Институт повышения квалификации
работников телевидения и радиовещания.

Технология TCP/IP

Миронов В.Ю.

Учебное пособие

2002г.

Введение

Предлагаемое учебное пособие предназначено телережиссерам, художникам, монтажерам - тем, кто работает с цифровыми данными и сетями.

Данная работа может помочь слушателям более глубоко разобраться в понятии: современных сетевых протоколов.

Автор изучил наиболее функциональные работы в данной области, такие как:

Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн. UNIX: руководство системного администратора.

Р.Д. Мэтьюз, П. Джонс и др. Web-сервер под Unix.

TCP/IP Illustrated, volume I. The Protocols

TCP/IP. Учебное руководство для специалистов MCSE

Дрю Х. Внутренний мир TCP/IP

Д. Комер "Межсетевой обмен с помощью TCP/IP"

Это информационно емкое пособие представляет собой дополнительный материал по курсу веб дизайна.

Протокол IP является сегодня стдартом о для посроения сложных составных сетей, объединяющих подсети различных технологий. Он был отшлифован многолетней практикой применения в Интернете, а затем у твердился и в корпоративных сетях, потеснив IPX и ряд других протоколов сетевого у ровня.

История TCP/IP

Технология TCP/IP появилась на свет благодаря разработкам, финансировавшимся Американским агентством передовых исследований в области обороны (Defense Advanced Research Projects Agency, DARPA). Работы но созданию распределенной компьютерной сети нового типа начались в 1969 году. Экспериментальная компьютерная сеть, получившая название ARPANET, начала свое полноценное функционирование в 1975 году после нескольких лет исследований и испытаний. В 1983 году в качестве стандартного протокола передачи данных через сеть ARPANET был принят набор протоколов TCP/IP, Когда в конце концов сеть ARPANET превратилась в Интернет (сама сеть ARPANET прекратила свое существование в 1990 году), протокол TCP/IP получил широкое распространение, Чаще всего этот протокол использовался в локальных сетях, основанных на UNIX, С появлением высокоскоростных телефонных технологий, таких как ISDN, технология TCP/IP стала использоваться также в качестве транспортного протокола для передачи данных через каналы телефонной связи.

Гибкая система адресации, применяемая в IP-сетях, внесла важный вклад в успех технологии IP.

Эта система позволяет объединять сети с различными собственными системами адресации, например сети Ethernet с сетями frame realy а сети X.25 - с сетями ATM. Открытость IP-адресации дает принципиальную возможность включать в интерсеть подсеть любой новой технологии - для этого нужно только разработать новую версию протокола разрешения

адресов ARP. Кроме такой универсальности система IP-адресации обладает также многими полезными дополнительными свойствами: поддержкой групповой адресации, необходимой для эффективной работы широковещания в Интерпете, возможностью агрегирования адресов для упрощения маршрутизации и рядом других.

Конечно, система IP-адресации не свободна от недостатков и ограничений, ведь она была разработана более 20 лет назад, а сетевой мир с тех пор существенно изменился. Поэтому при разработке новой версии протокола IPv6 (текущая его версия это версия 4) система адресации была модифицирована и наделена рядом новых возможностей в соответствии с требованиями времени и новым статусом Интернета как универсальной публичной сети.

Данная статья знакомит читателя со всеми основными особенностями системы адресации как в текущей версии IPv4, так и в нивой версии IPv6.

Сети Ethernet

Чаще всего при создании локальных сетей используется аппаратная архитектура, называемая Ethernet. В сети Ethernet данные передаются но одному длинному кабелю, к которому при помощи разъемов, коннекторов и трансиверных кабелей подключаются все сетевые узлы. Сеть Ethernet несложно установить, требуемое для этого оборудование стоит недорого, а скорость передачи данных (10 Мбит/с) вполне достаточна для решения большинства задач, связанных с обменом данными. Благодаря всем этим факторам Ethernet является самой популярной аппаратной архитектурой, используемой при создании локальных сетей. Существуют три разновидности Ethernet: тонкий, толстый и витая пара. При использовании

тонкого или толстого Ethernet данные передаются через коаксиальный кабель различной толщины. Метод соединения компьютеров с кабелем также отличается. Для подключения компьютера к тонкому кабелю Ethernet используется разъем специальной Т-образной формы, называемый Т-коннектором. Чтобы подключить компьютер к толстому кабелю Ethernet, требуется просверлить в кабеле небольшое отверстие и при помощи специального прокалывающего приспособления (vampire tap) подсоединить к нему вспомогательный трансиверный кабель. К трансиверному кабелю можно подсоединить один или несколько сетевых узлов. Тонкий кабель Ethernet может достигать 200 метров в длину. Толстый - 500 метров. Эти разновидности Ethernet называют 10base-2 и 10base-5 соответственно. При использовании витой пары данные передаются но кабелю, состоящему из двух медных проводов. Обычно при этом требуется установить дополнительное устройство, называемое активным концентратором (active hub). Витую пару обозначают 10base-T.

Подсоединить к сети, использующей толстый кабель Ethernet, новый сетевой узел несколько сложно, однако при этом не требуется останавливать работу сети. Чтобы подсоединить сетевой узел к тонкому кабелю Ethernet, требуется но крайней мере на несколько минут прервать передачу всех сетевых данных, так как в этом случае необходимо разорвать кабель и вставить в разрыв новый Т-коннектор. Чаще всего для создания сетей используется тонкий кабель Ethernet, так как при этом требуются относительно небольшие финансовые затраты. Однако в случае если требуется соединить в сеть большое количество компьютеров, толстый Ethernet является более приемлемым решением. Например, в коммерческом отделе фирмы Maxisoft компьютерная сеть построена на базе толстого Ethernet, так как при этом, чтобы подсоединить к общему кабелю новый сетевой узел, не требуется

нарушать работу всей сети.

Одним из существенных недостатков Ethernet является ограничение на длину общего кабеля. Относительно небольшая длина сетевого сегмента позволяет использовать Ethernet только при создании локальных сетей. Однако несколько сетевых сегментов Ethernet можно соединить друг с другом при помощи повторителей (repeaters), мостов (bridges) или маршрутизаторов (routers). Повторители только лишь передают сигналы из сегмента в сегмент, при этом усиливая их. Благодаря этому все сегменты сети работают так, как будто они являются единым сегментом Ethernet. Из-за ограничений, связанных с временными задержками, между любыми двумя сетевыми узлами может быть установлено не более чем четыре повторителя. Мосты и маршрутизаторы являются более сложными устройствами. Они анализируют поступающие данные и передают их и другой сегмент только в случае, если принимающий сетевой узел расположен в другом сегменте сети, Сеть Ethernet работает подобно единой шине, через которую любой узел может пересылать пакеты (или фреймы) размером до 1500 байт, предназначенные для другого узла, подключенного к этому же сегменту Ethernet, Узел адресуется шестибайтовым адресом, хранящимся в постоянном запоминающем устройстве сетевой карты. Каждая сетевая карта обладает своим собственным уникальным адресом Ethernet, который присваивается ей на этане производства и который сменить нельзя. Адрес Ethernet обычно записывают как последовательность из шести двухзначных шестнадцатеричных чисел, разделенных символом двоеточия. Например; aa:bb:cc:dd:ee:ff.

Фрейм, посланный одним из узлов, принимается всеми подключенными к сегменту Ethernet узлами, однако только узел назначения обращает на него

внимание и начинает его обработку, Если два узла пытаются переслать фрейм одновременно, происходит коллизия (collision) или, по-другому, столкновение. Чтобы разрешить конфликт, оба узла прекращают передачу и осуществляют новую попытку, спустя некоторое короткое время,

Пользовательский протокол дейтаграмм

Помимо протокола TCP в сетях IP используются также некоторые другие протоколы. Напомним, что TCP используется для разбиения единого потока данных на пакеты. Он также отмечает за то, чтобы на принимающем конце все пересланные пакеты были приняты и объединены в единый ноток данных. Однако некоторые приложения обмениваются через сеть сообщениями, которые вполне умещаются в рамках одного пакета. Чтобы переслать через сеть столь короткое сообщение, нет необходимости использовать TCP. В этом случае для передачи данных вместо TCP используют похожий на него пользовательский протокол дейтаграмм (User Datagram Protocol, UDP). Этот протокол предназначен для пересылки через сеть отдельных пакетов, которые не требуется объединять в единый ноток данных. Благодаря этому заголовок UDP занимает меньший объем, позволяя более экономно расходовать пропускную способность каналов связи. Мало того, UDP не требует создания отдельного логического канала связи между двумя компьютерами. Таким образом, не требуется тратить время на выполнение процедур установления и разрыва сеанса связи.

Типы адресов
в составных сетях

В стеке TCP/IP используются три типа адресов: локальные (называемые также аппаратными), IP-адреса и символьные доменные имена.

В терминологии TCP/IP под локальным адресом понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные сгеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес - это MAC-адрес. MAC-адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC-адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байт, например 11-AO-17-3D-BC-01. Однако протокол IP может работать и над протоколами более высокого уровня, например над протоколом IPX или X.25. В этом случае локальными адресами для протокола IP, соответственно, будут адреса IPX и X.25. Следует учесть, что компьютер в локальной сети может иметь несколько локальных адресов даже при одном сетевом адаптере. Некоторые сетевые устройства не имеют локальных адресов. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа «точка - точка».

Для того чтобы сетевой уровень, представленный в стеке TCP/IP протоколом IP, мог выполнить свою задачу, ему необходима собственная система адресации, не зависящая от способов адресации узлов в отдельных подсетях, которая позволила бы ему ссылаться универсальным и однозначным способом на любой узел составной сети. Эта система адресации основана на так называемых IP-адресах. Естественным способом формирования адреса сетевого уровня является уникальная нумерация всех подсетей составной сети с последующей нумерацией всех узлов в пределах каждой подсети.

Таким образом, IP-адрес представляет собой пару: номер сети (подсети) и номер узла. Заметим, что в протоколах локальных сетей понятие «номер сети» отсутствует - предполагается, что все узлы принадлежат одной сети. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты в сетях любой топологии. В качестве номера узла может быть использован либо локальный адрес этого узла (такая схема принята в стеке IPX/SPX), либо некоторое число, никак не связанное с локальной технологией, которое однозначно идентифицирует узел в пределах данной подсети. В первом случае сетевой адрес становится зависимым от локальных технологий, что ограничивает его применение. Например, сетевые адреса IPX/SPX рассчитаны на работу в составных сетях, объединяющих сети, в которых в качестве локальных адресов используются только MAC-адреса. Второй подход более универсален, именно он использован в стеке TCP/IP - IP-адрес назначается узлу независимо от его локального адреса. Примеры IP-адресов: 193.27.21.15,140.45.23.155,12.146.0.129. Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/IP полагается на IP-адреса, поэтому для доступа к сетевому ресурсу в параметрах программы вполне достаточно указать IP-адрес, чтобы программа правильно поняла, к какому хосту ей нужно обратиться.

Однако пользователи обычно предпочитают работать с символьными именами компьютеров, и операционные системы локальных сетей приучили их к этому удобному способу. Символьные имена в IP-сетях (называемые также доменными) строятся по иерархическому признаку. Примером доменного имени может служить имя

site2.sale.ats.ru Между доменным именем и IP-адресом узла нет никакого алгоритмического соответствия, поэтому необходимо использовать какие-то

дополнительные таблицы или службы, чтобы узел сети однозначно определялся как по доменному имени, так и по IP-адресу. В сетях TCP/IP используется специальная распределенная служба Domain Name System (DNS) которая устанавливает это соответствие на основании набираемых администраторами сети таблиц соответствия.

Классы IP адресов

IP-адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками, например, 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса.

Адрес состоит из двух логических частей - номера сети и номера интерфейса узла в сети.

Часто для упрощения номер интерфейса узла называют номером узла. Какая часть адреса относится к номеру сети, а какая - к номеру узла, определяется значениями первых бит адреса.

Значения этих бит являются также признаками того, к какому классу относится тот или иной IP-адрес:

• Если адрес начинается с 0, то сеть относят к классу A, и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сетей класса A немного, зато количество узлов в них теоретически может достигать 224, то есть 16777 216 узлов.

• Если первые два бита адреса равны 10, то сеть относится к классу B. В сетях класса B под номер сети и под номер узла отводится по 2 байта. Таким образом, сеть класса B является сетью средних размеров с максимальным числом узлов 65 536.

• Если адрес начинается с последовательности 110, то это сеть класса C.

В этом случае под номер сети отводится три байта, а под номер узла - один байт. Сети этого класса наиболее распространены, число узлов в них ограничено 256 узлами.

• Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которым
присвоен данный адрес.

• Если адрес начинается с последовательности 11110, то это
значит, что данный адрес относится к классу E. Адреса этого
класса зарезервированы для будущих применений.

Адреса классов A, B и C относят к адресам типа unicast, которые, в отличие от групповых адресов типа multicast, уникально идентифицируют отдельные узлы (а более точно, отдельные интерфейсы узлов) составной сети.

При адресации сетей и узлов необходимо учитывать те ограничения, которые вносятся из-за особого назначения некоторых IP-адресов. Так, сеть не может иметь нулевой номер, а номер узла не может состоять только из одних двоичных единиц или только из одних двоичных нулей. Если весь IP-адрес состоит только из двоичных нулей, то он обозначает адрес того узла, который сгенерировал этот пакет. Если в поле номера сети назначения стоят только нули, то по умолчанию считается, что узел назначения принадлежит той же самой сети, что и узел, который отправил пакет. Если все двоичные разряды IP-адреса равны 1, то пакет с таким адресом назначения должен рассылаться всем узлам, находящимся в той же сети, что и источник этого пакета (limited boardcast - ограниченное широковещательное сообщение). Наконец, если номер узла назначения состоит только из единиц, то пакет, имеющий такой адрес, рассылается всем узлам сети с заданным номером сети

(boardcast - широковещательное сообщение).

Отсюда следует, что максимальное количество узлов, указанное выше для сетей каждого класса, на практике должно быть уменьшено на 2. Например, в сетях класса C под номер узла отводится 8 бит, которые позволяют задавать 256 номеров: от 0 до 255. Однако на практике максимальное число узлов в сети класса C не может превышать 254, так как адреса 0 и 255 имеют специальное назначение. Из этих же соображений следует, что конечный узел не может иметь адрес типа 98.255.255.255, поскольку номер узла в этом адресе класса A состоит из одних двоичных единиц.

Особый смысл имеют IP-адреса, первый октет которых равен 127. Такие адреса, называемые localhost, используются для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные, например, по IP-адресу 127.0.0.1, то они не передаются по сети, а возвращаются модулям верхнего уровня как только что принятые.

Поэтому в IP-сети запрещается присваивать узлам IP-адреса, начинающиеся со 127.

Характеристики адрессов разного класса

класс	первые биты	наименьший номер сети	наибольший номер сети	максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2.24-2
B	10	128.0.0.0	191.255.0.0	2.16-2
C	110	192.0.1.0	223.255.255.0	2.8-2
D	1110	224.0.0.0	239.255.255.255	multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервирован

В таблице (#1) приведены диапазон номеров сетей и максимальное количество узлов, соответствующие каждому классу сетей. Уже упоминавшаяся форма группового IP-адреса - multicast - означает, что данный пакет должен быть доставлен сразу нескольким узлам, которые образуют группу с номером, указанным в поле адреса. Узлы сами идентифицируют себя, то есть определяют, к какой из групп они относятся. Один и тот же узел может входить в несколько групп.

Члены какой-либо группы multicast не обязательно должны принадлежать одной сети. В общем случае они могут распределяться по совершенно различным сетям, находящимся друг от друга на произвольном количестве хопов. Групповой адрес не делится на поля номера сети и узла и обрабатывается маршрутизатором особым образом. Основное назначение multicast-адресов - распространение информации по схеме «один-ко-многим». Хост, который хочет передавать одну и ту же информацию многим абонентам, с помощью специального протокола IGMP (Internet Group Management Protocol) сообщает о создании в сети новой мультивещательной группы с определенным адресом. Машрутизаторы, поддерживающие мультивещательность, распространяют информацию о создании новой группы в сетях, которые непосредственно подключены к портам этого маршрутизатора. Хосты, которые хотят присоединиться к вновь создаваемой мультивещательной группе, сообщают об этом своим локальным маршрутизаторам, и те передают эту информацию хосту - инициатору создания новой группы. Группы могут быть постоянными (permanent) или временными (transient). Постоянная группа имеет адрес, централизованно назначенный административным органом Интернета, и существует всегда, независимо от того, сколько членов она насчитывает в данный момент. Временная группа существует только тогда, когда в ней имеются

присоединившиеся к ней члены. Все множество адресов класса D разделяется на три диапазона. Адреса диапазона 224.0.0.1 - 224.0.0.255 представляют собой зарезервированные, так называемые хорошо известные (well-know) адреса постоянных групп локального назначения. Например, адрес 224.0.0.1 обозначает группу, включающую все узлы данной сети, адрес
224.0.0.2 - группу маршрутизаторов, присоединенных к данной сети, адрес 224.0.0.9 - группу RIP-маршрутизаторов данной сети. Адреса диапазона 224.0.1.0 - 238.255.255.255 предназначены для использования в масштабах Интернета. Часть этого диапазона уже распределена: например, адрес 224.0.0.7 выделен группе хостов, являющихся абонентами службы аудионовостей, а 224.0.1.16 - абонентами музыкального сервиса. Адреса диапазона 239.0.0.0 - 239.255.255.255 предназначены для создания временных групп локального назначения.

Чтобы маршрутизаторы могли автоматически распространять пакеты с адресом multicast по составной сети, необходимо использовать в конечных маршрутизаторах модифицированные протоколы обмена маршрутной информацией, такие, как, напри-
мер, MOSPF (Multicast OSPFаналог OSPF).

Групповая адресация предназначена для экономичного распространения в Интернете или большой корпоративной сети аудио- или видеопрограмм, предназначенных сразу большой аудитории слушателей или зрителей. Если такие средства найдут широкое применение (сейчас они представляют в основном небольшие экспериментальные островки в общем Интернете, то Интернет сможет создать серьезную конкуренцию радио и телевидению.

Порядок распределения IP-адресов

Номера сетей назначаются либо централизованно, если сеть является частью Интернета, либо произвольно, если сеть работает автономно. Номера узлов и в том, и в другом случае администратор волен назначать по своему усмотрению, не выходя, разумеется, из разрешенного для этого класса сети диапазона. Координирующую роль в централизованном распределении IP-адресов до некоторого времени играла организация InterNIC, однако с ростом сети задача распределения адресов стала слишком сложной, и InerNIC делегировала часть своих функций другим организациям и крупным поставщикам услуг Интернета.

Уже сравнительно давно наблюдается дефицит IP-адресов. Очень трудно получить адрес класса B и практически невозможно стать обладателем адреса класса A. При этом надо отметить, что дефицит обусловлен не только ростом сетей, но и тем, что имеющееся множество IP-адресов используется нерационально. Например, часто для вырожденной сети, образованной каналом, связывающим порты двух смежных маршрутизаторов, соединенных по схеме «точка - точка», выделяется отдельный номер сети. В таком случае из всего возможного диапазона номеров узлов используются только 2, а остальные «пропадают» зря. Если же некоторая IP-сеть создана для работы в «автономном режиме», без связи с Интернетом, тогда администратор этой сети волен назначить ей произвольно выбранный номер. Но и в этой ситуации для того, чтобы избежать каких-либо коллизий, в стандартах Интернета определены несколько диапазонов адресов, рекомендуемых для локального использования. Эти адреса не обрабатываются маршрутизаторами Интернета ни при каких условиях. Адреса, зарезервированные для локальных целей, выбраны из разных

классов:

в классе А - это сеть 10.0.0.0,

в классе В - это диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0,

в классе С -это диапазон из 255 сетей - 192.168.0.0-192.168.255.0.

Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы. Принципиальным решением является переход на новую версию IPv6, в которой резко расширяется адресное пространство за счет использования 16-байтных адресов. Однако и текущая версия IPv4 поддерживает некоторые технологии, направленные на более экономное расходование IP-адресов.

Одной из таких технологий является трансляция адресов (Network Adress Translator, NAT) Узлам внутренней сети адреса назначаются произвольно (естественно, в соответствии с общими правилами, определенными в стандарте), так, как будто эта сеть работает автономно.

Внутренняя сеть соединяется с Интернетом через некоторое промежуточное устройство (маршрутизатор, межсетевой экран). Это промежуточное устройство получает в свое распоряжение некоторое количество внешних «нормальных» IP-адресов, согласованных с провайдером или другой организацией, распределяющей IP-адреса. Промежугочное устройство способно преобразовывать внутренние адреса во внешние, используя для этого некие таблицы соответствия. Для внешних пользователей все многочисленные узлы внутренней сети выступают под несколькими внешними IP-адресами. При по лучении внешнего запроса это устройство анализирует его содержимое и при необходимости пересылает его во внутреннюю сеть, заменяя IP-адрес на внутренний адрес этого узла. Процедура трансляции адресов определена в RFC 1631.

Другая технология, которая может быть использована для снятия

дефицита адресов, - это технология масок и ее развигие технология бесклассовой междоменной маршрутизации (Classess Inter-Domain Routing, CIDR).

Использование масок в IP-адресации

Механизм масок широко распространен в IP-маршрутизации, причем маски могут использоваться для разных целей. С их помощью администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей. На основе этого же механизма поставщики услуг могут объединять адресные пространства нескольких сетей путем введения так называемых префиксов с целью уменьшения объема таблиц маршрутизации и повышения за счет этого производительности маршрутизаторов.

Традиционная схема деления IP-адреса на номер сети и номер узла основана на понятии класса, который определяется значениями нескольких первых битов адреса. Именно потому, что первый байт адреса 185.23.44.206 попадает в диапазон 128-191, мы можем сказать, что этот адрес относится к классу B, а значит, номером сети являются первые два байта, дополненные двумя нулевыми байтами, - 185.23.0.0, а номером узла - 0.0.44.206. А что, если использовать какой-либо другой признак, с помощью которого можно было бы более гибко устанавливать границу между номером сети и номером узла? В качестве такого признака сейчас получили широкое распространение маски. Маска - это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную

последовательность.

Для стандартных классов сетей маски имеют следующие значения:

• класс А - 11111111. 00000000. 00000000. 00000000
(255.0.0.0);

• класс В -
(255.255.0.0);

• класс С -
(255.255.255.0).

Для записи масок используются и другие форматы, например, удобно интерпретировать значение маски, записанной в шестнадцатеричном коде: FF.FF.00.00 - маска для адресов класса В.

Часто встречается и такое обозначение: 185.23.44.206/16 - эта запись говорит о том, что маска для этого адреса содержит 16 единиц или что в указанном IP-адресе под номер сети отведено 16 двоичных разрядов. Снабжая каждый IP-адрес маской, можно отказаться от понятий классов адресов и сделать более гибкой систему адресации. Например, если рассмотренный выше адрес 185.23.44.206 ассоциировать с маской 255.255.255.0, то номером сети будет 185.23.44.0, а не 185.23.0.0, как это определено системой классов. В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты. Пусть, например, для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде IP-адрес 129.64.134.5 - 10000001.01000000. 10000110. 00000101; маска 255.255.128.0 - 11111111.11111111.10000000.00000000.

Если игнорировать маску, то, в соответствии с системой клас сов, адрес 129.64.134.5 относится к классу В, а значит, номером сети являются первые 2 байта - 129.64.0.0, а номером узла - 0.0.134.5.

Если же использовать для определения границы номера сети маску, то 17 последовательных единиц в маске, «наложенные» на IP-адрес, определяют в качестве номера сети в двоичном выражении число 10000001. 01000000. 10000000. 00000000 или в десятичной форме записи - номер сети 129.64.128.0, а номер узла 0.0.6.5.

Технология масок позволяет разделять одну сеть на несколько сетей. Представим, что администратор получил в свое распоряжение адрес класса B: 129.44.0.0. Он может организовать сеть с большим числом узлов, номера которых он может брать из диапазона 0.0.0.1-0.0.255.254. Однако ему не нужна одна большая неструктурированная сеть, производственная необходимость диктует администратору другое решение, в соответствии с которым сеть должна быть разделена на три отдельных подсети, при этом трафик в каждой подсети должен быть надежно локализован. Это позволит легче диагностировать сеть и проводить в каждой из подсетей особую политику безопасности.

Посмотрим, как решается эта проблема путем использования механизма масок.

Итак, номер сети, который администратор получил от поставщика услуг, - 129.44.0.0 (10000001 00101100 00000000 00000000). В качестве маски было выбрано значение 255.255.192.0 (1111111111111111 11000000 00000000). После наложения маски на этот адрес число разрядов, интерпретируемых как номер сети, увеличилось с 16 (стандартная длина поля номера сети для класса B) до 18 (число единиц в маске), то есть администратор получил возможность использовать для нумерации подсетей два дополнительных бита. Это позволяет ему сделать из одного, централизованно заданного ему, номера сети еще четыре:

129.44.0.0 (10000001 00101100 00000000 00000000);

129.44.64.0 (10000001 00101100 01000000 00000000);

129.44.128.0 (10000001 00101100 10000000 00000000);

129.44.192.0(10000001 00101100 1100000000000000).

Два дополнительных последних бита в номере сети часто интерпретируются как номера подсетей (subnet), и тогда четыре перечисленных выше подсети имеют номера 0 (00), 1 (01), 2 (10) и 3 (11) соответственно.

ПРИМЕЧАНИЕ

Некоторые программные и аппаратные маршрутизаторы не поддерживают номера подсетей, которые состоят либо только из одних нулей, либо только из одних единиц. Например, для некоторых типов оборудования номер сети 129.44.0.0 с маской 255.255.192.0, использованный в нашем примере, окажется недопустимым, поскольку в этом случае разряды в поле номера подсети имеют значение 00. По аналогичным соображениям недопустимым может оказаться и номер сети 129.44. 192.0 с тем же значением маски. Здесь номер подсети состоит только из единиц. Однако более современные маршрутизаторы свободны от этих ограничений. Поэтому, принимая решение об использовании механизма масок, необходимо выяснить характеристики того оборудования, которым вы располагаете, чтобы соответствующим образом сконфигурировать маршрутизаторы и компьютеры сети. В результате использования масок была предложена следующая схема распределения адресного пространства (рис. 1).

1 байт	2байт	3байт	4байт
Поле номера сети класса B (неизменяемое поле) 129 44	№ подсети	Поле адресов узлов (адресное пространство)	
10000001 00101100	0 0	000000	00000000
10000001 00101100	1 1	111111	11111111
10000001 00101100	0 1	000000	00000000
00101100	0 1	111111	11111111
10000001 00101100	1 0	000000	00000000
10000001 00101100	1 0	111111	11111111
10000001 00101100	1 1	000000	00000000
10000001 00101100	1 1	000000	00000001
10000001 00101100	1 1	000000	00000010
неиспользованные адреса			

Рис. 1. Разделение адресного пространства сети класса B 129.44.0.0 на четыре равных части путем использования масок одинаковой длины 255.255.192.0

Сеть, получившаяся в результате проведенной структуризации, показана на рис. 2. Весь трафик во внутреннюю сеть 129.44.0.0, направляемый из внешней сети, поступает через маршрутизатор M1. В целях структуризации информационных потоков во внутренней сети установлен дополнительный маршрутизатор M2. (Заметим, что разделение большой сети, имеющей один адрес старшего класса, например A или B, с помощью масок несет в себе еще одно преимущество по сравнению с использованием нескольких адресов стандартных классов для сетей меньшего размера, например C. Оно позволяет скрыть внутреннюю структуру сети предприятия от внешнего наблюдения и тем повысить ее безопасность.) Все узлы были распределены по трем разным сетям, которым

были присвоены номера 129.44.0.0, 129.44.64.0 и 129.44.128.0 и маски одинаковой длины - 255.255.192.0. Каждая из вновь образованных сетей была подключена к соответственно сконфигурированным портам внутреннего маршругизатора М2. Кроме того, еще одна сеть (номер 129.44.192.0, маска 255.255.192.0) была выделена для создания соединения между внешним и внутренним маршрутизаторами.

В этой сети для адресации узлов было занято всего два адреса, 129.44.192.1 (порт маршрутизатора М2) и 129.44.192.2 (порт маршрутизатора М1), еще два адреса,

Рис. 2. Маршрутизация с использованием масок одинаковой длины

129.44.192.0 и 129.44.192.255, являются особыми адресами.

Следовательно, огромное число узлов (2/14степени -4) в этой подсети никак не используются.

В этом случае, как и во многих других, более эффективным явилось бы разбиение сети на подсети разного размера. Администратор может более рационально распределить имеющееся в его распоряжении адресное пространство с помощью масок переменной длины.

На рис. 3 приведен пример распределения адресного пространства, а на рис. 4 показана схема структуризации сети путем использования масок переменной длины. Половина из имеющихся адресов (2/15 степени) была отведена для создания сети с адресом 129.44.0.0 и маской 255.255.128.0. Следующая порция адресов, составляющая четверть всего адресного пространства (2\14степени), была назначена для сети 129.44.128.0 с маской 255.255.192.0. Далее в пространстве адресов был «вырезан» небольшой

фрагмент для создания сети, предназначенной для связывания внутреннего маршрутизатора М2 с внешним маршрутизатором М1. Для поля номера узла в IP-адресе такой вырожденной сети, как минимум, должно быть отведено два двоичных разряда. Из четырех возможных комбинаций номеров узлов: 00, 01, 10и11- два номера имеют специальное назначение и не могут быть присвоены узлам, но оставшиеся два, 10 и 01, позволяют адресовать порты маршрутизаторов. В нашем примере сеть была выбрана с некоторым запасом - на 8 узлов. Поле номера узла в таком случае имеет 3 двоичных разряда, маска в десятичной нотации имеет вид 255.255.255.248, а номер сети, как видно из рисунка, равен в данном конкретном случае

Рис. 3. Разделение адресного пространства сети класса В 129.44.0.0 на сети разного размера путем использования масок переменной длины

129.44.192.0. Если эта сеть является локальной, то на ней могут быть расположены четыре узла помимо двух портов маршу ртизаторов.

ПРИМЕЧАНИЕ

Заметим, что глобальным связям между маршругизаторами типа «точка - точка» не обязательно давать Р-адреса, так как к такой сети не могут подключаться никакие другие узлы, кроме двух портов маршрутизаторов. Однако чаще всего такой вырожденной сети все же дают IP-адрес, как это и было сделано в предыдущем примере. Это делается для того, чтобы при необходимости скрыть внутреннюю структуру сети к ней можно было бы обращаться по адресу входного порта маршрутизатора, в данном примере - по адресу 129.44.192.1. Кроме того, этот адрес может понадобиться при туннелировании немаршрутизируемых протоколов в IP-пакетах.

Рис. 4. Сеть, структурированная с использованием масок

переменной длины

Оставшееся адресное пространство администратор может «нарезать» на разное количество сетей разного объема в зависимости от своих потребностей. Из оставшегося пула (2\14степени-4) адресов администратор может образовать еще одну достаточно большую сеть с числом узлов 2\13степени. При этом свободными останутся почти столько же адресов (2\13степени-4), которые также могут быть использованы для создания новых сетей. К примеру, из этого «остатка» можно образовать 31 сеть, каждая из которых равна размеру стандартной сети класса С, и к тому же еще несколько сетей меньшего размера. Ясно, что разбиение может быть другим, но в любом случае с помощью масок переменного размера администратор всегда имеет возможность гораздо рациональнее использовать все имеющиеся у него адреса.

Технология бесклассовой междоменной маршрутизации CIDR

За последние несколько лет в сети Интернет многое изменилось: резко возросло число узлов и сетей, повысилась интенсивность трафика, изменился характер передаваемых данных. Из-за несовершенства протоколов маршрутизации обмен сообщениями об обновлении таблиц стал иногда приводить к сбоям магистральных маршрутизаторов из-за перегрузки при обработке большого объема служебной информации. Так, в 1994 году таблицы магистральных маршрутизаторов в Интернете содержали до 70 000 маршрутов. На решение этой проблемы была направлена, в частности, и технология бесклассовой междоменной маршрутизации (Classless Inter-Domain Routing, CIDR), о которой впервые было официально объявлено в

1993 году, когда были опубликованы RFC 1517, RFC 1518, RFC 1519 и RFC 1520.

Суть технологии CIDR заключается в следующем. Каждому поставщику услуг Интернета должен назначаться непрерывный диапазон в пространстве IP-адресов. При таком подходе адреса всех сетей каждого поставщика услуг имеют общую старшую часть префикс, поэтому маршрутизация на магистралях Интернета может осуществляться на основе префиксов, а не полных адресов сетей.

Агрегирование адресов позволит уменьшить объем таблиц в маршрутизаторах всех уровней, а следовательно, ускорить работу маршрутизаторов и повысить пропускную способность Интернета.

Рис. 5. Технология CIDR

Рис. 6. Выигрыш в количестве записей в маршрутизаторе

при использовании технологии CIDR Деление IP-адреса на номер сети и номер узла в технологии CIDR происходит не на основе нескольких старших бит, определяющих класс сети (A, B или C), а на основе маски переменной длины, назначаемой поставщиком услуг. На рис. 5 показан пример некоторого пространства IP-адресов, которое имеется в распоряжении гипотетического поставщика услуг. Все адреса имеют общую часть в k старших разрядов - префикс. Оставшиеся n разрядов используются для дополнения неизменяемого префикса переменной частью адреса. Диапазон имеющихся адресов в таком случае составляет 2n. Когда потребитель услуг обращается к поставщику услуг с просьбой о выделении ему некоторого количества адресов, то в имеющемся пуле адресов «вырезается» непрерывная область соответствующего размера. Причем границы этой области

выбираются такими, чтобы для нумерации требуемого числа узлов хватило некоторого числа младших разрядов, а значения всех оставшихся (старших) разрядов были одинаковыми у всех адресов данного диапазона. Таким условиям могут удовлетворять только области, размер которых кратен степени двойки. А границы выделяемого участка должны быть кратны требуемому размеру. Рассмотрим пример. Пусть поставщик услуг Интернета располагает пулом адресов в диапазоне 193.20.0.0-193.23.255.255 (1100 0001.0001 0100.0000 0000.0000 0000-1100 0001.0001 0111.1111 1111.1111 1111) с общим префиксом 193.20 (1100 0001.0001 01) и маской, соответствующей этому префиксу, 255.252.0.0.

Если абоненту этого поставщика услуг требуется совсем немного адресов, например 13, то поставщик мог бы предложить ему различные варианты: сеть 193.20.30.0, сеть 193.20.30.16 или сеть 193.21.204.48, все с одним и тем же значением маски 255.255.255.240. Во всех случаях в распоряжении абонента для нумерации узлов имеется 4 младших бита. Рассмотрим другой вариант, когда к поставщику услуг обратился крупный заказчик, сам, возможно, собирающийся оказывать услуги по доступу в Интернет.

Ему требуется блок адресов в 4000 узлов. В этом случае поставщик услуг мог бы предложить ему, например, диапазон адресов 193.22.160.0-193.22.175.255 с маской 255.255.240.0.

Агрегированный номер сети (префикс) в этом случае будет равен 193.22.160.0.

Администратор маршрутизатора М2 (рис. 6) поместит в таблицу маршрутизации только по одной записи на каждого клиента, которому был выделен пул адресов, независимо от количества подсетей, организованных клиентом. Если клиент, получивший сеть 193.22.160.0, через некоторое время разделит ее адресное пространство в 4096 адресов на 8 подсетей, то в

маршрутизаторе М2 первоначальная информация о выделенной ему сети не изменится.

Для поставщика услуг верхнего уровня, поддерживающего клиентов через маршрутизатор М1, усилия поставщика услуг нижнего уровня по разделению его адресного пространства также не будут заметны.

Запись 193.20.0.0 с маской 255.252.0.0 полностью описывает сети поставщика услуг нижнего уровня в маршрутизаторе М 1.

Итак, внедрение технологии CIDR позволяет решить две основные задачи:

• Более экономное расходование адресного пространства.

• Уменьшение числа записей в таблицах маршрутизаторов за счет объединения маршрутов.

Технология CIDR уже успешно используется в текущей версии IPv4 и поддерживается такими протоколами маршрутизации, как OSPF, RIP-2, BGP4. Предполагается, что эти же протоколы будут работать и с новой версией протокола IPv6. Следует отметить, что в настоящее время технология CIDR поддерживается в основном магистральными маршрутизаторами Интернета. Использование CIDR в сетях IPv4 в общем случае требует перенумерации сетей. Поскольку эта процедура сопряжена с определенными временными и материальными затратами, для ее проведения пользователей нужно каким-либо образом стимулировать. В качестве такого стимула рассматривается, например, введение оплаты за строку в таблице маршрутизации или же за количество узлов в сети. Требование оплаты каждого адреса узла поможет пользователю решиться па перенумерацию с тем, чтобы получить ровно столько адресов, сколько ему нужно.

IP через линии последовательной передачи данных

Стандартным протоколом для передачи данных через последовательные

линии связи является протокол SLIP (Serial Line IP). Модифицированный протокол под названием CSLIP (Compressed SLIP) предусматривает сжатие заголовков IP, обеспечивая при этом более эффективное использование пропускной способности последовательного канала передачи данных. Помимо SLIP для передачи данных через последовательные линии используется также совершенно другой протокол под названием PPP (Point-to-Point Protocol), который иногда называют протоколом «точка-точка». По сравнению со SLIP, протокол PPP обладает более широкими возможностями. В частности, он предусматривает фазу инициализации сеанса связи, а также позволяет передавать через последовательный канал не только пакеты IP, но и любые другие разновидности пакетов данных.

Особенности адресации в IPv6

Новая, шестая версия протокола IP (IPv6) внесла существенные изменения в систему адресации IP-сетей (RFC 2373). Адрес IPv6 состоит из 128 бит или 16 байт. Такое значительное увеличение длины адреса нужно не только для снятия проблемы дефицита адресов, но и для дальнейшего повышения эффективности работы всего стека TCP/IP. В частности, в новой версии уменьшаются затраты на маршрутизацию за счет стандартизации схем агрегирования адресов, более совершенной системы групповой адресации и введения нового типа адресов anycast.

Произошли и чисто внешние изменения - наконец-то разработчики стандарта отказались от десятичной формы записи IP-адреса, которая очень неудобна при определении номера сети для случая, когда граница маски не совпадает с границей байтов адреса. Теперь предпочтительной формой записи адреса стало его шестнадцатеричное представление, причем каждые четыре

шестпадцатеричные цифры отделяются друг от друга двоеточием, например: FEDC:0A98:0:0:0:0:7654:3210.

Если в адресе имеегся длинная последовательность нулей, то запись адреса можно сократить. Например, приведенный выше адрес можно записать так: FECD:0A98::7654:3210.

Сокращение «::» 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, а для старших 12 байт - предпочтительную для IPv6 шестнадцатеричную форму: 0:0:0:0:0:FFFF:129.144.52.38 или ::FFFF:129.144.52.38.

В IPv6 определено 3 основных типа адресов: unicast, multicast и anycast. Тип адреса задается значением нескольких старших бит адреса, которые названы префиксом формата. Адрес типа unicast определяет уникальный идентификатор отдельного интерфейса конечного узла или маршрутизатора. Назначение этого типа адреса 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, адреса этого типа делятся на несколько подтипов для отражения специфики некоторых часто встречающихся в современной составной сети ситуаций.

Основным подтипом является глобальный агрегируемый уникальный адрес, который предназначен для идентификации узлов и Интернете. Такие адреса могут агрегироваться в стиле технологии CIDR для упрощения маршрутизации. В отличие от уникальных адресов узлов версии ***4, которые состоят и.) двух полей - номера сети и номера узла, глобальные агрегируемые уникальные адреса IPv6 имеют более сложную структуру,

включающую шесть полей. Поле FP - это префикс формата, который для этого типа адресов состоит из 3 бит и имеет значение 001. В соответствии с идеями технологии CIDR эти три поля рассматриваются как префиксы трех уровней - верхнего уровня агрегирования адресов (Top-Level Aggregation, TLA) следующего уровня агрегирования (Next-Level Aggregation, NLA) и местного уровня агрегирования (Cite-Level Aggregation, CLA)
Префиксы верхнего уровня могут идентифицровать, например, крупных провайдеров.

Конкретное значение этого префикса представляет собой общую часть адресов всех абонентов этого провайдера. Префикс местного уровня предназначен для агрегирования адресов подсетей отдельного абонента. Префикс следующего уровня играет промежуточную роль в агрегировании адресов. Однобайтовое поле между полями TLA и SLA пока зарезервировано. Префиксы агрегирования образуют соответствующий номер подсети. Идентификатор интерфейса (Interface ID)является аналогом номера узла IPv4. Идентификаторы интерфейсов используются в адресах типа unicast для однозначного определения интерфейсов в пределах какой-либо подсети. Отличием версии IPv6 является то, что в общем случае идентификатор интерфейса просто совпадает с его локальным адресом, а не представляет собой произвольно назначенный администратором номер узла. Идентификатор интерфейса имеет длину 64 бита, что позволяет поместить туда MAC-адрес (48 бит), или адрес X.25 (до 60 бит), или адрес конечного узла ATM (48 бит), или номер виртуального соединения ATM (до 28 бит), а также дает возможность использовать локальные адреса технологий, которые могут появиться в будущем. Такой подход в стиле протокола IPX делает ненужным использование протокола 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.

Существуют два специальных адреса типа unicast - адрес обратратной связи и неопределенный адрес. Они имеют префикс формата 0000 0000 и отличаются только значением младшего бита.

Адрес обратной связи 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. Неопределенный адрес ::, состоящий из одних нулей, является аналогом адреса 0.0.0.0 протокола версии IPv4. Такое значение говорит о том, что у узла отсутствует назначенный IP-адрес. Этот адрес не должен появляться в IP-пакетах в качестве адреса назначения. Если же он появляется в поле адреса источника, то это означает, что пакет послан до того, как узел изучил свой IP-адрес (например. до получения его от DHCP-сервера).

Еще две разновидности unicast-адресов с префиксом формата 0000 0000 предназначены для обеспечения совместимости версий IPv4 и IPv6. Разработчики IPv6 придают очень большое значение средствам, обеспечивающим плавный переход с версии IPv4 на IPv6. 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 протокола IPv6. могли использовать технику туннелирования пакетов IPv6 через сеть IPv4, разработан специальный подтип адресов, которые переносят адрес IPv4 в младших 4 байтах адреса IPv6, а в старших 12 байтах адреса содержат нули. Такой тип unicast-адресов делает очень простой процедуру преобразования

адресов "IPv6-IPv4" и называется IPv4-совместимыми адресами IPv6.

Имеется еще одна разновидность адреса IPv6, переносящего адрес IPv4, - это так называемый IPv4-отображенный адрес IPv6. Он предназначен для решения обратной задачи - передачи пакетов IPv4 через части Интернета, работающие по протоколу IPv6. Этот тип адреса по-прежнему содержит в 4 младших байтах адрес IPv4, в старших 10 байтах - нули, а в 5-м и 6-м байтах адреса IPv6 - единицы, которые показывают, что узел поддерживает только 4-ю версию протокола IP. Существует специальный подтип unicast-адреса, предназначенный для отображения адресов IPX на адреса IPv6. Эти адреса отличаются 7 битным префиксом формата 0000 010, а остальные 121 бит отводятся под адрес IPX и, возможно, еще какую-то дополнительную информацию, точное назначение которой стандартом пока еще не определено. В 6-й версии протокола, так же, как и в 4-й, имеются адреса, предназначенные для локальною использования, то есть в сетях, не входящих в Интернег (не следует путать эти адреса с локальными адресами). В отличие от 4-й версии, в 6-й версии эти адреса имеют специальный формат. Адреса для локального использования представлены в IPv6 двумя разновидностями. Во-первых, это адреса для сетей, не разделенных на подсети (не использующих маршрутизацию). Они называются Linc-Local и имеют 10-битный префикс формата 1111 111010. Адрес Linc-Local содержит только 64-разрядное поле идентификатора интерфейса, а остальные разряды, кроме префикса формата, должны быть пулевыми, поскольку потребность в номере подсеги здесь отсутствует.

Вовторых. это адреса локального использования для сетей, разделенных на подсети. Такие адреса называют Site-Local, они имеют префикс формата 1111 1110 11 и содержат по сравнению с адресами Linc-Local дополнительное двухбайговое поле номера подсети. Адрес типа multicast - групповой адрес,

аналогичный по назначению групповому адресу IPv6. Он имеет префикс формата 1111 1111 и иденгифицируег группу интерфейсов, относящихся, как правило, к разным узлам. Пакет с таким адресом доставляется всем интерфейсам с этим адресом. Адреса типа multicast используется в IPv6 и для замены широковещательных адресов, для этого вводится особый адрес группы, объединяющей все интерфейсы подсети.

В версии IPv6 групповой адрес имеет признак обзора (scope), отсутствовавший в групповом адресе версии IPv4. Этот признак позволяет гибко задавагь областгь действия группового адреса, которая может представлять собой, например, только одну подсеть, либо все подсети данного предприятия, либо весь Интерпет. Это упрощает работу маршрутизаторов, которым необходимо выявлять все узлы, относящиеся к какой-либо группе. Еще один признак задаег тип группы - постоянная или временная.

Адрес типа anycast - это новый тип адреса, который так же, как и multicast, определяет группу интерфейсов. Но пакет с таким адресом доставляется одному из интерфейсов группы, как правило, «ближайшему» в соответствии с метрикой, используемой протоколами маршрутизации. Синтаксически anycast-адрес ничем не отличается от адреса типа unicast, он назначается из того же диапазона адресов, что и unicast-адреса. Адрес типа unicast может быть назначен только интерфейсам маршрутизатора. Интерфейсы маршрутизаторов, входящие в одну anycast-группу, имеют индивидуальные unicast-адреса и, кроме того, общий anycast-адрес. Адреса такого типа ориентированы па применение маршрутизации от источника (Source Routing) когда маршрут прохождения пакета определяется узлом-отправителем путем указания IP-адресов всех промежуточных маршрутизаторов. Например, провайдер может присвоить всем своим

маршрутизаторам один и тот же anycast-адрес и сообщить его абонентам. Если абонент желает, чтобы его пакеты передавались через сеть этого провайдера, то ему достаточно указать этот anycast-адрес в цепочке адресов маршрута от источника, и пакет будет передан через ближайший маршрутизатор этого провайдера.

Работа по детализации подтипов адресов IPv6 еще далека от завершения. Сегодня определено назначение только для 15% адресного пространства IPv6, а оставшаяся часть адресов еще ждет своей очереди, чтобы найти применение в какой-либо часто встречающейся в Интернете ситуации и упростить ее разрешение.

СПИСОК ЛИТЕРАТУРЫ:

1.Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн. UNIX: руководство системного администратора.

2.Р.Д. Мэтьюз, П. Джонс и др. Web-сервер под Unix.

3.TCP/IP Illustrated, volume I. The Protocols

4.TCP/IP. Учебное руководство для специалистов MCSE

5.Дрю Х. Внутренний мир TCP/IP

6.Д. Комер "Межсетевой обмен с помощью TCP/IP"

ИНТЕРНЕТ:

1.http://www.signal-com.ru/rus/articles/articles.html

2.http://antstar.narod.ru/library/tl/tcpip/3.html

3.http://www.yura-k.kiev.ua/net_bookshelf/index/idx_e.htm

4.http://info.star.spb.ru/Network/mv-manage/ch10.htm

5.http://www.cisco.com.ru/univercd/cc/td/doc/product/software/ios121/121cgcr/ibm_c/bcprt2/bcdclaw.htm