Занятие №22 «Адресация в IP сетях»

Значительная часть технологии TCP/IP направлена на решение следующих задач адресации:

□ *Задача согласованного использования адресов различного типа* включает отображение адресов разных типов, например, преобразование сетевого IP-адреса в локальный, доменного имени — в IP-адрес.

□ *Обеспечение уникальности адресов.* В зависимости от типа адреса требуется обеспечивать однозначность адресации в пределах компьютера, подсети, корпоративной сети или Интернета.

□ *Конфигурирование сетевых интерфейсов и сетевых приложений.*

Каждая из перечисленных задач имеет достаточно простое решение для сети, число узлов которой не превосходит нескольких десятков. Например, для отображения символьного доменного имени в IP-адрес достаточно поддерживать на каждом хосте таблицу всех символьных имен, используемых в сети, и соответствующих им IP-адресов. Так же просто «вручную» присвоить всем интерфейсам в небольшой сети уникальные адреса. Однако в крупных сетях эти же задачи усложняются настолько, что требуют принципиально других решений.

Ключевым словом, которое характеризует подход к решению этих проблем, принятый в TCP/IP является **масштабируемость.**

Процедуры, предлагаемые TCP/IP для назначения, отображения и конфигурирования адресов одинаково хорошо работают в сетях разного масштаба. В этой главе наряду с собственно схемой образования IP-адресов мы познакомимся с наиболее популярными масштабируемыми средствами поддержки адресации в сетях TCP/IP: технологией бесклассовой междоменной маршрутизации, системой доменных имен, протоколом динамического конфигурирования хостов.

1. Типы адресов стека TCP/IP

В целом, в сетях TCP/IP используются три типа адресов:

– локальный (аппаратный, физический) (MAC-адрес);

– сетевой (IP-адрес);

– символьный (DNS-имя).

• MAC-адрес - Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 11-A0-17-3D-BC-01. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизовано. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети. Преобразование адресов MAC⇔IP выполняет протокол ARP.

• IP-адрес, состоящий из 4 байт, например, 109.26.17.100. Этот адрес используется на сетевом уровне. Он назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Network Information Center, NIC), если сеть должна работать как составная часть Internet. Обычно провайдеры услуг Internet получают диапазоны адресов у подразделений NIC, а затем распределяют их между своими абонентами.

Номер узла в протоколе IP назначается независимо от локального адреса узла. Деление IP-адреса на поле номера сети и номера узла - гибкое, и граница между этими полями может устанавливаться весьма произвольно. Узел может входить в несколько IP-сетей. В этом случае

узел должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

• DNS-имя (Domain Name System) - символьный идентификатор-имя, например, SERV1.IBM.COM. Этот адрес назначается администратором и состоит из нескольких частей, например, имени машины, имени организации, имени домена. Адрес имеет вложенную многоуровневую древовидную структуру. Верхнему уровню соответствует последняя справа часть адреса. Как правило, верхний уровень отражает или географический регион (государство), например, RU - Россия, US - США, UA -Украина Такой адрес, называемый также DNS-именем , используется на прикладном уровне, например, в протоколах HTTP (WWW), FTP или telnet.

Между доменным именем и IP-адресом узла нет никакой функциональной зависимости, поэтому единственный способ установления соответствия — это таблица. В сетях TCP/IP используется специальная система доменных имен (Domain Name System, DNS), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS-именами.

Классы IP-адресов

Признаком, на основании которого IP-адрес относится к тому или иному классу, являются значения нескольких первых битов адреса. Таблица 1 иллюстрирует структуру IP-адресов разных классов.

Существуют 5 классов IP-адресов, отличающиеся количеством бит в сетевом номере и номере оконечной установки (узла). Класс адреса определяется значением его первого октета.

Адреса *класса A* предназначены для использования в больших сетях общего пользования. Они допускают большое количество номеров узлов. Адреса *класса B* используются в сетях среднего размера, например, сетях университетов и крупных компаний. Адреса *класса C* используются в сетях с небольшим числом компьютеров. Адреса *класса D* используются при обращениях к группам объектов адресования, а адреса класса E зарезервированы на будущее.

В Табл.1 приведено соответствие классов адресов значениям первого октета и указано количество возможных IP-адресов каждого класса.

Таблица 1.

Класс	Начальные биты адреса (признак класса)	Диапазон значений первого октета	Возможное количество сетей	Возможное количество узлов
A	0	1 - 126	126	16777214
B	10	128-191	16382	65534
C	110	192-223	2097150	254
D	1110	224-239	-	2^{28}
E	11110	240-247	-	2^{27}

Некоторые IP-адреса являются выделенными и трактуются по-особому. В выделенных IP-адресах все нули соответствуют либо данному узлу, либо данной IP-сети, а IP-адреса, состоящие из всех единиц, используются при широковещательных передачах. Для ссылок на всю IP-сеть в целом используется IP-адрес с нулевым номером узла. Особый смысл имеет IP-адрес, первый октет которого равен 127. Он используется для тестирования программ и взаимодействия процессов в пределах одной машины. Когда программа посылает данные по IP-адресу 127.0.0.1, то образуется как бы "петля". Данные не передаются по сети, а возвращаются модулям верхнего уровня, как только что принятые. Поэтому в IP-сети запрещается присваивать машинам IP-адреса, начинающиеся со 127.

2. Порядок назначения IP адресов

По определению схема IP-адресации должна обеспечивать уникальность нумерации сетей, а также уникальность нумерации узлов в пределах каждой из сетей. Следовательно, процедуры

назначения номеров как сетям, так и узлам сетей должны быть *централизованными.* Рекомендуемый порядок назначения IP-адресов дается в RFC 2050.

Назначение адресов автономной сети

Когда дело касается сети, являющейся частью Интернета, уникальность нумерации может быть обеспечена только усилиями специально созданных для этого центральных органов. В небольшой же автономной IP-сети условие уникальности номеров сетей и узлов может быть выполнено силами сетевого администратора.

В этом случае в распоряжении администратора имеются все адресное пространство, так как совпадение IP-адресов в не связанных между собой сетях не вызовет никаких отрицательных последствий. Администратор может выбирать адреса произвольным образом, соблюдая лишь синтаксические правила и учитывая ограничения на особые адреса. (Напомним, что номер узла в технологии TCP/IP назначается независимо от его локального адреса.)

Однако при таком подходе исключена возможность в будущем подсоединить данную сеть к Интернету. Действительно, произвольно выбранные адреса данной сети могут совпасть с централизовано назначенными адресами Интернета. Для того чтобы избежать коллизий, связанных с такого рода совпадениями, в стандартах Интернета определено несколько так называемых частных адресов, рекомендуемых для автономного использования:

в классе A — сеть 10.0.0.0;

в классе B — диапазон из 16 номеров сетей 172.16.0.0-172.31.0.0;

в классе C - диапазон из 255 сетей - 192.168.0.0-192.168.255.0.

Эти адреса, исключенные из множества централизованно распределяемых, составляют огромное адресное пространство, достаточное для нумерации узлов автономных сетей практически любых размеров. Заметим также, что частные адреса, как и при произвольном выборе адресов, в разных автономных сетях могут совпадать. В то же время использование частных адресов для адресации автономных сетей делает возможным корректное подключение их к Интернету. Применяемые при этом специальные технологии подключения[1] исключают коллизии адресов.

Централизованное распределение адресов

В больших сетях, подобных Интернету, уникальность сетевых адресов гарантируется централизованной, иерархически организованной системой их распределения. Номер сети может быть назначен только по рекомендации специального подразделения Интернета. Главным органом регистрации глобальных адресов в Интернете с 1998 года является неправительственная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers). Эта организация координирует работу региональных отделов, деятельность которых охватывает большие географические площади: ARIN — Америка, RIPE (Европа), APNIC (Азия и Тихоокеанский регион). Региональные отделы выделяют блоки адресов сетей крупным поставщикам услуг, а те, в свою очередь, распределяют их между своими клиентами, среди которых могут быть и более мелкие поставщики.

Проблемой централизованного распределения адресов является их дефицит. Уже сравнительно давно 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 адресное пространство используется нерационально. Очень часто владельцы сетей класса C расходуют лишь небольшую часть из имеющихся у них 254 адресов.

Для смягчения проблемы дефицита адресов разработчики стека TCP/IP предлагают разные подходы. Принципиальным решением является переход на новую версию протокола IP — протокол IPv6, в котором резко расширяется адресное пространство. Однако и текущая версия протокола IP (IPv4) поддерживает технологии, направленные на более экономное расходование IP-адресов, такие например, как NAT и CIDR.

3. Протоколы разрешения адресов

Для определения локального адреса по IP-адресу используется протокол разрешения адресов (Address Resolution Protocol, ARP). Протокол разрешения адресов реализуется различным образом в зависимости от того, работает ли в данной сети протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещания или же какой-либо из протоколов глобальной сети (X.25, Frame Relay), которые, как правило, не поддерживают широковещательный доступ.

Рассмотрим работу протокола ARP в локальных сетях с широковещанием.

На рис. 1 показан фрагмент IP-сети, включающий две сети — Ethernet 1 (из трех конечных узлов A, B и C) и Ethernet 2 (из двух конечных узлов D и E). Сети подключены соответственно к интерфейсам 1 и 2 маршрутизатора. Каждый сетевой интерфейс имеет IP-адрес и MAC-адрес. Пусть в какой-то момент IP-модуль узла C направляет пакет узлу D. Протокол IP узла C определил IP-адрес интерфейса следующего маршрутизатора — это IP1. Теперь, прежде чем упаковать пакет в кадр Ethernet и направить его маршрутизатору, необходимо определить соответствующий MAC-адрес. Для решения этой задачи протокол IP обращается к протоколу ARP. Протокол ARP поддерживает на каждом интерфейсе сетевого адаптера или маршрутизатора отдельную ARP-таблицу, в которой в ходе функционирования сети накапливается информация о соответствии между IP-адресами и MAC-адресами других интерфейсов данной сети. Первоначально, при включении компьютера или маршрутизатора в сеть все его ARP-таблицы пусты.

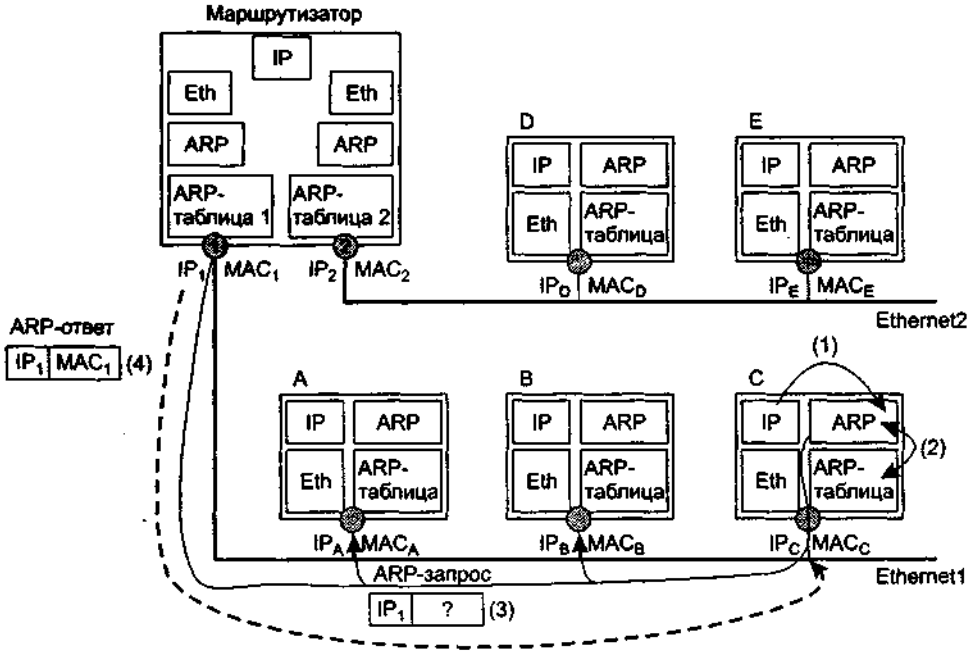

Рис. 1. Схема работы протокола ARP

На первом шаге происходит передача от протокола IP протоколу ARP примерно такого сообщения: «Какой MAC-адрес имеет интерфейс с адресом IP?»

Работа протокола ARP начинается с просмотра ARP-таблицы соответствующего интерфейса. Предположим, что среди содержащихся в ней записей отсутствует запрашиваемый IP-адрес.
В этом случае исходящий IP-пакет, для которого оказалось невозможным определить локальный адрес из ARP-таблицы, запоминается в буфере, а протокол ARP формирует ARP-запрос, вкладывает его в кадр протокола Ethernetи широковещательно рассылает.

Все интерфейсы сети Ethernet 1 получают ARP-запрос и направляют его «своему» протоколу ARP. ARP сравнивает указанный в запросе адрес IP с IP-адресом интерфейса, на который поступил этот запрос. Протокол ARP, который констатировал совпадение (в данном случае это ARP маршрутизатора 1) формирует ARP-ответ.

В ARP-ответе маршрутизатор указывает локальный адрес MACi своего интерфейса и отправляет его запрашивающему узлу (в данном примере узлу C), используя его локальный адрес.

Широковещательный ответ в этом случае не требуется, так как формат ARP-запроса предусматривает поля локального и сетевого адресов отправителя. Заметим, что зона распространения ARP-запросов ограничивается сетью Ethernet 1, так как на пути широковещательных кадров барьером стоит маршрутизатор.

Протокол Proxy-ARP – это одна из разновидностей протокола ARP, позволяющая отображать IP-адреса на аппаратные адреса в сетях, поддерживающих широковещание, даже в тех случаях, когда искомый узел находится за пределами данного домена коллизий.

На рис. 2 показана сеть, один из конечных узлов которой (компьютер D) работает в режиме удаленного узла. Подробнее об этом режиме вы прочитаете в главе 23 части V, а сейчас достаточно знать, что конечный узел в таком режиме обладает всеми возможностями компьютеров, работающих в основной части сети Ethernet, в частности, он имеет IP-адрес (IP_D), относящийся к той же сети. Для всех конечных узлов сети Ethernet особенности подключения удаленного узла (наличие модемов, коммутируемая связь, протокол PPP) абсолютно прозрачны – они взаимодействуют с ним обычным образом. Чтобы такой режим взаимодействия стал возможным, среди прочего, необходим протокол Proxy-ARP. Поскольку удаленный узел подключен к сети по протоколу PPP, то он, очевидно, не имеет MAC-адреса.

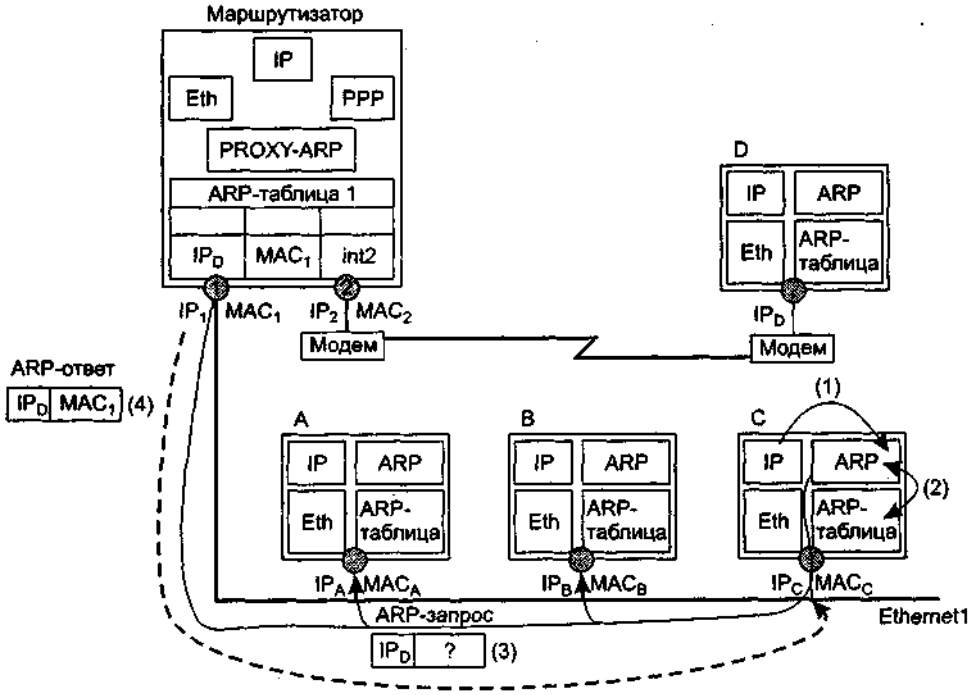

Рис. 2. Схема работы протокола Proxy-ARP

Пусть приложение, работающее, например, на компьютере C, решает послать пакет компьютеру D. Ему известен IP-адрес узла назначения (IP_D). однако как мы уже не раз отмечали, для передачи пакета по сети Ethernet его необходимо упаковать в кадр Ethernet и снабдить MAC-адресом. Для определения MAC-адреса IP-протокол узла C обращается к протоколу ARP, который посылает широковещательное сообщение с ARP-запросом. Если бы в этой сети на маршрутизаторе не был установлен протокол Proxy-ARP, на этот запрос не откликнулся бы ни один узел.

Однако протокол Proxy-ARP установлен на маршрутизаторе и работает следующим образом. При подключении к сети удаленного узла D в таблицу ARP-маршрутизатора заносится запись

$$IP_D – MAC_1 - int2,$$

которая означает, что:

при поступлении ARP-запроса на маршрутизатор относительно адреса IPDв ARP-ответ будет помещен аппаратный адрес MAC_1 соответствующий аппаратному адресу интерфейса 1 маршрутизатора;

узел, имеющий адрес IPD, подключен к интерфейсу 2 маршрутизатора.

В ответ на посланный узлом C широковещательный ARP-запрос откликается маршрутизатор с установленным протоколом Proxy-ARP. Он посылает «ложный» ARP-ответ, в котором на место аппаратного адреса компьютера D помещает собственный адрес MAC_1. Узел C, не подозревая «подвоха», посылает кадр с IP-пакетом по адресу MAC_1. Получив кадр, маршрутизатор с установленным протоколом Proxy-ARP «понимает», что он направлен не ему (в пакете указан чужой IP-адрес) и, следовательно, надо искать адресата в ARP-таблице. Из таблицы видно, что кадр надо направить узлу, подключенному ко второму интерфейсу.

Мы рассмотрели простейшую схему применения протокола Proxy-ARP, которая тем не менее достаточно полно отражает логику его работы.