Занятие №21 «Архитектура и технологии построения глобальных сетей на базе протоколов TCP/IP»

Термин "TCP/IP" обычно обозначает все, что связано с протоколами TCP и IP. Он охватывает целое семейство протоколов, прикладные программы и даже саму сеть. TCP/IP - это технология межсетевого взаимодействия, технология internet. Сеть, которая использует технологию internet, называется "internet". Если речь идет о глобальной сети, объединяющей множество сетей с технологией internet, то ее называют Internet.

Существует совет по развитию сети Internet (Internet Activities Board - IAB), который присваивает протоколам семейства TCP/IP состояние и статус.

Более подробную информацию по протоколам семейства TCP/IP и способам организации сетей internet можно найти в RFC (Request for Comment) - документах, распространяемых DDN Network Information Center (NIC) (DDN-цифровая сеть передачи данных). Полный каталог RFC, а также сами документы можно получить по электронной почте, обратившись по адресу service@nic.ddn.mil.

Большой вклад в развитие стека TCP/IP внес университет Беркли, реализовав протоколы стека в своей версии ОС UNIX. Широкое распространение ОС UNIX привело и к широкому распространению протокола IP и других протоколов стека. На этом же стеке работает всемирная информационная сеть Internet, чье подразделение Internet Engineering Task Force (IETF) вносит основной вклад в совершенствование стандартов стека, публикуемых в форме спецификаций RFC. Реализация стека протоколов TCP/IP в последних версиях сетевых операционных систем для персональных компьютеров (Windows NT 3.5, NetWare 4.1, Windows 95, 98, 2000) является хорошей предпосылкой для дальнейшего широкого применения и развития данного стека протоколов.

1. Архитектура протоколов TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) - это промышленный стандарт стека протоколов, разработанный для глобальных сетей.

Базовые протоколы TCP/IP созданы в начале 70-х годов на основе разработок агентства DARPA организациями МО и других ведомств США (Сеть ARPAnet - существовала до 1990г. ARPA – Advanced Research Projects Agency – агентство перспективных научных исследований). Сейчас они используются в глобальной сети ПД Internet, а также в ряде специальных сетей ПД Российской федерации. Работа по их совершенствованию координируется специальными структурами сети Internet. Протоколы TCP/IP успешно конкурируют со стандартами OSI/ISO, в перспективе, возможно, их совместное использование на базе конвергенции этих двух протокольных платформ.

Основным элементом протоколов TCP/IP является Internet Protokol (IP) - протокол межсетевого взаимодействия, который реализует дейтаграммный процесс передачи пакетов данных в интерсети (т.е. в совокупности объединенных сетей ПД). Надежность доставки информации и ее целостность обеспечивает протокол управления передачей данных с организацией виртуальных соединений на транспортном уровне (TCP). Архитектура сетей ПД, использующих протоколы TCP/IP, показана на Рис. 1.

Приложения реализуют различные прикладные службы такие, как электронная почта, обмена файлами, терминального доступа к удаленным серверам и т.п. Приложения формируют и передают транспортному уровню массив сообщений, имеющих соответствующий объем и структуру.

Транспортный уровень, реализуемый протоколами UDP или TCP, формирует сегменты данных (пакеты), которые передаются сетевому уровню - IP-протоколу, главной задачей которого является маршрутизация при доставке пакетов от отправителя к получателю. На сетевом уровне используется также протокол управления сетью ICMP (Internet Control Message Protocol).

В качестве среды передачи могут использоваться различные сети ПД (например, X.25, FR и др.) или различные каналы связи. Межсетевой уровень (IP-протокол) формирует IP-пакеты, которые могут отличаться по объему от сегментов (пакетов), получаемых от транспортного уровня.

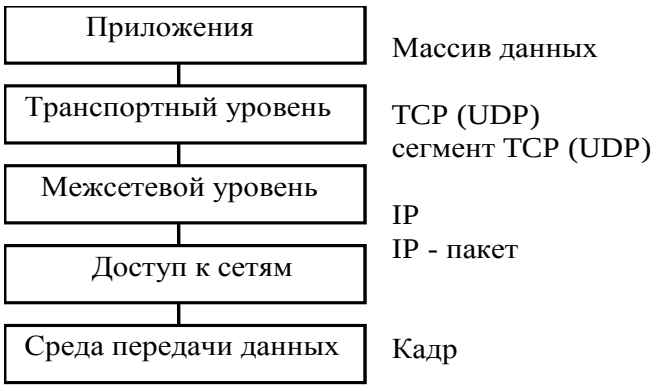


Рис. 1

Уровень доступа к сетям (к среде передачи) формирует кадры (фрагменты пакетов), имеющие формат, структура которого определяется характеристиками используемых сетей передачи или каналов связи. Основное назначение уровня доступа к сетям (сетевого интерфейса) - обеспечение независимости функционирования протоколов TCP/IP от среды передачи. Эта независимость определяет возможность их использования в различных сетях ПД, в том числе и в сетях, использующих разнотипную аппаратуру ПД.

2. Протоколы прикладного уровня

Протоколы прикладного уровня ориентированы на конкретные прикладные задачи. Они определяют как процедуры по организации взаимодействия определенного типа между прикладными процессами, так и форму представления информации при таком взаимодействии. Рассмотрим некоторые из прикладных протоколов.

Протокол TELNET позволяет обслуживающей машине рассматривать все удаленные терминалы как стандартные "сетевые виртуальные терминалы" строчного типа, работающие в коде ASCII, а также обеспечивает возможность согласования более сложных функций (например, локальный или удаленный эхоконтроль, страничный режим, высота и ширина экрана и т.д.).

TELNET работает на базе протокола TCP. На прикладном уровне над TELNET находится либо программа поддержки реального терминала (на стороне пользователя), либо прикладной процесс в обсуживающей машине, к которому осуществляется доступ с терминала.

Работа с TELNET походит на набор телефонного номера. Пользователь набирает на клавиатуре что-то вроде telnet delta и получает на экране приглашение на вход в машину delta.

Протокол TELNET существует уже давно. Он хорошо опробован и широко распространен. Создано множество реализаций для самых разных операционных систем. Вполне допустимо, чтобы процесс-клиент работал, скажем, под управлением ОС VAX/VMS, а процесс-сервер под ОС UNIX System V.

Протокол FTP (File Transfer Protocol - протокол передачи файлов) распространен также широко как TELNET. Он является одним из старейших протоколов семейства TCP/IP. Также как TELNET он пользуется транспортными услугами TCP.

Существует множество реализаций для различных операционных систем, которые хорошо взаимодействуют между собой. Пользователь FTP может вызывать несколько команд, которые позволяют ему посмотреть каталог удаленной машины, перейти из одного каталога в другой, а также скопировать один или несколько файлов.

Протокол SMTP (Simple Mail Transfer Protocol - простой протокол передачи почты) поддерживает передачу сообщений (электронной почты) между произвольными узлами сети Internet. Имея механизмы промежуточного хранения почты и механизмы повышения надежности

доставки, протокол SMTP допускает использование различных транспортных служб. Он может работать даже в сетях, не использующих протоколы семейства TCP/IP.

Протокол SMTP обеспечивает как группирование сообщений в адрес одного получателя, так и размножение нескольких копий сообщения для передачи в разные адреса. Над модулем SMTP располагается почтовая служба конкретных вычислительных систем.

Сетевая файловая система NFS (Network File System) использует транспортные услуги UDP и позволяет монтировать в единое целое файловые системы нескольких машин с ОС UNIX. Бездисковые рабочие станции получают доступ к дискам файл-сервера так, как будто это их локальные диски.

NFS значительно увеличивает нагрузку на сеть. Если в сети используются медленные линии связи, то от NFS мало толку. Однако, если пропускная способность сети позволяет NFS нормально работать, то пользователи получают большие преимущества. Поскольку сервер и клиент NFS реализуются в ядре ОС, все обычные несетевые программы получают возможность работать с удаленными файлами, расположенными на под монтированных NFS-дисках, точно также как с локальными файлами.

Протокол SNMP (Simple Network Management Protocol - простой протокол управления сетью) работает на базе UDP и предназначен для использования сетевыми управляющими станциями. Он позволяет управляющим станциям собирать информацию о положении дел в сети Internet. Протокол определяет формат данных, их обработка и интерпретация остаются на усмотрение управляющих станций или менеджера сети.

Система X-Window использует протокол X-Window, который работает на базе TCP, для многооконного отображения графики и текста на растровых дисплеях рабочих станций (используется в качестве оконного интерфейса в операционных системах UNIX и LINUX).

В 90-е годы появились новые протоколы прикладного уровня.

Протокол HTTP - протокол передачи гипертекстовой информации (Hyper Text Transfer Protocol). Основа формирования всемирной информационной службы (всемирной информационной паутины) - WWW (World Wide Web).

Протокол RTP – (Real Time Protocol) протокол передачи данных в реальном времени. Разработан для обеспечения передачи аудио- и видеосигналов по сети Интернет с малой задержкой (IP-телефония).

Протокол RSVP – (Resource reSerVation Protocol) протокол резервирования ресурса. Разработан для обеспечения гарантированной скорости передачи (полосы пропускания) в виртуальном канале по определенному маршруту.

3. Протоколы транспортного уровня

Транспортный уровень в объединенных сетях может быть реализован при использовании дейтаграммного протокола пользователя UDP (User Datagram Protocol) или протокола управления передачей данных TCP (Transmission Control Protocol).

Транспортный уровень обеспечивает обмен между прикладными процессами. Идентификация процесса получателя осуществляется по расширенному адресу, состоящему из двух частей - IP-адреса, идентифицирующего оконечную установку, и номера порта, идентифицирующего прикладной процесс.

Дейтаграммный протокол пользователя UDP обеспечивает ретрансляцию услуг протокола IP приложениям. Он не гарантирует доставку (т.е. возможны как потери, так и дублирования дейтаграмм) и порядок следования дейтаграмм. Сообщение протокола UDP состоит из заголовка и блока данных.

Сегмент данных при использовании протокола UDP

Заголовок				Данные
1 16	17 32	33 48	49 64	65 …
Адр. порта отпр-ля	Адр.порта получ-ля	Указатель длины	Контрольная сумма	

Заголовок состоит из четырех 16-битовых полей, содержащих адреса портов процессов отправителя и получателя, указатель полной длины сообщения и контрольную сумму. Таким

образом, основной функцией протокола UDP является мультиплексирование и демультиплексирование (распределения по портам) потока дейтаграмм между приложениями. Кроме этого, использование контрольной суммы позволяет контролировать достоверность данных.

Не все поля UDP-пакета обязательно должны быть заполнены. Если посылаемая дейтаграмма не предполагает ответа, то на месте адреса отправителя могут помещаться нули. Можно отказаться и от подсчета контрольной суммы, однако следует учесть, что протокол IP подсчитывает контрольную сумму только для заголовка IP-пакета, игнорируя поле данных.

Протокол управления передачей данных TCP обеспечивает полноценную транспортную службу, которая обеспечивает обмен потоками данных. При этом протокол TCP не накладывает ограничений на состав потока, освобождая прикладной процесс от функции структурирования данных. Передача данных протоколу TCP аналогична их записи в неструктурированный файл.

Протокол TCP буферизирует данные, передаваемые в сеть, оптимизирует трафик выбором объемов сообщений. Для передачи данных протоколом TCP организуются перед началом обмена виртуальные соединения. Соединения обеспечивают двустороннюю одновременную передачу данных между компьютерами, причем передача управляющей информации обеспечивается совместно с потоком данных. Соединение идентифицируется двумя точками, каждая из которых определяется IP адресом и номером протокольного порта. Соединение устанавливается по запросу приложения - инициатора соединения, по которому операционной системой выделяется протокольный порт и высылается сообщение процессу-получателю, устанавливающее счетчики переданных сообщений данных в исходное состояние. Процесс-получатель отвечает согласием на соединение и получает от своей операционной системы номер протокольного порта.

Целостность потока данных обеспечивается квитированием, при этом для управления потоком данных используется механизм окна. Управление шириной окна позволяет решать две задачи - защищать от перегрузок, как промежуточные узлы сети, так и буферную память протокола TCP, принимающего данные. Первую задачу решают маршрутизаторы, направляя протоколам оконечных станций требования об уменьшении размера окна.

Вторая задача решается непосредственно протоколом TCP, который декларирует выбранную ширину окна, используя при необходимости и нулевую ширину окна, т.е. запрещая передачу.

Формат сообщения протокола TCP, которое часто называют сегментом, в большинстве случаев выбирают таким образом, чтобы обеспечивалась возможность его включения в IP-пакет. Сегмент TCP состоит из заголовка и поля данных:

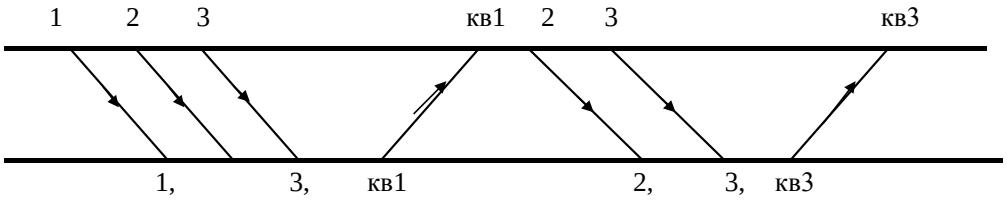
Поля заголовка, содержащие номера портов отправителя и получателя (по 16 бит каждый), идентифицируют прикладные процессы отправителя и получателя. Затем для управления потоком данных передаются номера последнего переданного байта и ожидаемого байта (т.е. увеличенный на единицу номер последнего принятого байта). Поле длины заголовка из 4 бит определяет длину заголовка сегмента TCP, измеренную в 32-битовых блоках. Длина заголовка не фиксирована, она зависит от числа бит в поле с дополнительной информацией. Следующие 6 бит зарезервированы для последующего использования. После резервных передаются 6 служебных бит, используемые для указания признаков 1) срочности сообщения, 2) квитанции на принятый сегмент, 3) требования передачи сообщения без ожидания заполнения буфера, 4) запроса на переустановку соединения, 5) синхронизации счетчиков переданных данных при установлении соединения и 6) последнего байта в передаваемом потоке данных. Активному состоянию служебного бита соответствует значение 1. Ширина приемного окна декларируется в байтах, для чего используется поле из 16 бит.

Контрольная сумма из 16 бит определяется по сегменту и псевдозаголовку из 96 бит (12 байт), включающему IP адреса отправителя и получателя и другие данные из заголовка IP-пакета.

Поле, содержащее число, указывающее на окончание срочных данных, используется совместно с соответствующим служебным битом. Дополнительная информация используется при решении вспомогательных задач при обмене данных.

Особенностью управления потоком данных является указание ширины окна, а также номеров последнего переданного и ожидаемого элементов потока данных в байтах при осуществлении обмена сегментами данных. Далее на рисунке показан пример передачи трех сегментов из 4 байтов (фактически число байтов в сегменте намного больше и число 4 берется для наглядности рассмотрения примера).

Передача сегментов данных, приём квитанций



Приём сегментов данных, передача квитанций

Номера последних переданных байтов НП в 1, 2 и 3 сегментах будут соответственно равны 4, 8 и 12. Пусть сегменты 1 и 3 будут приняты правильно, а сегмент 2 - не принят. Тогда передается квитанция на сегмент 1, содержащая номер ожидаемого байта ОН, равный 5. В соответствии с этим значением ОН повторяются сегменты 2 и 3. После их приема передается квитанции с ОН, равным 13, разрешающая передачу следующего сегмента. Обмен данных завершается передачей служебного бита - признака последнего бита в передаваемом потоке данных.

4. Протоколы сетевого уровня

Сетевой уровень (протокол IP) обеспечивает только маршрутизацию и доставку пакетов данных и полностью освобожден от задач обеспечения надежности. Функции транспортного и сетевого уровней четко разделены, чем исключено их дублирование.

Объединенная сеть ПД, использующая протоколы TCP/IP (например, сеть Internet, сети DDN и т.п.), представляет из себя совокупность сетей ПД, территориальных и локальных, объединенных маршрутизаторами.

Межсетевой протокол IP реализуется программным обеспечением оконечных установок пользователей и маршрутизаторов и не зависит от характеристик используемых территориальных и локальных сетей.

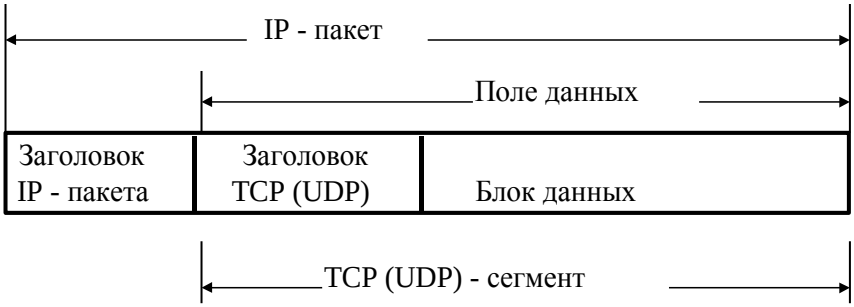
Основными характеристиками протокола IP являются:

– формат IP пакета;

– способ обработки конфликтных ситуаций;

– способ маршрутизации.

Формат пакета включает заголовок и поле данных.



Полная длина пакета может достигать 65535 байт. В заголовке указываются:

– версия протокола;

– приоритет;

– IP-адреса получателя и отправители (по 32 бита);

– "время жизни", т.е. время, в течение которого пакет может существовать в сети (для устранения из сети пакетов, задержанных вследствие каких-либо причин). Значение этого времени уменьшается при прохождении пакета по сети, а по его истечении пакет уничтожается с уведомлением отправителя. Такая мера защищает сеть от циклических маршрутов и от перегрузок.

– тип протокола транспортного уровня (UDP или TCP), для которого предназначена информация, содержащаяся в поле данных пакета IP.

IP протокол реализует операции сборки и разборки пакетов, связанные с использованием сетей, в которых применяются форматы меньших длин, чем в пакетах получаемых от транспортного уровня. Формат IP-пакета согласуется с форматами пакетов используемых сетей, путем деления пакета, включающего один сегмент на определенное количество фрагментов, зависящее от указанных форматов (с добавлением к каждому из них заголовка пакета).

Рассмотрим более подробно адресование в сети TCP/IP.

IP- адреса, содержащиеся в заголовке, являются 32-битовыми идентификаторами объектов сети - оконечных установок и маршрутизаторов. Они состоят из идентификаторов сетей и идентификаторов оконечных установок, причем в зависимости от класса сети число бит, выделяемых для идентификации сетей и оконечных установок, может меняться. Предусмотрена также возможность использования групповых адресов.

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

– 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.

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.

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.

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}

С описанными классами адресов есть проблема несоответствия размеров сетей согласно классам размерам реальных сетей. Сети класса A громадны, а класса C очень малы; свободных сетей класса B больше нет. Существуют три основных решения данной проблемы: разделение сетей на подсети, введение адресации, основанной на префиксах, и переход к новой 6-й версии протокола IP с размером адреса 128 байт.

Способ обработки конфликтных ситуаций реализуется специальным протоколом ICMP (Internet Control Message Protocol), функционирующим при возникновении нештатных ситуаций. Он предназначен для выяснения природы ошибок и извещения о них приложений, сформировавших пакет. Основными функциями этого протокола являются:

- выяснение наличия и активности узлов связи путем обмена тестовыми сообщениями;
- выяснение достижимости узлов получателей, сброс пакетов, направляемых к недостижимым узлам;
- изменение маршрутов;
- уничтожение пакетов с истекшим временем жизни;
- синхронизация времени в узлах связи;
- управление потоками данных.

Способ маршрутизации обеспечивает определение оптимального маршрута доведения пакета до получателя, адрес которого указан в заголовке пакета. Направление передачи пакета определяется по данным маршрутной таблицы специальным протоколом, на вход которого поступают пакеты от протоколов верхнего уровня - TCP, UDP или ICMP.

В протоколе IP используются как статический, так и динамический способы маршрутизации.

Статическая маршрутизация используется в оконечных установках локальных сетей, а также в сетях с ограниченным числом абонентов. Маршрутная таблица имеет ограниченный объем и содержит лишь данные о соседних оконечных установках. Пакеты к другим адресатам направляются в маршрутизатор, имеющий существенно больше данных об адресатах сети. Таким образом, маршрутизация в этом случае осуществляется на основе неполной информации.

При использовании **динамической маршрутизации** осуществляется постоянная корректировка маршрутных таблиц на основе данных, содержащихся в служебных сообщениях, которыми маршрутизаторы обмениваются между собой. При определении оптимальных маршрутов используются два класса протоколов. Первый класс протоколов (**RIP**) основан на подсчете числа промежуточных ретрансляций в маршрутизаторах и не учитывает реальную пропускную способность каналов передачи данных между маршрутизаторами. В протоколах второго типа (**OSPF**) оптимизация маршрутов осуществляется на основе измерения времени задержки пакетов, что обеспечивает лучшие условия для выравнивания нагрузки в сети, но приводит к усложнению реализации.