**46. Протокол IP (версия 4). IP-адреса. Классы. Маски. Понятие об IP–сети. Работа протокола IP. Маршрутизация IP.**

**1. Функции протокола IP**

Протокол IP находится на межсетевом уровне стека протоколов TCP/IP. Функции протокола IP определены в стандарте RFC-791 следующим образом: “Протокол IP обеспечивает передачу блоков данных, называемых дейтаграммами, от отправителя к получателям, где отправители и получатели являются компьютерами, идентифицируемыми адресами фиксированной длины (*IP-адресами*). Протокол IP обеспечивает при необходимости также фрагментацию и сборку дейтаграмм для передачи данных через сети с малым размером пакетов”.

Протокол IP является *ненадежным* протоколом *без установления соединения*. Это означает, что протокол IP не подтверждает доставку данных, не контролирует целостность полученных данных и не производит операцию квитирования (handshaking) - обмена служебными сообщениями, подтверждающими установку соединения с узлом назначения и его готовность к приему данных. Протокол IP обрабатывает каждую дейтаграмму как независимую единицу, не имеющую связи ни с какими другими дейтаграммами в Интернет. После того, как дейтаграмма отправляется в сеть, ее дальнейшая судьба никак не контролируется отправителем (на уровне протокола IP). Если дейтаграмма не может быть доставлена, она уничтожается. Узел, уничтоживший дейтаграмму, может оправить по обратному адресу *ICMP-сообщение* о причине сбоя.

Гарантию правильной передачи данных предоставляют протоколы вышестоящего уровня (например, протокол TCP), которые имеют для этого необходимые механизмы.

Одна из основных задач, решаемых протоколом IP, - маршрутизация дейтаграмм, т.е. определение пути следования дейтаграммы от одного узла сети к другому на основании адреса получателя.

Общий сценарий работы модуля IP на каком-либо узле сети, принимающего дейтаграмму из сети, таков:

* с одного из интерфейсов уровня доступа к среде передачи (например, с Ethernet-интерфейса) в модуль IP поступает дейтаграмма;
* модуль IP анализирует заголовок дейтаграммы;
* если пунктом назначения дейтаграммы является данный компьютер:
  + если дейтаграмма является фрагментом большей дейтаграммы, ожидаются остальные фрагменты, после чего из них собирается исходная большая дейтаграмма;
  + из дейтаграммы извлекаются данные и направляются на обработку одному из протоколов вышележащего уровня (какому именно - указывается в заголовке дейтаграммы);
* если дейтаграмма не направлена ни на один из IP-адресов данного узла, то дальнейшие действия зависят от того, разрешена или запрещена ретрансляция (forwarding) “чужих” дейтаграмм;
* если ретрансляция разрешена, то определяются следующий узел сети, на который должна быть переправлена дейтаграмма для доставки ее по назначению, и интерфейс нижнего уровня, после чего дейтаграмма передается на нижний уровень этому интерфейсу для отправки; при необходимости может быть произведена фрагментация дейтаграммы;
* если же дейтаграмма ошибочна или по каким-либо причинам не может быть доставлена, она уничтожается; при этом, как правило, отправителю дейтаграммы отсылается ICMP-сообщение об ошибке.

При получении данных от вышестоящего уровня для отправки их по сети IP-модуль формирует дейтаграмму с этими данными, в заголовок которой заносятся адреса отправителя и получателя (также полученные от транспортного уровня) и другая информация; после чего выполняются следующие шаги:

* если дейтаграмма предназначена этому же узлу, из нее извлекаются данные и направляются на обработку одному из протоколов транспортного уровня (какому именно - указывается в заголовке дейтаграммы);
* если дейтаграмма не направлена ни на один из IP-адресов данного узла, то определяются следующий узел сети, на который должна быть переправлена дейтаграмма для доставки ее по назначению, и интерфейс нижнего уровня, после чего дейтаграмма передается на нижний уровень этому интерфейсу для отправки; при необходимости может быть произведена фрагментация дейтаграммы;
* если же дейтаграмма ошибочна или по каким-либо причинам не может быть доставлена, она уничтожается.

Здесь и далее ***узлом сети*** называется компьютер, подключенный к сети и поддерживающий протокол IP. Узел сети может иметь один и более *IP-интерфейсов*, подключенных к одной или разным сетям, каждый такой интерфейс идентифицируется уникальным *IP-адресом*.

***IP-сетью*** называется множество компьютеров (IP-интерфейсов), часто, но не всегда подсоединенных к одному физическому каналу связи, способных пересылать IP-дейтаграммы друг другу непосредственно (то есть без ретрансляции через промежуточные компьютеры), при этом IP-адреса интерфейсов одной IP-сети имеют общую часть, которая называется адресом, или номером, IP-сети, и специфическую для каждого интерфейса часть, называемую адресом, или номером, данного интерфейса в данной IP-сети.

***Маршрутизатором***, или ***шлюзом***, называется узел сети с несколькими IP-интерфейсами, подключенными к разным IP-сетям, осуществляющий на основе решения задачи маршрутизации перенаправление дейтаграмм из одной сети в другую для доставки от отправителя к получателю.

***Хостами*** называются узлы IP-сети, не являющиеся маршрутизаторами. Обычно хост имеет один IP-интерфейс (например, связанный с сетевой картой Ethernet или с модемом), хотя может иметь и несколько.

Маршрутизаторы представляют собой либо специализированные вычислительные машины, либо компьютеры с несколькими IP-интерфейсами, работа которых управляется специальным программным обеспечением. Компьютеры конечных пользователей, различные серверы Интернет и т.п. вне зависимости от своей вычислительной мощности являются хостами.

Неотъемлемой частью IP-модуля является протокол ICMP (Internet Control Message Protocol), отправляющий диагностические сообщения при невозможности доставки дейтаграммы и в других случаях. Совместно с протоколом IP работает также протокол ARP (Address Resolution Protocol), выполняющий преобразования IP-адресов в MAC-адреса (например, адреса Ethernet).

**2. IP-адреса**

IP-адрес является уникальным 32-битным идентификатором IP-интерфейса в Интернет. Часто говорят, что IP-адрес присваивается узлу сети (например, хосту); это верно в случае, если узел является хостом с одним IP-интерфейсом, иначе следует уточнить, об адресе какого именно интерфейса данного узла идет речь. Далее для краткости там, где это не вызовет неверного толкования, вместо *адреса IP-интерфейса узла сети* говорится об *IP-адресе хоста*.

IP-адреса принято записывать разбивкой всего адреса по октетам, каждый октет записывается в виде десятичного числа, числа разделяются точками. Например, адрес

10100000010100010000010110000011

записывается как

10100000.01010001.00000101.10000011 = 160.81.5.131.

IP-адрес хоста состоит из номера IP-сети, который занимает старшую область адреса, и номера хоста в этой сети, который занимает младшую часть. Положение границы сетевой и хостовой частей (обычно оно характеризуется количеством бит, отведенных на номер сети) может быть различным, определяя различные типы IP-адресов, которые рассматриваются ниже.

**2.1. Классовая модель**

В классовой модели IP-адрес может принадлежать к одному из четырех классов сетей. Каждый класс характеризуется определенным размером сетевой части адреса, кратным восьми; таким образом, граница между сетевой и хостовой частями IP-адреса в классовой модели всегда проходит по границе октета. Принадлежность к тому или иному классу определяется по старшим битам адреса.

*Класс А*. Старший бит адреса равен нулю. Размер сетевой части равен 8 битам. Таким образом, может существовать всего примерно 27 сетей класса А, но каждая сеть обладает адресным пространством на 224 хостов. Так как старший бит адреса нулевой, то все IP-адреса этого класса имеют значение старшего октета в диапазоне 0 — 127, который является также и номером сети.

*Класс В*. Два старших бита адреса равны 10. Размер сетевой части равен 16 битам. Таким образом, может существовать всего примерно 214 сетей класса В, каждая сеть обладает адресным пространством на 216 хостов. Значения старшего октета IP-адреса лежат в диапазоне 128 — 191, при этом номером сети являются два старших октета.

*Класс С*. Три старших бита адреса равны 110. Размер сетевой части равен 24 битам. Количество сетей класса С примерно 221, адресное пространство каждой сети рассчитано на 254 хоста. Значения старшего октета IP-адреса лежат в диапазоне 192 - 223, а номером сети являются три старших октета.

*Класс D*. Сети со значениями старшего октета IP-адреса 224 и выше. Зарезервированы для специальных целей. Некоторые адреса используются для мультикастинга - передачи дейтаграмм группе узлов сети, например:

224.0.0.1 - всем хостам данной сети;

224.0.0.2 - всем маршрутизаторам данной сети;

224.0.0.5 - всем OSPF-маршрутизаторам;

224.0.0.6 - всем выделенным (designated) OSPF-маршрутизаторам;

В классе А выделены две особые сети, их номера 0 и 127. Сеть 0 используется при маршрутизации как указание на маршрут по умолчанию и в других особых случаях.

IP-интерфейс с адресом в сети 127 используется для адресации узлом себя самого (*loopback, интерфейс обратной связи*). Интерфейс обратной связи не обязательно имеет адрес в сети 127 (особенно у маршрутизаторов), но если узел имеет IP-интерфейс с адресом 127.0.0.1, то это - интерфейс обратной связи. Обращение по адресу loopback-интерфейса означает связь с самим собой (без выхода пакетов данных на уровень доступа к среде передачи); для протоколов на уровнях транспортном и выше такое соединение неотличимо от соединения с удаленным узлом, что удобно использовать, например, для тестирования сетевого программного обеспечения.

В любой сети (это справедливо и для бесклассовой модели, которую мы рассмотрим ниже) все нули в номере хоста обозначают саму сеть, все единицы - адрес широковещательной передачи (broadcast).

Например, 194.124.84.0 - сеть класса С, номер хоста в ней определяется последним октетом. При отправлении широковещательного сообщения оно отправляется по адресу 194.84.124.255. Номера, разрешенные для присваивания хостам: от 1 до 254 (194.84.124.1 — 194.84.124.254), всего 254 возможных адреса.

Другой пример: в сети 135.198.0.0 (класс В, номер хоста занимает два октета) широковещательный адрес 135.198.255.255, диапазон номеров хостов: 0.1 — 255.254 (135.198.0.1 — 135.198.255.254).

**2.2. Бесклассовая модель (CIDR)**

Предположим, в локальной сети, подключаемой к Интернет, находится 2000 компьютеров. Каждому из них требуется выдать IP-адрес. Для получения необходимого адресного пространства нужны либо 8 сетей класса C, либо одна сеть класса В. Сеть класса В вмещает 65534 адреса, что много больше требуемого количества. При общем дефиците IP-адресов такое использование сетей класса В расточительно. Однако если мы будем использовать 8 сетей класса С, возникнет следующая проблема: каждая такая IP-сеть должна быть представлена отдельной строкой в таблицах маршрутов на маршрутизаторах, потому что с точки зрения маршрутизаторов — это 8 абсолютно никак не связанных между собой сетей, маршрутизация дейтаграмм в которые осуществляется независимо, хотя фактически эти IP-сети и расположены в одной физической локальной сети и маршруты к ним идентичны. Таким образом, экономя адресное пространство, мы многократно увеличиваем служебный трафик в сети и затраты по поддержанию и обработке маршрутных таблиц.

С другой стороны, нет никаких формальных причин проводить границу сеть-хост в IP-адресе именно по границе октета. Это было сделано исключительно для удобства представления IP-адресов и разбиения их на классы. Если выбрать длину сетевой части в 21 бит, а на номер хоста отвести, соответственно, 11 бит, мы получим сеть, адресное пространство которой содержит 2046 IP-адресов, что максимально точно соответствует поставленному требованию. Это будет *одна* сеть, определяемая своим уникальным 21-битным номером, следовательно, для ее обслуживания потребуется только *одна* запись в таблице маршрутов.

Единственная проблема, которую осталось решить: как определить, что на сетевую часть отведен 21 бит? В случае классовой модели старшие биты IP-адреса определяли принадлежность этого адреса к тому или иному классу и, следовательно, количество бит, отведенных на номер сети.

В случае адресации вне классов, с произвольным положением границы сеть-хост внутри IP-адреса, к IP-адресу прилагается 32-битовая маска, которую называют *маской сети* (netmask) или *маской подсети* (subnet mask). Сетевая маска конструируется по следующему правилу:

* на позициях, соответствующих номеру сети, биты установлены;
* на позициях, соответствующих номеру хоста, биты сброшены.

Описанная выше модель адресации называется бесклассовой (CIDR - Classless Internet Direct Routing, прямая бесклассовая маршрутизация в Интернет). В настоящее время классовая модель считается устаревшей и маршрутизация и (большей частью) выдача блоков IP-адресов осуществляются по модели CIDR, хотя классы сетей еще прочно удерживаются в терминологии.

**2.3. Запись адресов в бесклассовой модели**

Для удобства записи IP-адрес в модели CIDR часто представляется в виде a.b.c.d / n, где a.b.c.d — IP адрес, n — количество бит в сетевой части.

Пример: 137.158.128.0/17.

Маска сети для этого адреса: 17 единиц (сетевая часть), за ними 15 нулей (хостовая часть), что в октетном представлении равно

11111111.11111111.10000000.00000000 = 255.255.128.0.

Представив IP-адрес в двоичном виде и побитно умножив его на маску сети, мы получим номер сети (все нули в хостовой части). Номер хоста в этой сети мы можем получить, побитно умножив IP-адрес на инвертированную маску сети.

Пример: IP = 205.37.193.134/26 или, что то же,

IP = 205.37.193.134 netmask = 255.255.255.192.

Распишем в двоичном виде:

IP = 11001101 00100101 11000111 10000110

маска = 11111111 11111111 11111111 11000000

Умножив побитно, получаем номер сети (в хостовой части - нули):

network = 11001101 00100101 11000111 10*000000*

или, в октетном представлении, 205.37.193.128/26, или, что то же, 205.37.193.128 netmask 255.255.255.192.

Хостовая часть рассматриваемого IP адреса равна 000110, или 6. Таким образом, 205.37.193.134/26 адресует хост номер 6 в сети 205.37.193.128/26. В классовой модели адрес 205.37.193.134 определял бы хост 134 в сети класса С 205.37.193.0, однако указание маски сети (или количества бит в сетевой части) однозначно определяет принадлежность адреса к бесклассовой модели.

*Упражнение.* Покажите, что адрес 132.90.132.5 netmask 255.255.240.0 определяет хост 4.5 в сети 132.90.128.0/20 (в классовой модели это был бы хост 132.5 в сети класса В 132.90.0.0). Найдите адрес broadcast для этой сети.

Очевидно, что сети классов А, В, С в бесклассовой модели представляются при помощи масок, соответственно, 255.0.0.0 (или /8), 255.255.0.0 (или /16) и 255.255.255.0 (или /24).

**3. Маршрутизация**

Процесс маршрутизации дейтаграмм состоит в определении следующего узла (*next hop*) в пути следования дейтаграммы и пересылки дейтаграммы этому узлу, который является либо узлом назначения, либо промежуточным маршрутизатором, задача которого — определить следующий узел и переслать ему дейтаграмму. Ни узел-отправитель, ни любой промежуточный маршрутизатор не имеют информации о всей цепочке, по которой пересылается дейтаграмма; каждый маршрутизатор, а также узел-отправитель, основываясь на адресе назначения дейтаграммы, находит только следующий узел ее маршрута.

Маршрутизация дейтаграмм осуществляется на уровне протокола IP.

Маршрутизация выполняется на основе данных, содержащихся в таблице маршрутов. Строка в таблице маршрутов состоит из следующих полей:

* адрес сети назначения;
* адрес *следующего* *маршрутизатора* (то есть узла, который знает, куда дальше отправить дейтаграмму, адресованную в сеть назначения);
* вспомогательные поля.

Таблица может составляться вручную или с помощью специализированных протоколов. Каждый узел сети, в том числе и хост, имеет таблицу маршрутов, хотя бы самую простую.