**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Гжельский государственный университет»** (ГГУ)

Колледж ГГУ

Специальность 09.02.07. Информационные системы и программирование.

**Реферат**

**по предмету «КС»**

**на тему** **«**Технологии глобальных сетей. Преобразование форматов IP-адресов. Расчет IP-адреса и маски подсети**»**

ВЫПОЛНИЛ:

Студент группы ИСП-О-17

Белкин И.В.

ПРОВЕРИЛА:

Прокуронова А. Ю.

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

п. Электроизолятор

2019 г.

**1. ОСОБЕННОСТИ IP –** **СЕТЕЙ**

В настоящее время в телекоммуникационных сетях применяются различные технологии передачи данных и разные алгоритмы управления и организации работы. Естественно, требуются специальные средства, позволяющие обеспечить корректное и эффективное взаимодействие этих разнородных телекоммуникационных технологий. Конечно, такие средства существуют, благодаря этим средствам стало реальным такое понятие как Internet. Если подходить строго с точки зрения телекоммуникационных технологий, понятие Internet является таким же виртуальным, как и многое другое. В мире существует достаточно много независимых друг от друга информационных сетей с различными технологиями передачи данных. Создать общее информационное пространство, т.е. Internet, позволяют именно эти средства организации взаимодействия, имеющие общее название IP – сети. Основой IP – сетей является стек коммуникационных протоколов TCP/IP.

IP- сети – это сети взаимосвязанных подсетей, основное назначение этой технологии – обеспечить взаимодействие автономных систем, которые соединены маршрутизаторами, называемыми граничными шлюзами. Автономные системы – самостоятельные сети, находящиеся под независимым управлением и использующие самостоятельные внутренние алгоритмы работы. В настоящее время автономные системы часто представляют собой тоже IP – сети. В принятой терминологии пакет данных при передаче от одного хоста (конечного узла) до другого хоста может пройти несколько автономных систем. Таким образом, основное назначение IP – сети заключается в организации межсетевого взаимодействия, основными элементами сети являются автономные системы (подсети), основная задача – передача данных между автономными системами через шлюзы, при условии, что маршруты доставки сообщений заранее неизвестны, и возможных маршрутов может быть несколько.

Стек TCP/IP основан на протоколе сетевого уровня IP, протоколе негарантированной доставки пакетов без установления соединения. В протоколе IP пакеты называют IP-дейтаграммами, для передачи используется дейтаграммный способ: все дейтаграммы передаются и обрабатываются сетью абсолютно независимо, нет никакой связи между отдельными дейтаграммами, нет ни механизмов контроля и восстановления потерянных дейтаграмм, ни гарантий доставки дейтаграмм. Если хост-отправитель передает дейтаграммы в определенной последовательности, сеть может доставлять их в хост-получатель в произвольном порядке. Каждая дейтаграмма проходит маршрутизацию независимо, не исключается возможность более ранней доставки дейтаграмм отправленных позже, потери или дублирования дейтаграмм.

Задача контроля целостности сообщений полностью возлагается на транспортный уровень, представленный протоколами TCP и UDP. Если задачами сетевого уровня являются задачи управления взаимодействием узлов сети при обмене данными, то транспортный уровень обеспечивает взаимодействие прикладных процессов в двух узлах сети. Взаимодействующие прикладные процессы идентифицируются протокольными портами (16 бит), порты 1-255 закреплены стандартами за широко известными приложениями, остальные порты могут назначаться произвольно. Управление на транспортном уровне требует номера порта (идентификатор прикладного процесса) и IP-адреса (идентификатор хоста), эта комбинация идентификаторов на транспортном уровне называется сокетом. Через сокет производится управление потоком данных между взаимодействующими процессами.

Транспортный протокол UDP выполняет негарантированную доставку данных без соединения между процессами передающего и принимающего хоста. Сообщения помещаются протоколом в поле данных одной или нескольких дейтаграмм с определенным идентификатором сокета, на принимающей стороне производится восстановление сообщения из принятых дейтаграмм. Если сообщение или его компоненты не доставлены, никаких механизмов восстановления не предусматривается. Этот протокол часто используется для передачи различных служебных сообщений, например, сообщений протоколов маршрутизации.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Приложения | FTP | SMTP | HTTP | RTR | DNS | … |
| Транспортный уровень | TCP | | | | | | UDP |
| Сетевой уровень | IP | | | | | | |
| Канальный уровень | PPP | | | | | | |
| Физический уровень | X.21 | | | | | | |

*Рис.1. Архитектура стека TCP* */* *IP*

Транспортный протокол TCP обеспечивает гарантированный поток данных между процессами, установившими виртуальное соединение. Идентифицируется соединение между процессами номером сокета. Поток данных сегментируется и передается также в виде дейтаграмм. Алгоритм подтверждения нумерует байты потока данных, передающая сторона ожидает подтверждения каждого сегмента. Если в течение определенного интервала времени подтверждение не поступило, передача сегмента повторяется. Уведомление о нормальном завершении процесса передачи отправляется только после успешной сборки сообщения приемником. Соединение в рамках TCP представляет собой набор параметров, определяющих процедуры обмена данными между процессами. Часть параметров должны быть неизменными, а некоторые параметры могут изменяться, адаптируя параметры процедур к текущему состоянию сети.

Особенностью алгоритма скользящего окна в TCP в том, что размер окна задается количеством байт, хотя единицей передаваемых данных является сегмент, размеры которого определяются при установлении соединения. Размер окна и время ожидания квитанций перед повторной отправкой сегментов являются адаптивно изменяемыми параметрами в процессе работы. Уменьшение окна и увеличение времени тайм-аута снижает скорость передачи данных.

Тайм-аут уточняется в процессе работы усреднением времени "двойного оборота" и умножением полученной величины на коэффициент >2. Размер окна при установлении соединения заявляется большим, а в процессе работы, как правило, уменьшается. Если принимающая сторона не справляется с потоком данных, она передает в квитанции нулевой размер окна. Передающая сторона при нулевом размере окна может время от времени продолжать попытки передачи данных, если состояние приемника изменилось, он передаст в квитанции ненулевой размер окна. Кроме того, имеется возможность передачи сообщений со специальным признаком, это сообщение будет обработано при перегрузке приемника даже за счет удаления из буфера принятых ранее сегментов. TCP, работая над потенциально ненадежным сетевым протоколом IP, выполняет необходимые процедуры контроля и обеспечивает восстановление потока данных при потере дейтаграмм.

Так как основная задача протокола IP – организация межсетевого взаимодействия, стек должен быть дополнен протоколами сетевых интерфейсов, которые обеспечивают преобразование дейтаграмм в пакеты или кадры других сетевых технологий. Это протоколы RFC1042 (IP – IEEE802), RFC1577 (IP – ATM) и другие. Стек коммуникационных протоколов TCP/IP содержит протоколы маршрутизации RIP, OSPF, протоколы передачи служебных управляющих сообщений ICMP, протоколы преобразования сетевых адресов автономных систем в IP-адреса ARP, RARP, протокол поддержки символьных доменных имен DNS и многие другие протоколы, состав протоколов постоянно расширяется. Тем не менее, в основе всех этих протоколов находятся процедуры передачи данных IP-протокола.

**2. СТРУКТУРА IP** **-ДЕЙТАГРАММ (ПАКЕТА)**

Каждая дейтаграмма обрабатывается IP-сетью как независимая единица. Если в процессе передачи возникли какие-либо ошибки, дейтаграмма просто отбрасывается, никаких средств повторной передачи, восстановления или просто уведомления об этом событии не предусмотрено. Как указывалось, задача контроля потока данных возлагается на транспортный уровень. Так как каждая дейтаграмма доставляется самостоятельно, она должна в служебных полях содержать все данные, необходимые для решения этой задачи. Поэтому независимо от характера передаваемых данных структура дейтаграмм одинакова. Дейтаграммы могут использоваться для решения различных задач, разными протоколами стека TCP/IP и характер задач не влияет на структуру дейтаграмм. Сложность служебных полей тесно связана со сложностью задач, которые решаются при продвижении дейтаграмм.

IP-дейтаграмма состоит из заголовка и поля данных. Стандартная длина заголовка со всеми необходимыми служебными полями – 20 байт, при необходимости длина может быть увеличена в поле Опции. Длина заголовка указывается количеством 4-х байтовых слов.

Номер версии протокола, используемой в настоящее время 4, хотя и существует версия 6. В поле длина заголовка указывается длина заголовка в 4-х байтовых словах, если длина заголовка не кратна 32 битам, заголовок дополняется нулями.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 бита  Номер  версии | 4 бита  Длина  заголовка | 8 бит  Тип сервиса | | | | | 16 бит Общая длина пакета | | | |
| PR | D | T | R | - |
| 16 бит Идентификатор пакета | | | | | | | 3 бита Флаги | | | 13 бит Смещение фрагмента |
| - | DF | MF |
| 8 бит Время жизни | | | 8 бит ротокол верхнего уровня | | | | 16 бит  Контрольное поле заголовка | | | |
| 32 бита  IP-адрес источника | | | | | | | | | | |
| 32 бита IP-адрес назначения | | | | | | | | | | |
| Опции и выравнивание | | | | | | | | | | |

*Рис. 2. Структура IP – дейтаграммы*

Поле «тип сервиса» задает приоритет и критерии выбора маршрута. PR имеет длину 3 бита и может определять приоритет от 0 (обычная дейтаграмма) до 7 (высокоприоритетная управляющая информация). Критерии выбора маршрута: D – минимальная задержка, T – максимальная пропускная способность, R – максимальная надежность. Обычно требования этих критериев противоречивы, поэтому нецелесообразно задавать выбор маршрута по двум критериям одновременно.

Поле Общая длина пакета указывает размер дейтаграммы в байтах, включая заголовок и поле данных. Дейтаграммы (пакеты) большого размера применяются редко только по согласования с протоколами автономных систем (подсетей), стандартная рекомендуемая длина – 576 байт.

Протокол IP предусматривает возможность фрагментации пакетов (дейтаграмм). Различные подсети могут определять разные размеры пакетов, при передаче из одной автономной системы в другую пакет может быть разделен на несколько пакетов, все фрагменты должны иметь одинаковое значение идентификатора пакета. Поле Флаги также связано с фрагментацией пакетов. Флаг DF запрещает фрагментацию данного пакета, MF говорит о том, что данный пакет является промежуточным фрагментом. Поле Смещение фрагмента и задает смещение в байтах поля данных фрагмента от начала общего поля данных исходного пакета.

Поле Время жизни задает предельный срок, в течение которого пакет может перемещаться по сети. Хотя считается, что время жизни задается в секундах, реально при перемещении от узла к узлу значение этого поля уменьшается на единицу. Если пакет не достиг узла назначения, а время жизни стало нулевым, этот пакет уничтожается. Этот механизм самоликвидации необходим для предотвращения бесконечно долгого блуждания пакетов по сети, задавая значение этого поля ограничивают количество промежуточных узлов, через которые пакет может достигнуть пункта назначения.

Идентификатор протокола верхнего уровня указывает, какому протоколу принадлежит информация в поле данных дейтаграммы. Значения идентификаторов приводятся в специальном стандарте.

Контрольное поле заголовка вычисляется как сумма по модулю 216 всех 16 битовых слов заголовка. Так как отдельные элементы заголовка могут изменяться в каждом узле, контрольная сумма проверяется при приеме дейтаграммы и формируется заново при передаче. Если при приеме обнаружены ошибки в заголовке с помощью контрольной суммы, дейтаграмма удаляется.

Поля IP-адресов имеют одинаковую структуру и длину 4 байта. В отличие от техники виртуальных каналов, в каждой дейтаграмме должны указываться полные IP-адреса. Поле Опции и выравнивание не является обязательным и используется при необходимости. Размер этого поля должен быть таким, чтобы граница заголовка всегда проходила по 32-битной границе.

**3. АДРЕСАЦИЯ В IP** **– СЕТЯХ**

В IP-сети используются три типа адресов: локальные, IP-адреса и символьные доменные имена. Локальный адрес – это адрес, используемый автономной системой (подсетью составной сети). Предполагается, что каждая автономная система может строиться по своей сетевой технологии, может иметь независимую систему адресации и использовать свои внутренние адреса. Если автономная система также является IP-сетью, локальный (внутренний) IP-адрес чаще всего не совпадает с внешним IP-адресом. Узел сети может не иметь локального адреса, а может иметь несколько различных локальных адресов. Существуют специальные процедуры, определяющие соответствие локальных (внутренних) адресов и IP-адресов, которые необходимы для передачи данных по составной сети.

Символьные доменные имена используются различными приложениями и пользователями. Для пользователей применение для адресации IP-адресов, представляющих достаточно громоздкие комбинации чисел, неудобно. Поэтому большинство приложений оперирует символьными именами вместо IP-адресов. Эти символьные имена строятся по иерархическому принципу. Отдельные элементы символьного доменного имени разделяются точками и по старшинству (подчиненности) располагаются справа налево. Крайний правый элемент имени определяет старший домен (.ru), следующий элемент за точкой его подчиненный домен (поддомен), например mydomain.ru. Второй домен может содержать свои поддомены (mysite.mydomain.ru) и т.д. Между символьным именем и IP-адресом какого либо алгоритмического соответствия нет, поэтому необходимо просто хранить таблицы соответствия. Для преобразования символьных имен в IP-адреса существует специальный протокол и специальная распределенная сетевая служба DNS. Таким образом, используя символьное доменное имя, мы обращаемся к DNS-серверу, который определяет соответствующий ему IP-адрес.

Основным адресом, обеспечивающим передачу данных, является IP-адрес. Этот адрес содержит 4 байта (в версии 6 протокола – 16 байт) и состоит из двух частей: номера сети (старшая часть адреса) и номера узла. В пределах подсети все узлы имеют один и тот же номер сети. В общем случае номер узла тоже может быть структурирован, элементами подсети также могут быть подсети следующего уровня иерархии. Глобальные IP-адреса не могут назначаться произвольно, правилами формирования этих адресов и их распределением занимается специальная служба InterNIC. Как уже отмечалось, структура и значение элементов адреса соответствует структуре сети, поэтому глобальные и локальные адреса назначаются независимо друг от друга. Маршрутизаторы, являясь элементами нескольких сетей, имеют отдельные адреса каждого порта. Хост может входить в состав нескольких сетей и иметь несколько адресов, поэтому принято считать, что IP-адрес характеризует не отдельное устройство, а одно сетевое соединение. Структура IP-адреса была основана на разделении сети по классам:

класс А 1.X.X.X. – 126.X.X.X.

|  |  |  |
| --- | --- | --- |
| байт1 | | байты 2, 3, 4 |
| 0 | № сети | № узла |

класс B128.0.X.X – 191.255.X.X

|  |  |  |
| --- | --- | --- |
| байты 1, 2 | | байты 3, 4 |
| 1 0 | № сети | № узла |

класс C192.0.1.Х – 223.255.255.Х

|  |  |  |
| --- | --- | --- |
| байты 1, 2, 3 | | байт 4 |
| 1 1 0 | № сети | № узла |

класс D 224.0.0.0 – 239.255.255.255

|  |  |
| --- | --- |
| байты 1, 2, 3, 4 | |
| 1 1 1 0 | адрес multicast |

Для использования в качестве локальных IP-адресов выделены специальные адреса: класса А 10.Х.Х.Х, класса B 172.16.X.X – 172.31.X.X, класса С 192.168.X.X – 192.168.X.X.

В протоколе определены особые адреса:

· если в поле номера сети только нули, то считается, что узел назначения принадлежит той же сети, что отправитель;

· если адрес содержит только единицы во всех двоичных разрядах, дейтаграмма рассылается всем узлам, находящимся в той же сети, что отправитель;

· если в поле номера узла содержатся только единицы, дейтаграмма направляется всем узлам сети с указанным номером;

· дейтаграмма с адресом 127 в первом байте используется для самотестирования узла, она не передается по сети, а возвращается к модулю верхнего уровня, как только что принятая.

Класс D используется специальным протоколом для групповой рассылки, дейтаграммы будут направлены всем узлам, зарегистрированным в этой группе.

К сожалению, разделение адресов на классы позволило создать недостаточно гибкую систему адресации. Граница между адресом сети и адресом узла находится на границе байтов. При использовании такой адресации довольно быстро проявился дефицит IP-адресов, рассматривались две возможности решения проблемы дефицита адресов: увеличение адресного поля до 16 байт (версия 6 протокола), или более эффективное использование адресного пространства.

Предложенные алгоритмы более гибкого использования адресного пространства позволили в рамках существующего формата адреса в значительной мере решить эту проблему. Вместо деления сетей на классы в настоящее время используются маски адреса. Маски позволяют установить границы элементов адреса на любом бите. Для стандартных классов маски имеют следующие значения: класс А – 255.0.0.0, класс В – 255.255.0.0, класс С – 255.255.255.0 и позволяют выделить для маршрутизации адрес сети только по границе байта. Маска 128 выделяет старший бит в байте, 192 – два старших бита, 224 – три старших бита и т.д. На применении масок, позволяющих произвольно устанавливать границы в адресе, основана технология бесклассовой междоменной маршрутизации (CIDR).

Второй алгоритм более эффективного использования адресов – трансляция адреса (NAT). Этот алгоритм основан на том, что все узлы автономной системы практически никогда не нуждаются в одновременном доступе во внешние сети. Поэтому количество необходимых для эффективной работы адресов существенно меньше количества узлов в автономной системе. В пределах автономной системы можно использовать независимую внутреннюю адресацию, например, на основе локальных адресов, указанных выше. Шлюз на границе автономной системы обеспечивает автоматическое преобразование локального адреса в глобальный. Этот внешний адрес передается в пользование узлу только на необходимое для работы время. После завершения работы внешний адрес передается другому узлу и т.д. С точки зрения внешнего доступа к автономной системе используется небольшое количество адресов, а количество узлов, которые используют эти адреса, намного больше. Существует специальный протокол распределения внешних адресов DHCP.

DHCP сервер получает от узлов автономной системы заявки на внешние адреса. При наличии свободных адресов, сервер этот адрес закрепляет и обеспечивает переадресацию пакетов преобразование локального адреса во внешний и наоборот. Этот адрес выделяется узлу на определенный период (время аренды). Если адрес продолжает использоваться, время аренды автоматически продлевается. Если адрес не используется к окончанию времени аренды, он считается свободным и может быть передан другому узлу.

Так как автономные системы могут использовать различные сетевые технологии, на уровне межсетевых интерфейсов необходимо решать целый ряд задач для обеспечения корректного взаимодействия. Одной из важнейших задач межсетевых интерфейсов является преобразование внешних адресов в локальные адреса. Уже рассмотренный протокол DHCP решает задачу распределения ограниченного числа внешних адресов по запросам узлов автономной системы. На входе в автономную систему внешний адрес дейтаграммы должен быть преобразован в локальный. За выполнение этой процедуры отвечает специальный протокол разрешения адреса ARP. В соответствии с этим протоколом ведется заполнение ARP-таблицы, которая содержит внешние адреса и соответствующие им локальные адреса автономной системы. Если поступившая дейтаграмма содержит внешний адрес, не зарегистрированный в ARP-таблице, выполняется специальная процедура поиска узла с этим адресом. Она может быть выполнена, например, рассылкой широковещательного сообщения с неизвестным внешним адресом. Узел автономной системы, обнаруживший в широковещательном сообщении свой внешний адрес, должен ответить сообщением со своим локальным адресом, по которому создается новая запись в ARP-таблице. Для сокращения объема этих таблиц записи обычно динамические, т.е. хранятся ограниченное время. Если в течение определенного интервала времени запись не используется, ее удаляют из таблицы.

Таким образом, топология сети и структура глобальных (внешних) адресов тесно связаны. Алгоритмы формирования и обработки IP-адресов предоставляют возможности гибкого конфигурирования сети, межсетевые интерфейсы автономных систем преобразуют и форматы представления данных, и адреса для организации корректного взаимодействия. Система адресации, кроме того, должна создавать необходимые предпосылки для эффективного решения задачи маршрутизации.

**4. МАРШРУТИЗАЦИЯ В IP** **– СЕТЯХ**

Маршрутизация в IP-сетях основана на иерархической структуризации сети и соответствующей структуризации адресов. Маршрутизаторы (шлюзы) могут быть внутренними, образующими внутреннюю структуру автономной системы, и внешними, обеспечивающими доступ к магистрали для выхода на верхние уровни структуры сети. Внутренние шлюзы должны содержать детальную информацию о структуре автономной системы и обеспечивать на ее основе маршрутизацию дейтаграмм в пределах автономной системы. Нет необходимости выполнять маршрутизацию вне автономной системы и обрабатывать соответствующую маршрутную информацию, необходимо только направить дейтаграмму во внешний шлюз. Внешние шлюзы, напротив, не должны поддерживать процедуры внутренней маршрутизации, но должны обладать информацией для маршрутизации дейтаграмм вне автономной системы. Маски адреса предоставляют возможность такого разделения маршрутизации. На каждом уровне сети можно выделить те элементы IP-адреса, которые имеют значение для выбора маршрута.

Разделение маршрутизации на внешнюю и внутреннюю позволяют существенно уменьшить объем обрабатываемой маршрутной информации и объем таблиц маршрутизации в каждом шлюзе. Внешний шлюз, получив дейтаграмму, адресованную в автономную систему, направляет ее во внутренний шлюз, обладающий информацией для маршрутизации в пределах автономной системы. Внутренний шлюз, получив дейтаграмму, адресованную за пределы автономной системы, просто должен направить ее во внешний шлюз.

Таблица маршрутизации имеет вид:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Адрес назначения | Маска адреса | Адрес следующего маршрутизатора | Адрес порта | Расстояние |

Заполняются таблицы маршрутизации специальными протоколами, основанными на алгоритмах адаптивной распределенной маршрутизации. Т.е. каждый шлюз самостоятельно формирует свою таблицу маршрутизации, на основе данных, получаемых от соседних шлюзов. Алгоритмы обмена этими данными и являются основным предметом протоколов маршрутизации.

**4.1 Дистанционно-векторный протокол RIP**

RIP – протокол внутренней маршрутизации, это один из наиболее старых протоколов и, хотя его постепенно вытесняет протокол OSPF, до настоящего времени широко применяется. В современных версиях протокола обработка адреса основана на применении масок адреса. Одно из существенных требований – метрика должна обладать свойством аддитивности, т. е. вес пути должен определяться суммой весов отдельных элементов пути. Вес может отражать параметры задержки, производительности или надежности, а также их комбинации. Для определения маршрута протокол предполагает выбор пути с минимальным весом в заданной метрике. Часто в качестве веса применяют количество промежуточных узлов до узла назначения. Таблицы маршрутизации создаются в узлах с определенной последовательности.

На первом этапе создается минимальная таблица, которая отражает только непосредственные связи (все расстояния 1). Ее несложно создать рассылкой запросов по всем выходным портам. На втором этапе эта минимальная таблица рассылается всем ближайшим соседям, это необходимо для получения от них RIP-пакетов. На третьем этапе маршрутизатор получает от соседних узлов содержание их таблиц маршрутизации в RIP-пакетах. Для каждой записи в полученной таблице маршрутизации расстояние увеличивается на единицу и производится сравнение расстояния с ранее записанным в создаваемой таблице маршрутизации. Если расстояние меньше, запись заменяют новой. Когда такие сообщения получены от всех соседних узлов, таблицу маршрутизации можно считать сформированной. Маршрутизатор переходит в стандартный режим периодической отправки RIP-пакетов со своей таблицей маршрутизации и получения, с соответствующей обработкой, таблиц маршрутизации соседних узлов. Таким образом, после определенного числа таких периодических коррекций изменение сети, связанное с появлением нового маршрутизатора становится известным всем остальным маршрутизаторам.

В RIP – протоколе не предусмотрено извещений об отказе отдельных путей. Для того, чтобы отказы не приводили к некорректной маршрутизации, используется два механизма. Во-первых, для каждой записи в таблице маршрутизации установлено время жизни (6 периодов рассылки RIP-пакетов). Если в принятых RIP-пакетах запись подтверждается, время жизни автоматически продлевается. Во-вторых, для недоступных узлов устанавливается специальное расстояние (16), что автоматически предполагает максимальное доступное расстояние 15. Если обнаруживается, что какие-либо адреса недоступны, для них устанавливается расстояние 16. При получении записи с этим расстоянием соответствующие маршруты автоматически удаляются из таблиц маршрутизации. Естественно, что это ограничение на расстояние по сети накладывает соответствующие ограничения на топологию автономной системы.

Используемый в RIP – протоколе алгоритм создания таблиц маршрутизации может приводить к созданию ложных маршрутов в виде петель или контуров. Для борьбы с ложными маршрутами применяют специальные алгоритмы: "расщепление горизонта", "триггерные обновления" и "замораживание изменений". Расщепление горизонта избавляет от петель между соседними маршрутизаторами, запрещая передавать записи в таблице маршрутизации тому соседу, на основе данных которого эта запись создана. Триггерные обновления – передача изменений в метрике немедленно, не ожидая окончания периода рассылки RIP-пакетов. Замораживание изменений требует запрета в течение определенного интервала времени на прием новых данных об адресах, ставших недоступными.

В целом протокол обеспечивает достаточно эффективное решение задачи маршрутизации в IP-сетях. Достоинство RIP–протокола – простота реализации, недостатки – большой поток служебных данных при обмене таблицами маршрутизации и не всегда корректное решение задачи с созданием ложных маршрутов.

**4.2 Протокол состояния связей OSPF**

Недостатки RIP–протокола связаны с применяемым алгоритмом формирования таблиц маршрутизации. В алгоритмах состояния связей создание таблиц маршрутизации сложнее, однако в процессе работы маршрутизаторов существенно сокращается обмен служебными данными и отсутствуют ложные маршруты в форме петель и контуров.

Построение таблиц маршрутизации разбивается на две задачи. Первая задача – создание модели топологии сети в форме графа связей (матрицы длин непосредственных связей). Вторая задача – по графу связей найти оптимальный маршрут и занести его в таблицу маршрутизации. Метрику для построения графа связей можно выбирать разную и, соответственно, оптимизировать маршрут по разным критериям. В протоколе OSPF для выбора оптимального маршрута используется алгоритм Дейкстры (нумерации вершин). Протокол позволяет хранить несколько маршрутов и реализовать режим баланса нагрузок, отправляя дейтаграммы по альтернативным маршрутам.

Для создания графа связей маршрутизаторы обмениваются специальными сообщениями – объявлениями о связях маршрутизатора. Эти сообщения просто передаются по сети без всяких изменений. Поэтому все маршрутизаторы создают на основе одних и тех же сообщений одинаковые графы связей. Определенные некорректности в RIP–протоколе связаны с тем, что каждый маршрутизатор модифицирует маршрутную информацию и отправляет ее дальше в измененном виде. Поддержание графа связей не требует передачи информации о связях в полном объеме. Протокол OSPF предусматривает периодическую передачу коротких сообщений HELLO, подтверждающих работу маршрутизатора. Периодичность рассылки выбирают меньше, изменения быстрее распространяются по сети, а малый объем сообщений не приводит к перегрузке. Если обнаруживаются изменения в структуре, передается только информация об этих изменениях. Маршрутизаторы перестраивают графы связей и соответствующие записи в таблицах маршрутизации.

Так как графы связей во всех маршрутизаторах одинаковы, петли и контура при маршрутизации не возникают. Некорректная маршрутизация может происходить только при запаздывании информации об изменениях. Это продолжается в гораздо меньшем интервале времени, чем в протоколе RIP, и приводит только к отправке дейтаграмм по недействующему маршруту. К особенностям протокола OSPF следует отнести существенно более высокие требования к вычислительным ресурсам маршрутизаторов