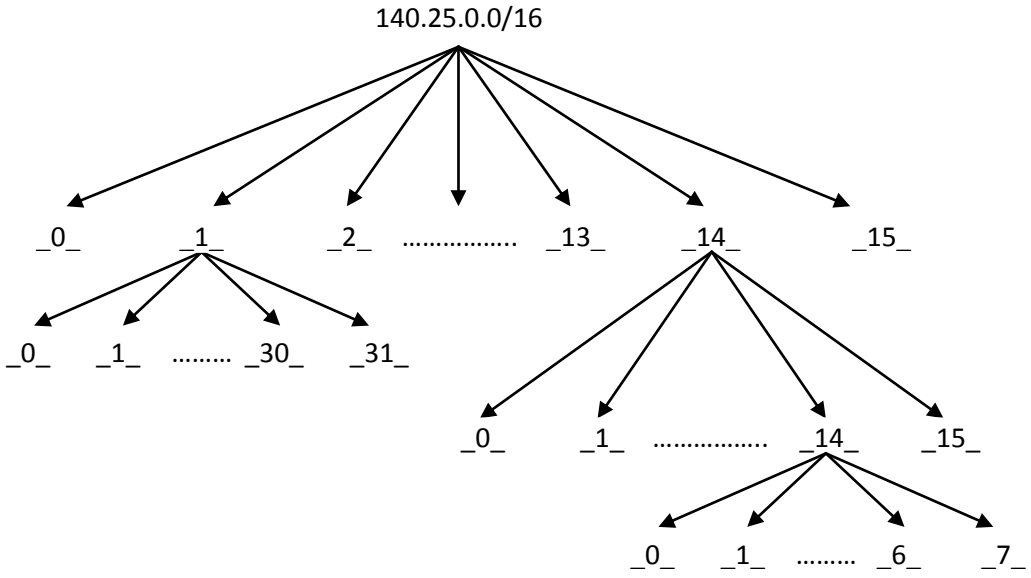

Рис. 3. Выделение 16 подсетей для адреса 140.25.0.0/16

Так как $16 = 2^4$, то потребуется четыре бита, чтобы идентифицировать каждую из этих 16 подсетей. Это означает, что организация нуждается в четырех битах или в расширенном сетевом префиксе равном /20, для того, чтобы выделить 16 подсетей. Каждая из этих подсетей представляет смежный блок из 2^{12} (32-20=12) адресов устройств. Таким образом мы получаем $2^{12} – 2 = 4094$ устройств.

Ниже приводятся эти 16 подсетей, выделенные из адресного блока 140.25.0.0/16. Данные подсети нумеруются от 0 до 15. Курсивная часть каждого адреса идентифицирует расширенный сетевой префикс, в то время как полужирные цифры задают 4-битовый номер подсети:

Базовая сеть: *10001100.00011001*.**0000**0000.00000000 = 140.25.0.0/16
Подсеть #0: *10001100.00011001*.**0000**0000.00000000 = 140.25.0.0/20
Подсеть #1: *10001100.00011001*.**0001**0000.00000000 = 140.25.16.0/20
Подсеть #2: *10001100.00011001*.**0010**0000.00000000 = 140.25.32.0/20
Подсеть #3: *10001100.00011001*.**0011**0000.00000000 = 140.25.48.0/20
Подсеть #4: *10001100.00011001*.**0100**0000.00000000 = 140.25.64.0/20
…
Подсеть #13: *10001100.00011001*.**1101**0000.00000000 = 140.25.208.0/20
Подсеть #14: *10001100.00011001*.**1110**0000.00000000 = 140.25.224.0/20
Подсеть #15: *10001100.00011001*.**1111**0000.00000000 = 140.25.240.0/20

Определение адресов устройств в подсетях

Определим адреса устройств, которые могут быть назначены в подсети #3 (140.25.48.0/20) (рис. 4).

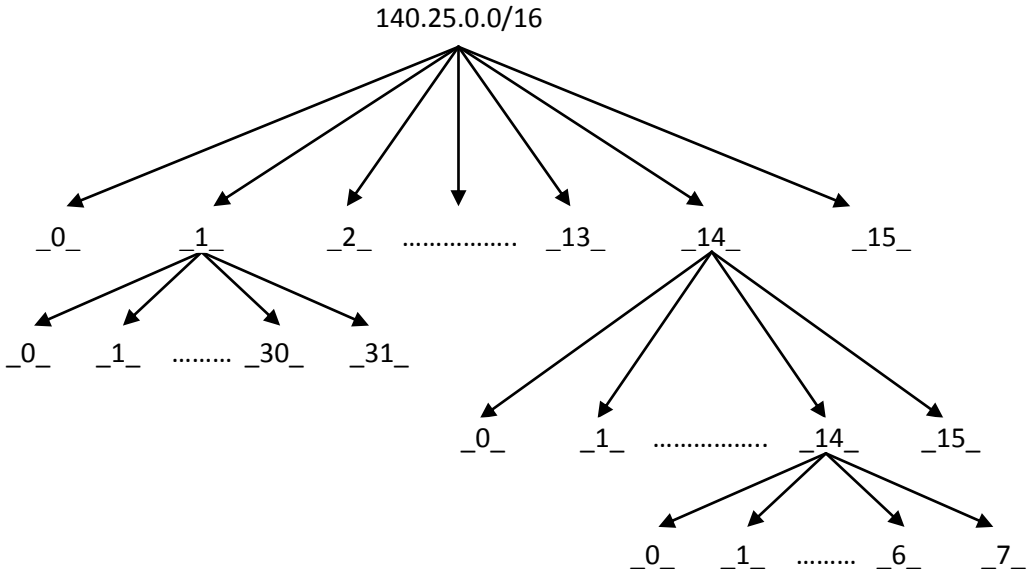

Рис. 4. Определение адресов устройств в подсети #3 (140.25.48.0/20)

Так как поле номера устройства в подсети #3 состоит из 12 бит, возможны 4 094 (2^{12} –2) корректных адресов устройств. Устройства нумеруются от 1 до 4 094. Адреса устройств для подсети #3 приводятся ниже. Курсивная часть каждого адреса идентифицирует расширенный сетевой префикс, в то время как полужирные цифры задают 12-разрядный номер устройства.

Подсеть #3: *10001100.00011001.0011*0000.00000000 = 140.25.48.0/20
Устройство #1: *10001100.00011001*.0011**0000.00000001** = 140.25.48.1/20
Устройство #2: *10001100.00011001*.0011**0000.00000010** = 140.25.48.2/20
Устройство #3: *10001100.00011001*.0011**0000.00000011** = 140.25.48.3/20
…
Устройство #4093: *10001100.00011001*.0011**1111.11111101** = 140.25.63.253/20
Устройство #4094: *10001100.00011001*.0011**1111.11111110** = 140.25.63.254/20

Широковещательный адрес для подсети #3 — это тот, в котором все биты в поле номера устройства установлены в единицу, то есть *10001100.00011001*. 0011**1111.11111111** = 140.25.63.255. Следует отметить, что широко-вещательный адрес для подсети #3 ровно на единицу меньше базового адреса для подсети #4 (140.25.64.0).

Определение подсетей нижнего уровня

Давайте определим подсети нижнего уровня (подсети подсетей) для подсети #14 (140.25.224.0/20). После того как основной сетевой адрес разделен на шестнадцать подсетей, подсеть #14 делится на 16 адресных блоков равного размера (рис.5).

Так как $16=2^4$, то, чтобы идентифицировать каждую из этих 16 подсетей, требуются еще четыре бита. Это означает, что организация будет должна использовать расширенный сетевой префикс, равный /24. Ниже приводятся 16 подсетей из адресного блока 140.25.224.0/20, которые нумеруются от 0 до 15.

Курсивная часть каждого адреса подсети нижнего уровня идентифицирует расширенный сетевой префикс, в то время как полужирные цифры показывают 4-битовое поле подсети нижнего уровня.

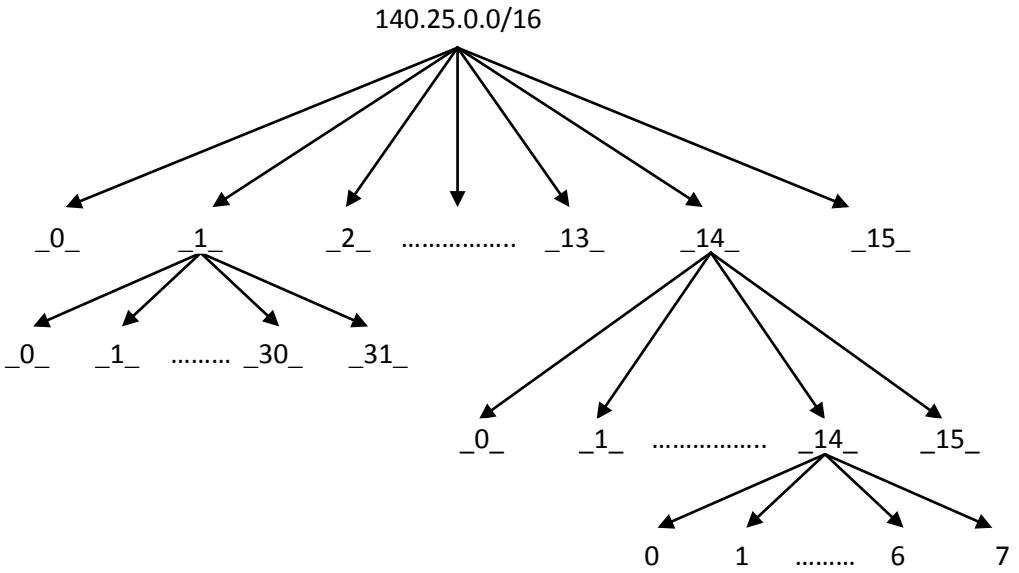

Рис. 5. Определение подсетей нижнего уровня для подсети #14 (140.25.224.0/20)

Подсеть #14: *10001100.00011001.111*00000.00000000 = 140.25.224.0/20
Подсеть #14-0: *10001100.00011001*.1110**0000**.00000000 = 140.25.224.0/24
Подсеть #14-1: *10001100.00011001*.1110**0001**.00000000 = 140.25.225.0/24
Подсеть #14-2: *10001100.00011001*.1110**0010**.00000000 = 140.25.226.0/24
Подсеть #14-3: *10001100.00011001*.1110**0011**.00000000 = 140.25.227.0/24
Подсеть #14-4: *10001100.00011001*.1110**0100**.00000000 = 140.25.228.0/24
…
Подсеть #14-14: *10001100.00011001*.1110**1110**.00000000 = 140.25.238.0/24
Подсеть #14-15: *10001100.00011001*.1110**1111**.00000000 = 140.25.239.0/24

Определение адресов устройств в подсетях нижнего уровня

Теперь следует определить адреса, которые могут быть назначены устройствам в подсетях нижнего уровня, например #14-3 (140.25.227.0/24) (рис. 6).

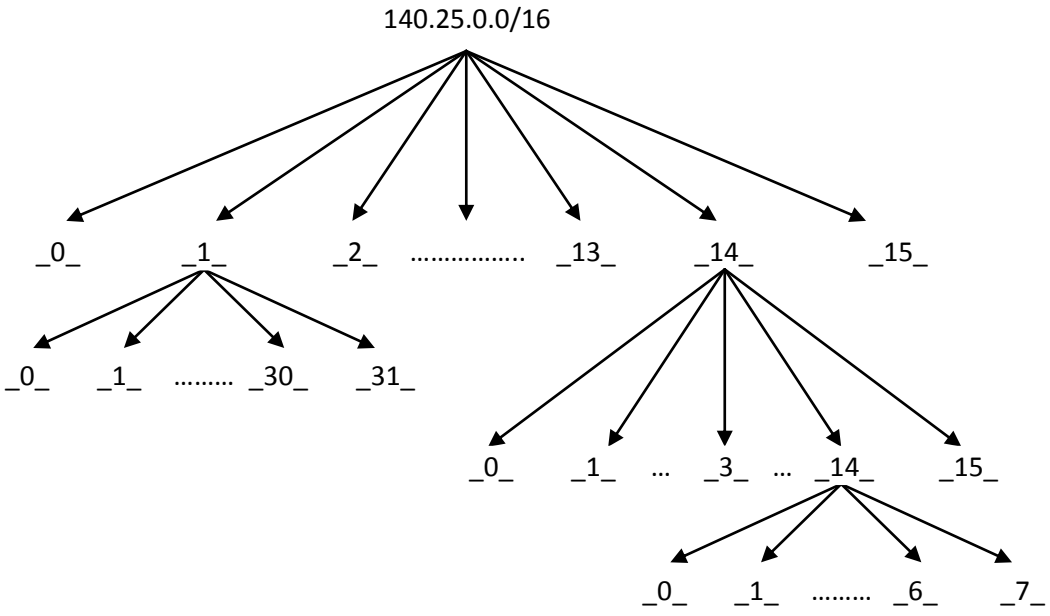

Рис. 6. Определение адресов устройств в подсети #14-3 (140.25.227.0/24)

В подсети нижнего уровня #14-3 можно использовать 8 бит для задания адресов устройств. Это означает, что каждая подсеть нижнего уровня #14-3 может поддерживать блок из 254 адресов устройств (2^8-2), которые нумеруются от 1 до 254. Адреса устройств в подсети #14-3 приводятся ниже. Курсивная часть каждого адреса идентифицирует расширенный сетевой префикс, в то время как полужирные цифры задают 8-битовый номер устройства (то есть представляют собой поле номера устройства).

Подсеть #14-3 *10001100.00011001.11100011*.00000000 = 140.25.227.0/24
Устройство #1 *10001100.00011001.11100011*.**00000001** = 140.25.227.1/24
Устройство #2 *10001100.00011001.11100011*.**00000010** = 140.25.227.2/24
Устройство #3 *10001100.00011001.11100011*.**00000011** = 140.25.227.3/24
Устройство #4 *10001100.00011001.11100011*.**00000100** = 140.25.227.4/24
Устройство #5 *10001100.00011001.11100011*.**00000101** = 140.25.227.5/24
…
Устройство #253: 10001100.*00011001.11100011*.**11111101** = 140.25.227.253/24
Устройство #254: *10001100.00011001.11100011*.**11111110** = 140.25.227.254/24

Широковещательный адрес для подсети #14-3 — это тот, в котором все биты в поле номера устройства установлены в единицу:

10001100.00011001.11100011.11111111=140.25.227.255.

Широковещательный адрес для подсети #14-3 ровно на единицу меньше, чем базовый адрес для подсети #14-4 (140.25.228.0).

Дальнейшее разбиение подсетей нижнего уровня

Чтобы лучше разобраться с назначением подсетей нижнего уровня, рассмотрим случай, когда в подсети нижнего уровня (в нашем случае — второго уровня), в свою очередь, вводятся подсети.

После того как подсеть #14 была разделена на шестнадцать подсетей нижнего уровня (под-подсетей), под-подсеть #14-14 (140.25.238.0/24) делится на 8 адресных блоков равного размера (рис. П3.7).

Широковещательный адрес для подсети #14-3 ровно на единицу меньше, чем базовый адрес для подсети #14-4 (140.25.228.0).

Дальнейшее разбиение подсетей нижнего уровня

Чтобы лучше разобраться с назначением подсетей нижнего уровня, рассмотрим случай, когда в подсети нижнего уровня (в нашем случае — второго уровня), в свою очередь, вводятся подсети.

После того как подсеть #14 была разделена на шестнадцать подсетей нижнего уровня (под-подсетей), под-подсеть #14-14 (140.25.238.0/24) делится на 8 адресных блоков равного размера (рис. 7).

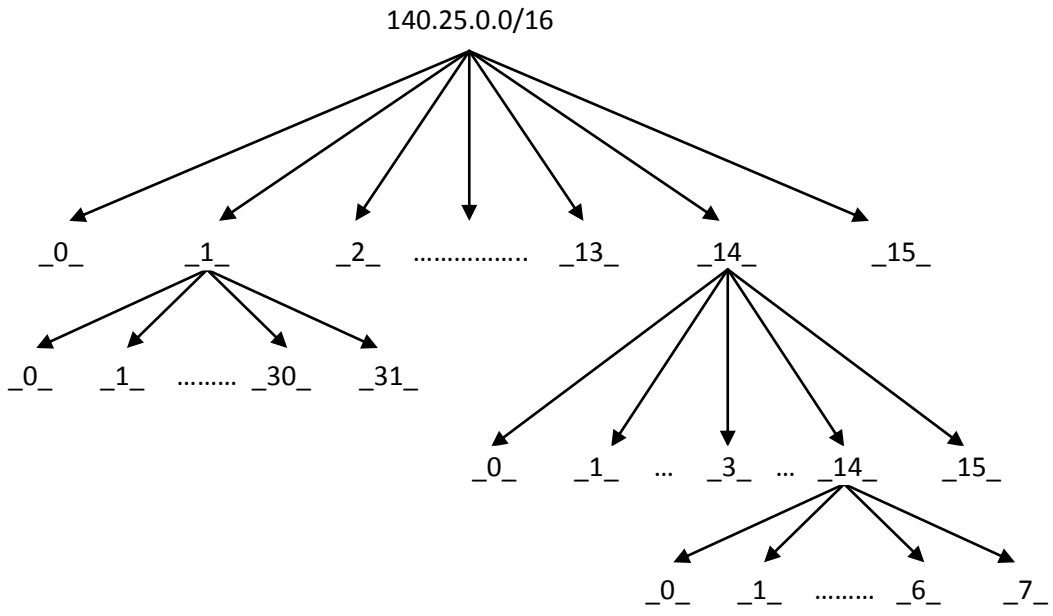

Рис. 7. Дальнейшая рекурсия в делении подсетей

Так как $8=2^3$, то, чтобы идентифицировать каждую из этих 8 подсетей, дополнительно требуется три бита. Это означает, что организация должна использовать расширенный сетевой префикс, равный /27. Адреса этих 8 подсетей из адресного блока 140.25.238.0/24 приведены ниже. Подсети нумеруются от 0 до 7. Курсивная часть каждого адреса под-под-подсети идентифицирует расширенный сетевой префикс, в то время как полужирные цифры указывают 3-битовый номер под-под-подсети.

Подсеть #14-14: *10001100.00011001*.11101110.00000000 = 140.25.238.0/24
Подсеть #14-14-0: *10001100.00011001*.11101110.**000**00000 = 140.25.238.0/27

Подсеть #14-14-1: *10001100.00011001*.11101110.**001**00000 = 140.25.238.32/27
Подсеть #14-14-2: *10001100.00011001*.11101110.**010**00000 = 140.25.238.64/27
Подсеть #14-14-3: *10001100.00011001*.11101110.**011**00000 = 140.25.238.96/27
Подсеть #14-14-4: *10001100.00011001*.11101110.**100**00000 = 140.25.238.128/27
Подсеть #14-14-5: *10001100.00011001*.11101110.**101**00000 = 140.25.238.160/27
Подсеть #14-14-6: *10001100.00011001*.11101110.**110**00000 = 140.25.238.192/27
Подсеть #14-14-7: *10001100.00011001*.11101110.**111**00000 = 140.25.238.224/27

Определение адресов устройств

Теперь, наконец, давайте определим адреса устройств в подсети #14-14-2 (140.25.238.64/27) (рис. 8).

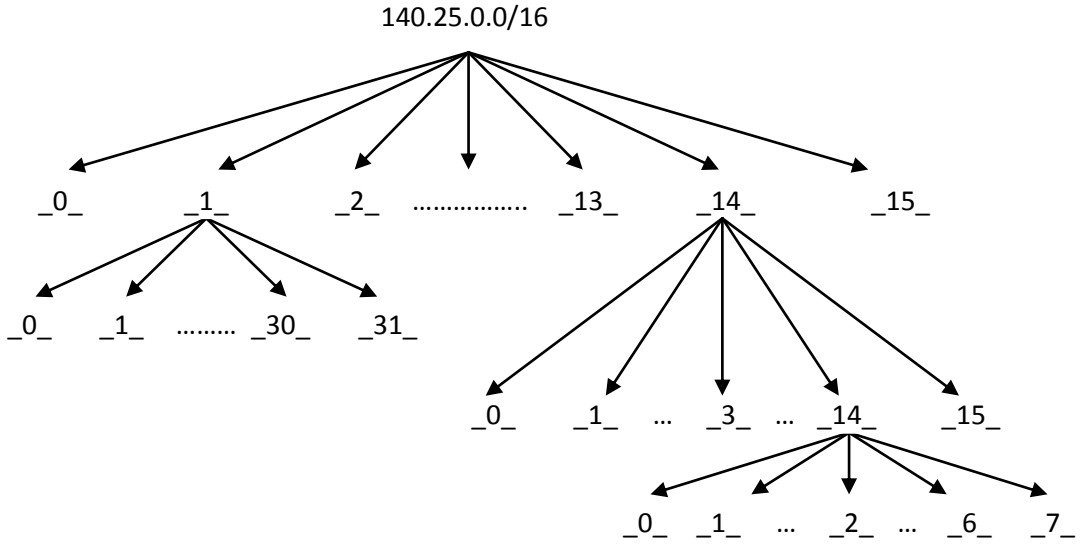

Рис. 8. Определение адресов устройств в подсети #14-14-2 (140.25.238.64/27)

Каждая из подсетей третьего уровня в подсети второго уровня #14-14 имеет 5 битов для задания адресов устройств. Это означает, что каждая из этих подсетей может поддерживать до 30 адресов устройств (2^5-2), которые нумеруются от 1 до 30. Адреса устройств для подсети #14-14-2 приводятся ниже. Курсивная часть каждого адреса идентифицирует расширенный сетевой префикс, в то время как полужирные цифры задают 5-битовый номер устройства:

Подсеть #14-14-2: *10001100.00011001.11101110.010*00000 = 140.25.238.64/27
Устройство #1: *10001100.00011001.11101110*.010**00001** = 140.25.238.65/27
Устройство #2: *10001100.00011001.11101110*.010**00010** = 140.25.238.66/27
Устройство #3: *10001100.00011001.11101110*.010**00011** = 140.25.238.67/27
Устройство #4: *10001100.00011001.11101110*.010**00100** = 140.25.238.68/27
Устройство #5: *10001100.00011001.11101110*.010**00101** = 140.25.238.69/27
…
Устройство #29: *10001100.00011001.11101110*.010**11101** = 140.25.238.93/27
Устройство #30: *10001100.00011001.11101110*.010**11110** = 140.25.238.94/27

Широковещательный адрес для подсети #14-14-2 — тот, в котором все биты в поле номера устройства установлены в единицу:

10001100.00011001.11011100.010**11111** = 140.25.238.95.

Широковещательный адрес для подсети #14-14-2 ровно на единицу меньше базового адреса подсети #14-14-3 (140.25.238.96).

Пример 5. Использование маски подсети переменной длины

Предположим, что организации был выделен сетевой адрес 140.25.0.0/16, и она планирует использовать маски подсети переменной длины. На рис. 9 показана схема выделения подсетей для этой организации.

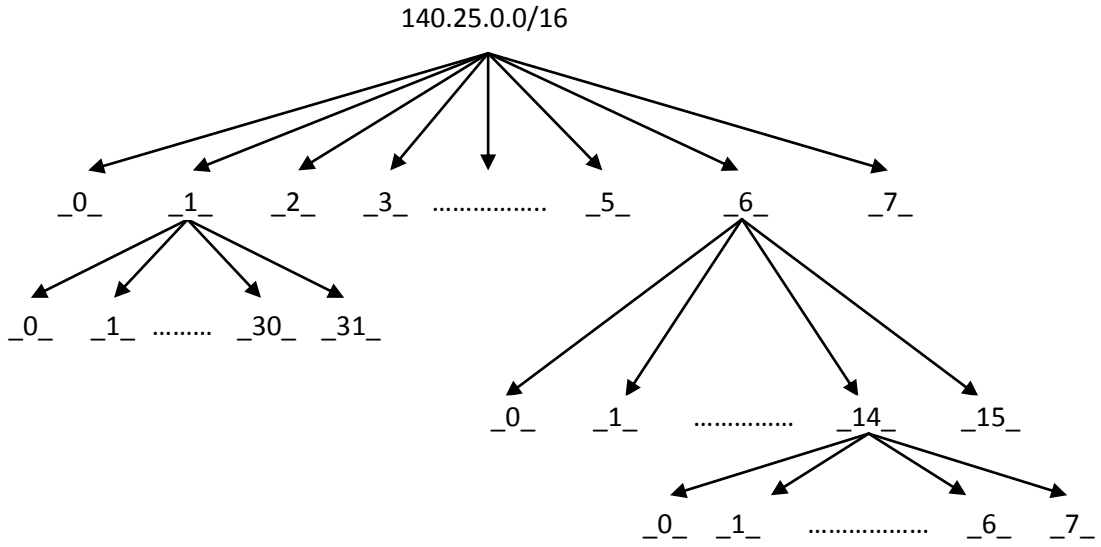

Рис. 9. Стратегия выделения подсетей

Первый шаг при организации подсетей состоит в делении основного сетевого адреса на 8 адресных блоков равного размера. Затем подсеть #1 делится на 32 адресных блока равного размера, а подсеть #6 делится на 16 адресных блоков равного размера. Затем получившиеся подсети нижнего уровня, например, подсеть #6-14, делятся на 8 адресных блоков равного размера.

Определим восемь подсетей сети с адресом 140.25.0.0/16.

Базовая сеть: *10001100.00011001*.00000000.00000000 = 140.25.0.0/16
Подсеть #0: *10001100.00011001*.**000**00000.00000000 = 140.25.0.0/16
Подсеть #1: *10001100.00011001*.**001**00000.00000000 = 140.25.32.0/16
Подсеть #2: *10001100.00011001*.**010**00000.00000000 = 140.25.64.0/16
Подсеть #3: *10001100.00011001*.**011**00000.00000000 = 140.25.96.0/16
Подсеть #4: *10001100.00011001*.**100**00000.00000000 = 140.25.128.0/16
Подсеть #5: *10001100.00011001*.**101**00000.00000000 = 140.25.160.0/16
Подсеть #6: *10001100.00011001*.**110**00000.00000000 = 140.25.192.0/16
Подсеть #7: *10001100.00011001*.**111**00000.00000000 = 140.25.224.0/16

Приведем список адресов устройств, которые могут использоваться в подсети #3 (140.25.96.0):

Подсеть #3: *10001100.00011001.011*00000.00000000 = 140.25.96.0/19
Устройство #1: *10001100.00011001*.011**00000.00000001** = 140.25.96.1/19
Устройство #2: *10001100.00011001*.011**00000.00000010** = 140.25.96.2/19
Устройство #3: *10001100.00011001*.011**00000.00000011** = 140.25.96.3/19
…
Устройство#8189: *10001100.00011001*.011**11111.11111101** = 140.25.127.253/19
Устройство#8190: *10001100.00011001*.011**11111.11111110** = 140.25.127.254/19

Определим широковещательный адрес для подсети #3 (140.25.96.0):

10001100.00011001.011**11111.11111111** = 140.25.127.255

Определим 16 подсетей нижнего уровня в подсети #6 (140.25.192.0/92):

Подсеть #6: *10001100.00011001.110*00000.00000000 = 140.25.192.0/23
Подсеть #6-0: *10001100.00011001*.110**00000**.00000000 = 140.25.192.0/23
Подсеть #6-1: *10001100.00011001*.110**00010**.00000000 = 140.25.194.0/23
Подсеть #6-2: *10001100.00011001*.110**00100**.00000000 = 140.25.196.0/23
Подсеть #6-3: *10001100.00011001*.110**00110**.00000000 = 140.25.198.0/23
Подсеть #6-4: *10001100.00011001*.110**01000**.00000000 = 140.25.200.0/23
…
Подсеть #6-14: *10001100.00011001*.110**11100**.00000000 = 140.25.220.0/23
Подсеть #6-15: *10001100.00011001*.110**11110**.00000000 = 140.25.222.0/23

Приведем список адресов устройств, которые могут использоваться в подсети нижнего уровня #6-3 (140.25.198.0/23):

Подсеть #6-3: *10001100.00011001.11000110*.00000000 = 140.25.198.2/23
Устройство #1: 10001100.00011001.1100011**0.00000001** = 140.25.198.1/23
Устройство #2: *10001100.00011001*.1100011**0.00000010** = 140.25.198.2/23
Устройство #3: *10001100.00011001*.1100011**0.0000011** = 140.25.198.3/23
Устройство #4: *10001100.00011001*.1100011**0.0000100** = 140.25.198.4/23
Устройство #5: *10001100.00011001*.1100011**0.0000101** = 140.25.198.5/53
…
Устройство #509: *10001100.00011001*.1100011**1.11111101** = 140.25.199.253/23
Устройство #510: *10001100.00011001*.1100011**1.11111110** = 140.25.199.254/23

Определим широковещательный адрес для подсети нижнего уровня #6-3 (140.25.198.0/23):

10001100.00011001.1100011**1.11111111** = 140.25.199.255

Определим восемь подсетей третьего уровня для подсети второго уровня #6-14 (140.25.220.0/23):

Подсеть #6: *10001100.00011001*.11011100.00000000 = 140.25.220.0/23

Подсеть #6-14-0: *10001100.00011001*.11000000**.00**000000 = 140.25.220.0/26
Подсеть #6-14-1: *10001100.00011001*.11000001**.01**000000 = 140.25.220.64/26
Подсеть #6-14-2: *10001100.00011001*.11000010**.10**000000 = 140.25.220.128/26
Подсеть #6-14-3: *10001100.00011001*.11000011**.11**000000 = 140.25.220.192/26
Подсеть #6-14-4: *10001100.00011001*.11001001**.00**000000 = 140.25.221.0/26
Подсеть #6-14-5: *10001100.00011001*.11001001**.10**000000 = 140.25.221.64/26
Подсеть #6-14-6: *10001100.00011001*.11011101**.10**000000 = 140.25.221.128/26
Подсеть #6-14-7: *10001100.00011001*.11011111**.11**000000 = 140.25.221.192/26

Приведем список адресов устройств, которые могут использоваться в подсети нижнего уровня #6-14-2 (140.25.220.128/26):

Подсеть #6-14-2: *10001100.00011001.11000110*.00000000 = 140.25.198.2/23
Устройство #1: *10001100.00011001.11000110.10***000001** = 140.25.198.1/23
Устройство #2: *10001100.00011001.11000110*.10**000010** = 140.25.198.2/23
Устройство #3: *10001100.00011001.11000110*.10**00011** = 140.25.198.3/23
Устройство #4: *10001100.00011001.11000110*.10**00100** = 140.25.198.4/23
Устройство #5: *10001100.00011001.11000110*.10**00101** = 140.25.198.5/53
…
Устройство #61: *10001100.00011001.11000111*.10**111101** = 140.25.199.253/23
Устройство #62: *10001100.00011001.11000111*.10**111110** = 140.25.199.254/23

Определим широковещательный адрес для подсети нижнего уровня #6-14-2 (140.25.198.0/23):

10001100.00011001.11011100.10**111111** = 140.25.220.191

Для более детального ознакомления с процедурами выделения подсетей и определения адресов устройств в организации, можно порекомендовать обратиться к источникам, указанным в списке литературы.

4. Контрольное задание

Контрольное задание предусматривает распределение масок переменной длины для организации 3-х уровневой структуры подсетей, подобной тем, которые были рассмотрены в примерах 4 и 5.

В табл. 4 представлены варианты контрольных заданий, в которых указаны номера подсетей в различных уровнях. В соответствии с принятой структурой обозначений сеть, представленная в примере 5, получит обозначение «B,6,14,6». Общее число подсетей в каком-либо уровне должно определяться как минимально возможное. Например, подсеть номер 5 в данном контрольном задании будет находиться в составе 8-и подсетей, обозначаемых 3-мя разрядами.

По результатам расчётов нужно выбрать адрес базовой сети и определить адреса 3-х подсетей (вместе с префиксами), а также найти максимально возможное

число устройств в подсети нижнего уровня. Кроме того, в 32-х разрядном поле необходимо любым способом отметить разряды, выделенные для обозначения сети, подсетей и устройства. Например: 1011110000010100 1100 101 10001 0001.

Таблица 4. Варианты контрольных заданий

Номер Варианта	Класс сети	Номера подсетей		
		1-й уровень	2-й уровень	3-й уровень
01	A	74	17	25
02	B	17	7	5
03	A	65	27	33
04	B	8	12	16
05	A	100	40	60
06	B	15	14	6
07	A	90	50	30
08	B	7	19	8
09	A	64	80	70
10	B	14	20	12
11	A	40	90	110
12	B	18	6	14
13	A	70	72	107
14	B	25	7	10
15	A	95	59	101
16	B	12	4	30
17	A	85	99	115
18	B	10	8	35
19	A	32	128	64
20	B	11	17	18

5. Вопросы и задания для домашней подготовки

1. В чем проявляется ненадежность протокола IP?

2. Сравните таблицу моста или коммутатора с таблицей маршрутизатора. Каким образом формируются эти таблицы? Какую информацию содержат? От чего зависит их объем?

3. Рассмотрим маршрутизатор на магистрали Интернета. Какие записи содержатся в поле адреса назначения его таблицы маршрутизации? Варианты ответов:

- номера всех сетей Интернета;
- номера некоторых сетей Интернета;
- номера некоторых сетей и полные адреса некоторых конечных узлов Интернета, для которых определены специфические маршруты;
- специальные адреса типа 127.0.0.0 или 255.255.255.255.

4.Сколько записей о маршрутах по умолчанию может включать таблица маршрутизации?

5.Приведите примеры, когда может возникнуть необходимость в использовании специфических маршрутов?

6.Передается ли в IP-пакете маска в тех случаях, когда маршрутизация реализуется с использованием масок?

7.Имеется ли связь между длиной префикса непрерывного пула IP-адресов и числом адресов, входящих в этот пул?

8.Почему в записи о маршруте по умолчанию в качестве адреса сети назначения часто указывается 0.0.0.0 с маской 0.0.0.0?

9. Какие элементы сети могут выполнять фрагментацию? Варианты ответов:

- только компьютеры;
- только маршрутизаторы;
- компьютеры, маршрутизаторы, мосты, коммутаторы;
- компьютеры и маршрутизаторы.

10. Что произойдет, если при передаче пакета он был фрагментирован и один из фрагментов не дошел до узла назначения после истечения тайм-аута? Варианты ответов:

- модуль IP узла-отправителя повторит передачу недошедшего фрагмента;
- модуль IP узла-отправителя повторит передачу всего пакета, в состав которого входил недошедший фрагмент;
- модуль IP узла-получателя отбросит все полученные фрагменты пакета, в котором потерялся один фрагмент, а модуль IP узла-отправителя не будет предпринимать никаких действий по повторной передаче данного пакета.

11. На рис. 1 показан компьютер с двумя сетевыми адаптерами, к которым подсоединены два сегмента. Компьютер работает под управлением Windows 2000. Может ли компьютер A в одном сегменте обмениваться данными с компьютером B, принадлежащем другому сегменту?

12. Может ли изменить ответ на предыдущий вопрос тот факт, что в сегментах используются разные канальные протоколы, например Ethernet и Token Ring?

13. Верно ли утверждение, что широковещательная рассылка является частным случаем групповой рассылки? Произвольной рассылки?

14. Может ли один сетевой интерфейс иметь одновременно несколько IPv6-адресов разных типов: уникальный адрес, адрес произвольной рассылки, групповой адрес?

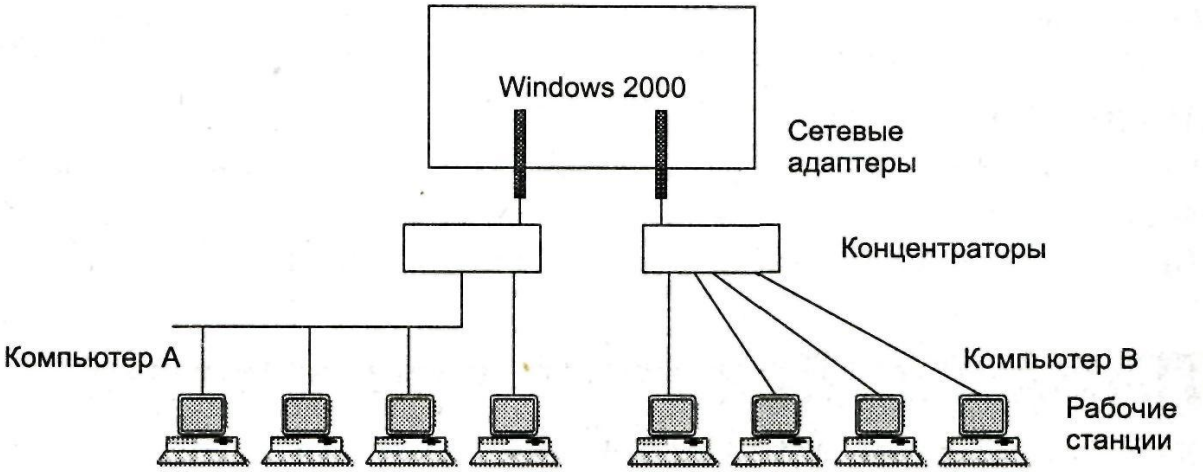

Рис. 10. Два сетевых сегмента, соединенные компьютером

Приложение

Протокол IPv6

В начале 90-х годов стек протоколов TCP/IP столкнулся с серьезными проблемами. Именно в это время началось активное промышленное использование Интернета: переход к построению сетей предприятий на основе транспорта Интернета, применение веб-технологии для доступа к корпоративной информации, ведение электронной коммерции через Интернет, внедрение Интернета в индустрию развлечений (распространение видеофильмов, звукозаписей, интерактивные игры).

Все это привело к резкому росту числа узлов сети (в начале 90-х годов новый узел в Интернете появлялся каждые 30 секунд), изменению характера трафика и к ужесточению требований, предъявляемых к качеству обслуживания сетью ее пользователей.

Направления модернизации стека TCP/IP

Сообщество Интернета, а вслед за ним и весь телекоммуникационный мир, начали решать новые задачи путем создания новых протоколов для стека TCP/IP, таких как протокол резервирования ресурсов (RSVP), защищенный протокол IP (IPSec), протокол коммутации меток (MPLS) и т. п. Однако ведущим специалистам было ясно, что только за счет добавления новых протоколов технологию TCP/IP развивать нельзя — нужно решиться на *модернизацию сердцевины стека,* протокола IP. Некоторые проблемы нельзя было решить без изменения формата IP-пакета и логики обработки полей заголовка IP-пакетов. Наиболее очевидной проблемой такого рода была проблема дефицита IP-адресов, которую невозможно снять, не расширив размер полей адресов источника и приемника.

Критике стала все чаще подвергаться масштабируемость маршрутизации. Дело в том, что быстрый рост сети вызвал перегрузку маршрутизаторов, которые должны уже сегодня обрабатывать в своих таблицах маршрутизации информацию о нескольких десятках тысяч номеров сетей, да еще решать некоторые вспомогательные задачи, такие, например, как фрагментация пакетов. Некоторые из предлагаемых решений данной проблемы также требовали внесения изменений в протокол IP.

Наряду с добавлением новых функций непосредственно в протокол IP необходимо было обеспечить его тесное взаимодействие с новыми протоколами — членами стека TCP/IP, что также требовало добавления в заголовок IP новых полей, обработку которых осуществляли бы эти протоколы. Например, для работы RSVP было желательно введение в заголовок IP поля метки потока, а для протокола IPSec — специальных полей для передачи данных, поддерживающих его функции обеспечения безопасности.

В результате сообщество Интернета после достаточно долгого обсуждения решило подвергнуть протокол IP серьезной переработке, выбрав в качестве основных целей модернизации:

- создание масштабируемой схемы адресации;
- сокращение объема работ, выполняемых маршрутизаторами;
- предоставление гарантий качества транспортных услуг;
- обеспечение защиты данных, передаваемых по сети.

Активные работы по модернизации протокола IP и разработке новых, ассоциированных с ним, протоколов начались в 1992 году. В это время сообществу Интернета были предложены несколько альтернативных вариантов протокола IP нового поколения: IPv7 (разработчик — Ullman), TUBA (Callon), ENCAPS (R. Hinden), SIP (S. Deering) и PIP (Francis).

В результате направления ENCAPS, SIP и PIP в 1993 году слились в единое предложение SIPP, которое в июле 1994 года на сессии сообщества Интернета было принято в качестве основы для создания **протокола IP нового поколения** (Next Generation Internet Protocol, IPng). Сейчас чаще для обозначения новой версии IP используется аббревиатура IPv6.

Документом, фиксирующим появление IPv6, стал RFC 1752. Базовый набор протоколов IPv6 был принят IETF в сентябре 1995 года. В августе 1998 года были приняты пересмотренные версии группы стандартов, определяющих как общую архитектуру IPv6 (RFC 2460), так и его отдельные аспекты, например систему адресации (RFC 2373).

Масштабируемая система адресации

Новая, шестая версия протокола IP (IPv6) внесла существенные изменения в систему адресации IP-сетей (RFC 2373). И, прежде всего, это коснулось *увеличения разрядности адреса.*

В IPv6 - адрес состоит из 128 бит, или 16 байт. Это дает возможность пронумеровать огромное количество узлов:

340 282 366 920 938 463 463 374 607 431 762 211 456.

Масштаб этого числа иллюстрирует, например, такой факт: если разделить это теоретически возможное количество IP-адресов между всеми жителями Земли (а их сегодня примерно 6 миллиардов), то на каждого из них придется невообразимо, если не сказать бессмысленно большое количество IP-адресов — $5{,}7 \times 10^{28}$! Очевидно, что такое значительное увеличение длины адреса было сделано не только и даже не столько для снятия проблемы дефицита адресов.

Главной целью изменения системы адресации было не механическое увеличение адресного пространства, а повышение эффективности работы стека TCP/IP в целом.

Вместо прежних двух уровней иерархии адреса (номер сети и номер узла) в IPv6 имеется 4 уровня, из которых три уровня используются для идентификации сетей, а один — для идентификации узлов сети. За счет увеличения числа уровней иерархии в адресе новый протокол эффективно поддерживает технологию CIDR (Classless Inter-Domain Routing, Бесклассовая междоменная маршрутизация). Благодаря этому, а также усовершенствованной системе групповой адресации и введению нового типов адресов новая версия IP позволяет *снизить затраты на маршрутизацию.*

Произошли и чисто внешние изменения — разработчики стандарта предложили использовать вместо десятичной *шестнадцатеричную* форму записи IP-адреса. Каждые четыре шестнадцатеричные цифры отделяются друг от друга двоеточием. Вот как, например, может выглядеть адрес IPv6:

FEDC:0A98:0:0:0:0:7654:3210.

Если в адресе имеется длинная последовательность нулей, то запись адреса можно сократить. Например, приведенный выше адрес можно записать и так:

FEDC:0A98::7654:3210.

Сокращение в виде двух двоеточий (::) может употребляться в адресе только один раз. Можно также опускать незначащие нули в начале каждого поля адреса, например, вместо FEDC:0A98::7654:3210 можно писать

FEDC:A98::7654:3210.

Для сетей, поддерживающих обе версии протокола (IPv4 и IPv6), разрешается использовать для младших 4 байт традиционную для IPv4 десятичную запись: 0:0:0:0:0:FFFF:129.144.52.38 или ::FFFF:129.144.52.38.

В новой версии IPv6 предусмотрено три основных типа адресов: индивидуальные адреса, групповые адреса и адреса произвольной рассылки. Тип адреса определяется значением нескольких старших битов адреса, которые названы **префиксом формата.**

□ **Индивидуальный адрес** (unicast) определяет уникальный идентификатор отдельного интерфейса конечного узла или маршрутизатора. Назначение адреса этого типа совпадает с назначением уникальных адресов в версии IPv4 - с их помощью пакеты доставляются определенному интерфейсу узла назначения. В версии IPv6, в отличие от версии IPv4, отсутствует понятие класса сети (A, B, C и D) и связанное с ним фиксированное разбиение адреса на номер сети и номер узла по границам байтов. Индивидуальные адреса делятся на несколько подтипов для отражения специфики некоторых часто встречающихся в современных сетях ситуаций.

□ **Групповой адрес** (multicast) IPv6 аналогичен по назначению групповому ад-

ресу IPv4. Он идентифицирует группу интерфейсов, относящихся, как правило, к разным узлам. Пакет с таким адресом доставляется *всем* интерфейсам с этим адресом. Групповые адреса используются в IPv6 для замены широковещательных адресов — для этого вводится адрес особой группы, объединяющей все интерфейсы подсети.

■ **Произвольной рассылки** (anycast) — это новый тип адреса, который так же, как и групповой адрес, определяет группу интерфейсов. Однако пакет с таким адресом доставляется *любому* из интерфейсов группы, как правило, «ближайшему» в соответствии с метрикой, используемой протоколами маршрутизации. Синтаксически адрес произвольной рассылки ничем не отличается от индивидуального адреса и назначается из того же диапазона адресов. Адрес произвольной рассылки может быть назначен только интерфейсам маршрутизатора. Интерфейсы маршрутизаторов, входящие в одну группу произвольной рассылки, имеют индивидуальные адреса и, кроме того, общий адрес группы произвольной рассылки. Адреса такого типа ориентированы на маршрутизацию от источника, при которой маршрут прохождения пакета определяется узлом-отправителем путем указания IP-адресов всех промежуточных маршрутизаторов. Например, поставщик услуг может присвоить всем своим маршрутизаторам один и тот же адрес произвольной рассылки и сообщить его абонентам. Если абонент желает, чтобы его пакеты передавались через сеть этого поставщика услуг, то ему достаточно указать этот адрес в цепочке адресов маршрута от источника, и пакет будет передан через ближайший маршрутизатор данного поставщика услуг. Так же как и в IPv4, в IPv6 имеются так называемые **частные адреса,** предназначенные для использования в автономных сетях. В отличие от версии IPv4 в версии IPv6 эти адреса представлены двумя разновидностями:

□ **Адреса локальных сетей, не разделенных на подсети,** содержат только 64-разрядное поле идентификатора интерфейса, а остальные разряды, кроме префикса формата, должны быть нулевыми, поскольку потребность в номере подсети здесь отсутствует.

□ **Адреса локальных сетей, разделенных на подсети,** содержат по сравнению с предыдущими адресами дополнительное двухбайтовое поле номера подсети.

Основным подтипом индивидуального адреса является **глобальный агрегируемый уникальный адрес.** Такие адреса могут агрегироваться для упрощения маршрутизации. В отличие от уникальных адресов узлов версии IPv4, которые состоят из двух полей — номера сети и номера узла, глобальные агрегируемые уникальные адреса IPv6 имеют более сложную структуру, включающую шесть полей (рис. П1).

□ **Префикс формата** (Format Prefix, FP) для этого типа адресов имеет размер три бита и значение 001. Следующие три поля — агрегирования верхнего (Top-Level Aggregation, TLA), следующего (Next-Level Aggregation, NLA) и местного (Site-Level Aggregation, SLA) уровней — описывают три уровня идентификации сетей.

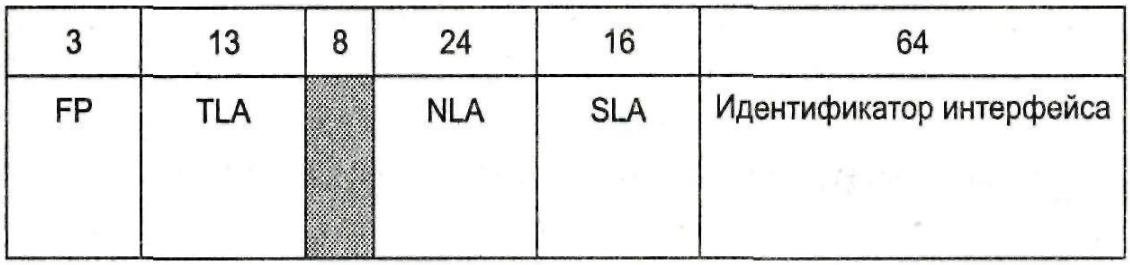

Рис. П1. Структура глобального агрегируемого уникального адреса в пакете IPv6

□ **Поле TLA** предназначено для идентификации сетей самых крупных поставщиков услуг. Конкретное значение этого поля представляет собой общую часть адресов, которыми располагает данный поставщик услуг. Сравнительно небольшое количество разрядов, отведенных под это поле (13), выбрано специально для ограничения размера таблиц маршрутизации в магистральных маршрутизаторах самого верхнего уровня Интернета. Это поле позволяет перенумеровать 8196 сетей поставщиков услуг верхнего уровня, а значит, число записей, описывающих маршруты между этими сетями, также будет ограничено значением 8196, что ускорит работу магистральных маршрутизаторов. Следующие 8 разрядов зарезервированы на будущее для расширения при необходимости поля TLA.

□ **Поле NLA** предназначено для нумерации сетей средних и мелких поставщиков услуг. Значительный размер поля NLA позволяет путем агрегирования адресов отразить многоуровневую иерархию поставщиков услуг.

□ **Поле SLA** предназначено для адресации подсетей отдельного абонента, например подсетей одной корпоративной сети. Предполагается, что поставщик услуг назначает некоторому предприятию номер его сети, состоящий из фиксированного значения полей TLA и NLA, которые в совокупности являются аналогом номера сети версии IPv4. Остальная часть адреса — поля SLA и идентификатор интерфейса — поступает в распоряжение администратора корпоративной сети, который полностью берет на себя формирование адреса и не должен согласовывать этот процесс с поставщиком услуг. Причем, поле идентификатора интерфейса имеет вполне определенное назначение — оно должно хранить физический адрес узла. На этом уровне также можно агрегировать адреса небольших подсетей в более крупные подсети, и размер поля SLA в 16 бит обеспечивает достаточную свободу и гибкость построения внутрикорпоративной иерархии адресов.

□ **Идентификатор интерфейса** является аналогом номера узла в IPv4. Отличием версии IPv6 является то, что в общем случае идентификатор интерфейса просто *совпадает с его локальным (аппаратным) адресом,* а не представляет собой произвольно назначенный администратором номер узла. Идентификатор интерфейса имеет длину 64 бита, что позволяет поместить туда MAC-адрес (48 бит), адрес X.25 (до 60 бит), адрес конечного узла ATM (48 бит) или номер виртуального соединения ATM (до 28 бит), а также, вероятно, даст возможность использовать локальные адреса технологий, которые могут появиться в будущем. Такой подход в стиле протокола IPX *делает ненужным, протокол ARP,* поскольку процедура

отображения IP-адреса на локальный адрес становится тривиальной — она сводится к простому отбрасыванию старшей части адреса. Кроме того, в большинстве случаев *отпадает необходимость ручного конфигурирования* конечных узлов, так как младшую часть адреса — идентификатор интерфейса — узел узнает от аппаратуры (сетевого адаптера и т. п.), а старшую — номер подсети — ему сообщает маршрутизатор.

Очевидно, что при таком изобилии сетей, которое предоставляется клиенту в IPv6, совершенно теряет смысл операция использования масок для *разделения сетей* на подсети, в то время как обратная процедура — *объединение подсетей* — приобретает особое значение. Разработчики стандартов IPv6 считают, что агрегирование адресов является основным способом эффективного использования адресного пространства в новой версии протокола IP.

Пример

Пусть клиент получил от поставщика услуг пул адресов IPv6, определяемый следующим префиксом:

20:0A:00:C9:74:05/48.

Давайте проведем анализ этого числа. Поскольку его первые 3 бита равны 001, следовательно, это *глобальный агрегируемый уникальный адрес* (рис. П2).

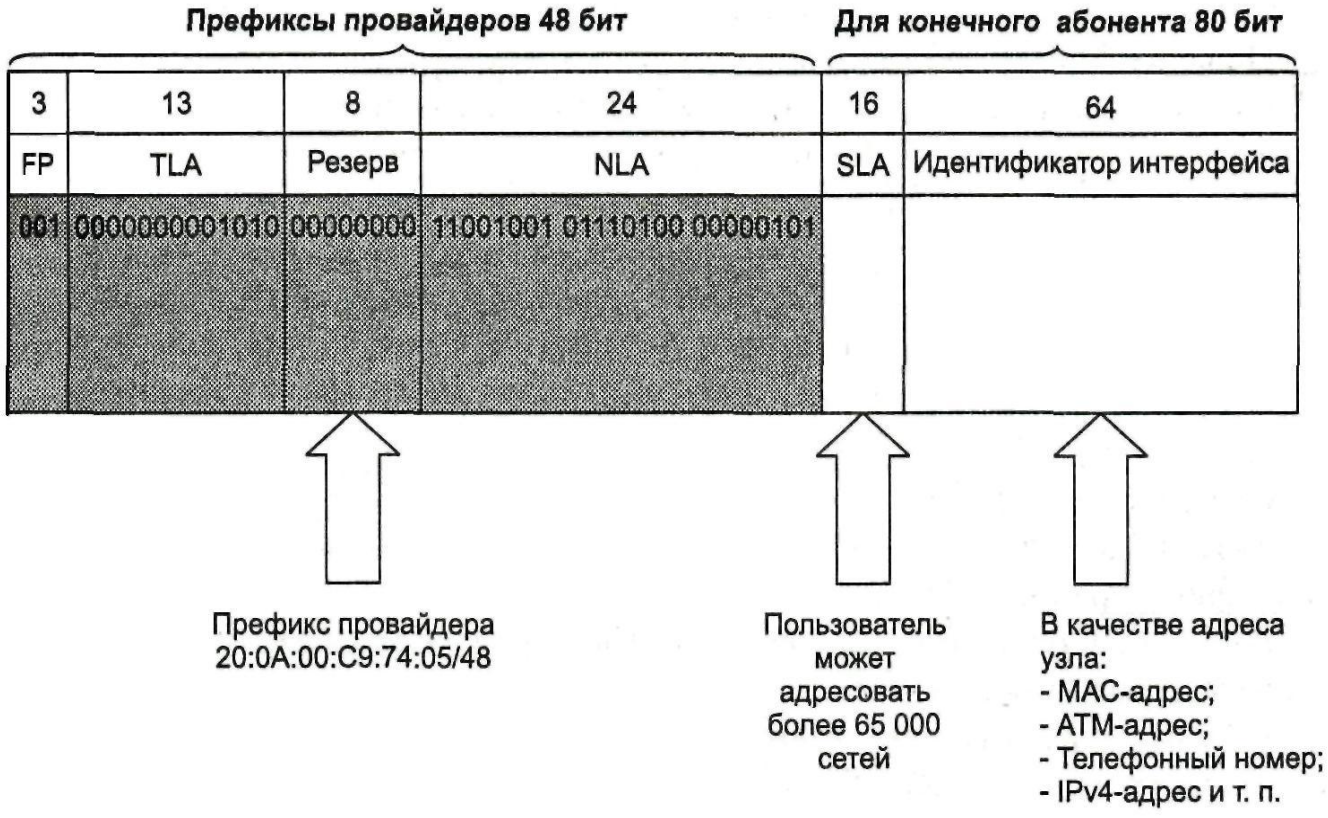

Рис. П2. Пример глобального агрегируемого адреса

Адрес этот принадлежит поставщику услуг верхнего уровня, у которого все сети имеют префикс 20:0A/16. Он может выделить поставщику услуг второго

уровня некоторый диапазон адресов с общим префиксом, образованным его собственным префиксом, а также частью поля NLA. Длина поля NLA, отводимая под префикс, определяется маской, которую поставщик услуг верхнего уровня также должен сообщить своему клиенту — поставщику услуг второго уровня. Пусть в данном примере маска состоит из 32 единиц в старших разрядах, а результирующий префикс поставщика услуг второго уровня имеет вид:

20:0A:00:C9/32.

В распоряжении поставщика услуг второго уровня остается 16 разрядов поля NLA для нумерации сетей своих клиентов. В качестве клиентов могут выступать поставщики услуг третьего и более низких уровней, а также конечные абоненты — предприятия и организации. Пусть, например, следующий байт (01110100) в поле NLA поставщик услуг использовал для передачи поставщику услуг более низкого (третьего) уровня, а тот, в свою очередь, использовал последний байт поля NLA для назначения пула адресов клиенту. Таким образом, с участием поставщиков услуг трех уровней был сформирован префикс 20:0A:00:C9:74:05/48, который получил клиент.

Протокол IPv6 оставляет в полном распоряжении клиента 2 байта (поле SLA) для нумерации сетей и 8 байт (поле идентификатора интерфейса) для нумерации узлов. Имея такой огромный диапазон номеров подсетей, администратор может использовать его по-разному. Он может выбрать простую плоскую организацию своей сети, назначая каждой имеющейся подсети определенное значение из диапазона в 65 535 адресов, игнорируя оставшиеся. В крупных сетях более эффективным способом (сокращающим размеры таблиц корпоративных маршрутизаторов) может оказаться иерархическая структуризация сети на основе *агрегирования адресов.* В этом случае используется та же технология CIDR, но уже не поставщиком услуг, а администратором корпоративной сети.

Помимо подробно рассмотренного выше глобального агрегируемого адреса, существуют и другие разновидности индивидуального адреса.

Адрес обратной петли 0:0:0:0:0:0:0:1 играет в версии IPv6 ту же роль, что и адрес 127.0.0.1 в версии IPv4, т.е. зарезервирован для тестирования сетевого программного обеспечения методом шлейфа.

□ **Неопределенный адрес,** состоящий из одних нулей, является аналогом адреса 0.0.0.0 протокола IPv4. Этот адрес может появляться в IP-пакетах только в качестве адреса источника, и это означает, что пакет послан до того, как узел изучил свой IP-адрес (например, до получения его от DHCP-сервера).

Предполагается, что довольно большое время будут сосуществовать островки Интернета, работающие по протоколу IPv6, и остальная часть Интернета, работающая на версии IPv4. Для того чтобы узлы, поддерживающие версию IPv6, могли

использовать технику передачи пакетов IPv6 через сеть IPv4 в автоматическом режиме, разработан специальный подтип адресов, которые переносят IPv4-адрес в младших 4-х байтах IPv6-адреса, а в старших 12 байтах адреса содержат нули (рис. П3). Такие индивидуальные адреса делают очень простой процедуру преобразования адресов между двумя версиями протокола IP и называются I**Pv4-совместимыми с IPv6-адресами.**

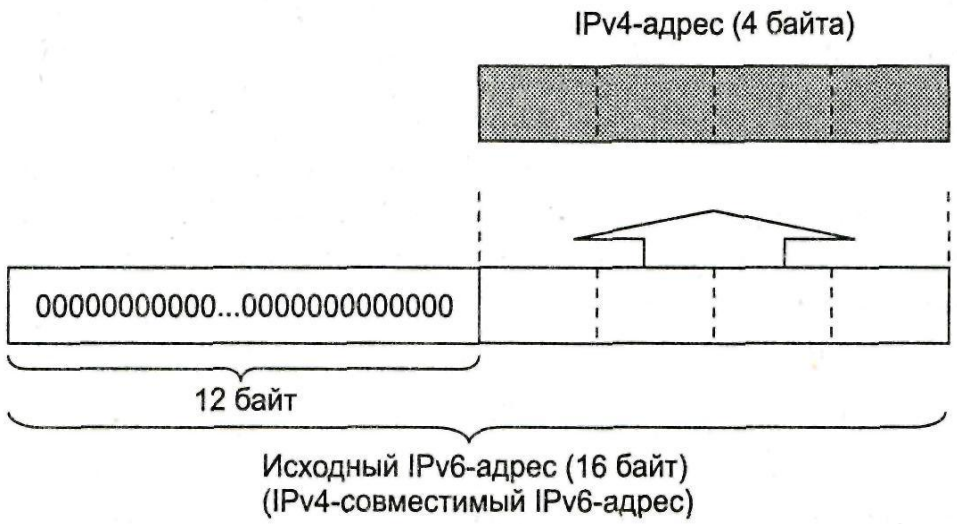

Рис. П3. Преобразование IPv6 в IPv4

Для решения обратной задачи — передачи IPv4-пакетов через части Интернета, работающие по протоколу IPv6, — предназначен **IPv4-отображенный в IPv6-адрес.** Этот тип адреса по-прежнему содержит в 4-х младших байтах IPv4-адрес, в старших 10-ти байтах — нули, а в 5-м и 6-м байтах IPv6-адреса — единицы, которые показывают, что узел поддерживает только 4-ю версию протокола IP (рис. П4).

Работа по детализации подтипов IPv6-адресов еще далека от завершения. Сегодня определено назначение только 15 % адресного пространства IPv6, а оставшаяся часть адресов еще ждет своей очереди, чтобы найти применение для решения одной из многочисленных проблем Интернета.

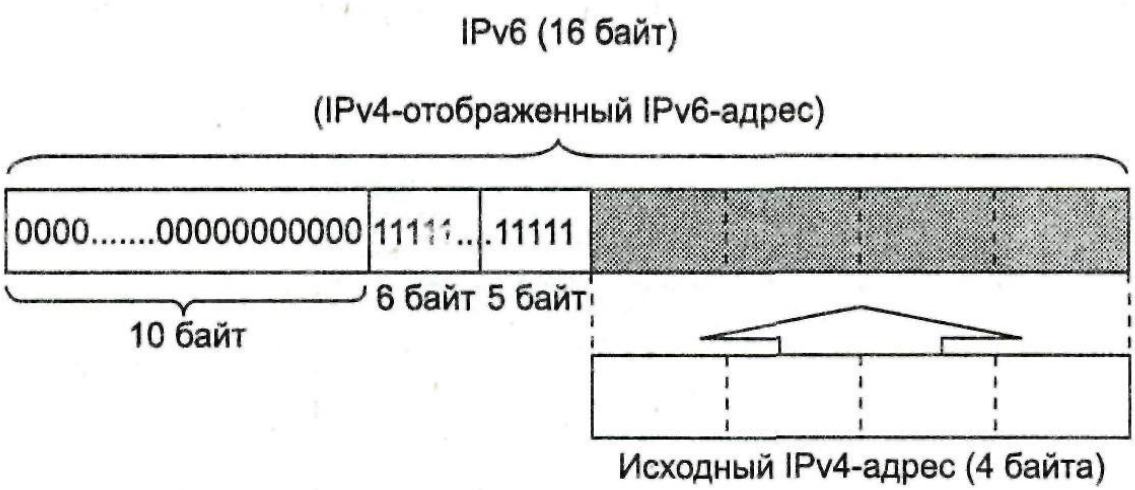

Рис. П4. Преобразование IPv4 в IPv6

Гибкий формат заголовка

Одной из основных целей изменения формата заголовка в IPv6 было снижение накладных расходов, то есть уменьшение объема служебной информации, передаваемой с каждым пакетом. Для этого в новом протоколе IP были введены понятия основного и дополнительного заголовков. Основной заголовок присутствует всегда, а дополнительные являются опциональными. Дополнительные заголовки могут содержать, например, информацию о фрагментации исходного пакета, полный маршрут следования пакета при маршрутизации от источника, информацию, необходимую для защиты передаваемых данных.

Основной заголовок имеет фиксированную длину в 40 байт, его формат показан на рис. П5.

Поле следующего заголовка соответствует по назначению полю протокола в версии IPv4 и определяет тип заголовка, который следует за данным. Каждый следующий дополнительный заголовок также содержит поле следующего заголовка. Если IP-пакет не содержит дополнительных заголовков, то в этом поле будет значение, закрепленное за протоколом TCP, UDP, RIP, OSPF или другим, определенным в стандарте IPv4.

В предложениях по поводу протокола IPv6 фигурируют пока следующие типы дополнительных заголовков:

□ **заголовок маршрутизации** — указание полного маршрута при маршрутизации от источника;

□ **заголовок фрагментации** — информация, относящаяся к фрагментации IP-пакета (поле обрабатывается только в конечных узлах);

□ **заголовок аутентификации** — информация, необходимая для аутентификации конечных узлов и обеспечения целостности содержимого IP-пакетов;

□ **заголовок системы безопасности** — информация, необходимая для

обеспечения конфиденциальности передаваемых данных путем шифрования и дешифрирования;

□ **специальные параметры** — параметры, необходимые для последовательной обработки пакетов на каждом ретрансляционном участке;

□ **параметры получателя** — дополнительная информация для узла назначения.

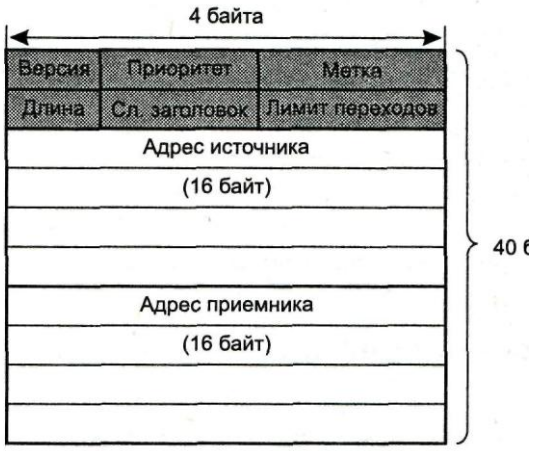

Рис. П5. Формат основного заголовка

Рис. П6. Структура IPv6-пакета

Таким образом, IP-пакет может иметь, например, формат, показанный на рис. П6.

Поскольку для маршрутизации пакета обязательным является только основной заголовок (почти все дополнительные заголовки обрабатываются только в конечных узлах), *это снижает нагрузку на маршрутизаторы.* С другой стороны, возможность использования большого количества дополнительных параметров *расширяет функциональность протокола IP* и делает его открытым для внедрения новых механизмов.

Снижение нагрузки на маршрутизаторы

Для того чтобы повысить производительность маршрутизаторов Интернета в части выполнения их основной функции — продвижения пакетов, в версии IPv6 предпринят ряд мер по освобождению маршрутизаторов от некоторых вспомогательных задач.

- *Перенесение функций фрагментации с маршрутизаторов на конечные узлы.* Конечные узлы в версии IPv6 обязаны найти минимальное значение MTU (длина пакета) вдоль всего пути, соединяющего исходный узел с узлом назначения (эта техника под названием Path MTU Discovery уже используется в IPv4). Маршрутизаторы IPv6 не выполняют фрагментацию, а только посылают ICMP-сообщение «Слишком длинный пакет» конечному узлу, который должен уменьшить размер пакета.
- *Агрегирование адресов,* ведущее к уменьшению размера адресных таблиц

маршрутизаторов, а значит, — к сокращению времени просмотра и обновления таблиц. При этом также сокращается служебный трафик, создаваемый протоколами маршрутизации.

- *Широкое использование маршрутизации от источника,* при которой узел-источник задает полный маршрут прохождения пакета через сети. Такая техника освобождает маршрутизаторы от необходимости просмотра адресных таблиц при выборе следующего маршрутизатора.
- *Отказ от обработки не обязательных параметров заголовка.*
- *Использование в качестве номера узла его MAC-адреса,* что избавляет маршрутизаторы от необходимости применять протокол ARP.

Новая версия протокола IP, являющаяся составной частью проекта IPv6, предлагает встроенные средства защиты данных. Размещение средств защиты на сетевом уровне делает их прозрачными для приложений, так как между уровнем IP и приложением всегда будет работать протокол транспортного уровня. Приложения переписывать при этом не придется. Новая версия протокола IP со встроенными средствами обеспечения безопасности называется **IPSec** (Security Internet Protocol — защищенный протокол IP).

Переход от версии IPv4 к версии IPv6 только начинается. Сегодня уже существуют фрагменты Интернета, в которых маршрутизаторы поддерживают обе версии протокола. Эти фрагменты объединены между собой через Интернет, образуя так называемую магистраль **6Bone.**

Список использованной литература

1. Таненбаум Э. Компьютерные сети/ Э.Таненбаум. – М:Питер, 2002.

2. Олифер В.Г. Основы компьютерных сетей/ В.Г. Олифер, Н.А. Олифер. – М: Питер, 2009.

3. Максимов В.А. Маршрутизация в IP-сетях/ В.А. Максимов. – М: Питер, 2003.