# IP

IP (Internet Protocol) представляет собой протокол уровня маршрутизируемых дейтаграмм в стеке TCP/IP. Все другие протоколы стека TCP/IP (кроме ARP и RARP) используют протокол IP для маршрутизации кадров между хостами. Заголовок кадров IP содержит маршрутную и управляющую информацию, связанную с доставкой дейтаграмм.

Структура заголовков IP показана на рисунке.

|  |  |  |  |
| --- | --- | --- | --- |
| 4 | 8 | 16 | 32 |
| Версия | IHL | Тип сервиса | Общий размер |
| Идентификация | Флаги | Смещение фрагмента |
| Время жизни | Протокол | Контрольная сумма заголовка |
| Адрес отправителя |
| Адрес получателя |
| Опции и заполнение |
| Данные |

Структура заголовка IP.

##### Версия

Поле версии определяет формат заголовка Internet.

##### IHL

Internet Header Length - размер заголовка Internet указывает размер заголовка в 32-битовых словах, задавая смещение данных от начала пакета. Минимальный размер заголовка составляет 5 слов (160 битов).

##### Тип сервиса

Показывает желаемый уровень качества обслуживания. Сети могут обеспечивать различный уровень преимуществ при доставке, играющий важную роль при условиях высокой загрузки сети. Поддерживаются также три опции качества обслуживания - малая задержка, высокая надежность и высокая пропускная способность.

Биты 0 - 2 - преимущественная доставка

111 сетевое управление

110 межсетевое управление

101 CRITIC/ECP

100 Flash override

011 Flash

010 немедленная доставка

001 приоритетная доставка

000 Routine (нормальный режим)

Бит 3 - задержка

0 Нормальная

1 Малая

Бит 4 - пропускная способность

0 Нормальная

1 Высокая

Бит 5 - надежность доставки

0 Нормальная

1 Высокая

Биты 6 - 7 - зарезервированы для использования в будущем

##### Общий размер

Размер дейтаграммы в байтах с учетом заголовка и данных. Размер поля позволяет использовать дейтаграммы длиной до 65535 байтов, хотя такой размер нежелателен для многих сетей и хостов. Все хосты должны быть готовы к приему дейтаграмм размером до 576 байтов, независимо от того как они доставляются - целиком или фрагментами. Рекомендуется передавать дейтаграммы, размер которых превышает 576 байтов только в тех случаях, когда адресат готов принять такие дейтаграммы.

##### Идентификация

Значение идентификатора, которое отправитель задает для обеспечения корректного порядка сборки фрагментов дейтаграммы на приемной стороне.

##### Флаги

Трехбитовое поле флагов управления:

Бит 0 - зарезервирован и должен иметь нулевое значение

Бит 1 - возможность фрагментирования

0 Можно фрагментировать

1 Не фрагментировать

Бит 2 - наличие дополнительных фрагментов

0 Последний фрагмент

1 Есть последующие фрагменты

##### Смещение фрагмента

13-битовое значение, задающее смещение фрагмента от начала целой дейтаграммы. Смещение фрагмента измеряется в 8-байтовых (64 бита) словах. Первый фрагмент имеет нулевое смещение.

##### Время жизни

Показывает максимальное время существования дейтаграммы в сети Internet. При нулевом значении этого поля дейтаграмма должна быть уничтожена. Время жизни дейтаграмм измеряется в секундах. Однако, поскольку каждый модуль, работающий с дейтаграммой, должен уменьшать значение поля TTL (time-to-life) по крайней мере на 1 (даже в тех случаях, когда обработка дейтаграммы занимает меньше секунды), значение этого поля должно быть не меньше желаемого времени жизни дейтаграммы. Дейтаграммы с истекшим в процессе доставки временем жизни не попадают к получателю.

##### Протокол

Указывает протокол следующего уровня, содержащийся в поле данных дейтаграммы IP.

##### Контрольная сумма заголовка

Контрольная сумма, рассчитанная с учетом только полей заголовка дейтаграммы. Поскольку некоторые поля заголовка (например, время жизни) могут меняться в процессе доставки, значение контрольной суммы заново вычисляется и проверяется в каждой точке обработки заголовков.

##### Адрес отправителя/ получателя

32-битовые значения адресов отправителя и получателя дейтаграммы. Следует четко различать имена, адреса и маршруты. Имя показывает название объекта, адрес говорит о его местоположении в сети, а маршрут - показывает путь к объекту. Протокол IP имеет дело преимущественно с адресами. Связь между адресами и именами реализуется протоколами вышележащих уровней. Модуль Internet отображает адреса IP на локальные сетевые адреса. Связь локальных сетевых адресов с маршрутами обеспечивается протоколами нижележащих уровней.

##### Опции

Это поле содержит необязательные опции дейтаграммы. Используемые опции должны быть реализованы во всех модулях IP (хосты и шлюзы). В некоторых опции безопасности являются обязательными для всех дейтаграмм.

Поле опций имеет переменную длину и может содержать различное число опций. Существуют два формата опций:

* Однооктетные опции
* Многооктетные опции, содержащие поля типа опции (1 октет), ее размера (1 октет) и собственно опций.

Поле длины опции учитывает все субполя опции - тип, размер и сами опции.

Октет типа опции имеет три поля:

1 бит - флаг копирования показывает, что должна ли данная опция копироваться во все фрагменты дейтаграммы:

0 опция копируется

1 опция не копируется.

2 бита - класс опции:

0 управление

1 зарезервировано

2 отладка и измерение

3 зарезервировано

5 битов - номер опции

##### Данные

Данные IP или протоколов вышележащих уровней.



**Межсетевой протокол IP**. Модуль IP является базовым элементом технологии Internet. Его центральной частью является таблица маршрутов. Таблица маршрутов заполняется администратором сети и обычно инициализируется в момент загрузки системы. Когда речь идет о простой локальной IP-сети, то протокол IP мало что добавляет к услугам Ethernet, за исключением того, что в сети будут работать все прикладные программы, реализованные для IP-технологии. Однако ситуация меняется, если речь идет о сетях, сопряженных шлюзом.

**Протокол RIP (Routing Information Protocol)**. Протокол предназначен для автоматического обновления таблицы маршрутов. При этом используется информация о состоянии сети, которая рассылается маршрутизаторами (routers). В соответствии с протоколом RIP любая машина может быть маршрутизатором. При этом все маршрутизаторы делятся на активные и пассивные. Активные маршрутизаторы сообщают о маршрутах, которые они поддерживают в сети. Пассивные маршрутизаторы читают эти широковещательные сообщения и исправляют свои таблицы маршрутов, но при этом сами информации в сеть не предоставляют. Обычно в качестве активных маршрутизаторов выступают шлюзы, а в качестве пассивных - обычные машины (hosts).

**Протокол UDP**. Этот протокол является одним из двух основных транспортных протоколов, расположенных сразу над IP. К заголовку IP-пакета UDP добавляет два поля: порт и контрольная сумма. Поле “порт” позволяет мультиплексировать информацию между разными прикладными процессами. Поле "контрольная сумма" позволяет поддерживать целостность данных

**Протокол TCP**. Предоставляет другой способ доставки сообщений, отличный от UDP. Вместо "ненадежной" доставки датаграмм без установления соединения, TCP обеспечивает гарантированную доставку с установлением соединения в виде байтовых потоков.

Прикладные программы взаимодействуют с модулем TCP также через порты. Существуют определенные стандартом номера портов, которые отведены под обслуживание стандартных сервисов Internet. Так telnet обслуживается через 23 порт, почта (SMTP) - через 25 и т.п.

Когда два процесса начинают общаться через модули TCP, то эти модули поддерживают информацию о состоянии соединения, которое называется виртуальным каналом. Канал является дуплексным, т.е. информация может передаваться одновременно в двух направлениях.

Согласно протоколу TCP, поток байтов разбивается на пакеты. Любые данные для модуля TCP представляются в виде потока байтов. На другом конце виртуального канала данные снова собираются в поток. Модуль TCP не сохраняет разделения потоков данных на записи. Так можно записать в канал 5 записей по 80 байт, а прочитать одну в 400 байтов длиной

# Подробное описание протокола TCP

TCP (Transmission Control Protocol, Протокол управления передачей) был спроектирован в качестве связующего протокола для обеспечения интерактивной работы между компьютерами. TCP обеспечивает надежность и достоверность обмена данными между процессами на компьютерах, входящих в общую сеть. TCP, с одной стороны, взаимодействует с прикладным протоколом пользовательского приложения, а с другой, с протоколом, обеспечивающим "низкоуровневые" функции: маршрутизацию и адресацию пакетов, которые, как правило, выполняет IP.

В операционной системе реализация TCP представляет собой отдельный системный модуль (драйвер), через который, как правило, проходят все вызовы функций протокола. Интерфейс между прикладным процессом и TCP представляет собой библиотеку вызовов, такую же как библиотека системных вызовов, например, для работы с файлами. Вы можете открыть или закрыть соединение (как открыть или закрыть файл) и отправить или принять данные из установленного соединения (аналогично операциям чтения и записи файла). Вызовы TCP могут работать с прикладным приложением в асинхронном режиме. Безусловно, реализация TCP в каждой системе может осуществлять множество собственных функций, но любая из этих реализации должна обеспечивать минимум функциональности, которая требуется стандартами TCP.

Схема работы пользовательского приложения с TCP, в общих чертах, состоит в следующем. Для передачи данных пользовательскому процессу надо вызвать соответствующую функцию TCP, с указанием на буфер передаваемых данных. TCP упаковывает эти данные в сегменты своего стека и вызывает функцию передачи протокола нижнего уровня, например IP.

На другом конце, получатель TCP группирует поступившие от протокола нижнего уровня данные в принимающие сегменты своего буфера, проверяет целостность данных, передает данные пользовательскому процессу и уведомляет отправителя об их получении.

Пользовательский интерфейс с TCP может выполнять такие команды как открыть (OPEN) или закрыть (CLOSE) соединение, отправить (SEND) или принять (RECEIVE) данные, или получить статус соединения (STATUS). Эти вызовы подобны любым другим вызовам функций операционной системы из пользовательской программы, таким как открытие, чтение или закрытие файла.

В модели межсетевого соединения взаимодействие TCP и протоколов нижнего уровня, как правило, не специфицировано, за исключением того, что должен существовать механизм, который обеспечивал бы асинхронную передачу информации от одного уровня к другому. Результатом работы этого механизма является инкапсуляция протокола более высокого уровня в тело протокола более низкого уровня. Реализуется этот механизм через интерфейс вызовов между TCP и IP.

В результате работы этого механизма каждый TCP-пакет вкладывается в "конверт" протокола нижнего уровня, например, IP. Получившаяся таким образом дейтаграмма содержит в себе TCP-пакет так же как TCP-пакет содержит пользовательские данные.

Простейшая модель работы TCP-протокола выглядит обманчиво гладко, поскольку на самом деле реальная работа изобилует множеством деталей и тонкостей.

Логическая структура сетевого программного обеспечения, реализующего протоколы семейства TCP/IP в каждом узле сети Internet, изображена на рис. 2.12.

Прямоугольники обозначают обработку данных, а линии, соединяющие прямоугольники, - пути передачи данных. Горизонтальная линия внизу рисунка обозначает кабель сети Ethernet, которая используется в качестве примера физической среды. Понимание этой логической структуры является основой для понимания всей технологии TCP/IP.

Далее более подробно рассмотрим возможности, принципы построения и основные функции протокола TCP:

 Потоки данных, стек протоколов, механизм гнезд и мультиплексирование соединений

 Процедура установления соединения и передача данных

 Механизмы обеспечения достоверности передаваемых данных

 Механизм контроля потока данных

 Флаг важности пакета, средства обеспечения безопасности протокола

### Потоки данных, стек протоколов, механизм гнезд и мультиплексирование соединений

Для установления соединения между двумя процессами на различных компьютерах сети необходимо знать не только Internet-адреса компьютеров, но и номер ТСР-порта, который процесс использует на данном компьютере. В совокупности с Internet-адресом компьютера порты образуют систему гнезд (sockets). Пара гнезд уникально идентифицирует каждое соединение или поток данных в сети Internet, а порт обеспечивает независимость каждого ТСР-канала на данном компьютере. Безусловно, несколько процессов на машине могут использовать один и тот же ТСР-порт, но с точки зрения удаленного процесса между этими процессами не будет никакой разницы.

Рассмотрим потоки данных, проходящие через протоколы. При использовании протокола TCP данные передаются между прикладным процессом и модулем TCP. Типичным прикладным процессом, использующим протокол TCP, является модуль FTP (File Transfer Protocol, Протокол передачи фай-лов). Стек протоколов в этом случае будет FTP/TCP/IP/ENET. При использовании протокола UDP (User Datagram Protocol, Протокол дейтаграмм пользователя) данные передаются между прикладным процессом и модулем UDP. Например, SNMP (Simple Network Management Protocol, Простой протокол управления сетью) пользуется транспортными услугами UDP. Его стек протоколов выглядит так: SNMP/UDP/IP/ENET.

Одно гнездо на компьютере может быть задействовано в соединениях с несколькими гнездами на удаленных компьютерах. Кроме того, одно и то же гнездо может передавать поток данных в обоих направлениях. Таким образом, механизм гнезд позволяет на одном компьютере одновременно работать нескольким приложениям и уникально идентифицирует каждый поток данных сети. Это называется мультиплексированием соединений.

Модули TCP, UDP и драйвер Ethernet являются мультиплексорами типа n x 1. Действуя как мультиплексоры, они переключают несколько входов на один выход. Они также являются демультиплексорами типа 1 х n. Как демультиплексоры, они переключают один вход на один из многих выходов в соответствии с полем типа в заголовке протокольного блока данных. Когда Ethernet-кадр попадает в драйвер сетевого интерфейса Ethernet, он может быть направлен либо в модуль ARP, либо в модуль IP. (Значение поля типа в заголовке кадра указывает, куда должен быть направлен Ethernet-кадр).

Если IP-пакет попадает в модуль IP, то содержащиеся в нем данные могут быть переданы либо модулю TCP, либо UDP, что определяется полем "Protocol" в заголовке IP-пакета. Если TCP-сообщение попадает в модуль TCP, то выбор прикладной программы, которой должно быть передано сообщение, осуществляется на основе значения поля "порт" в заголовке TCP-сообщения.

Мультиплексирование данных в обратную сторону осуществляется довольно просто, так как из каждого модуля существует только один путь вниз. Каждый протокольный модуль добавляет к пакету свой заголовок, на основании которого машина, принявшая пакет, выполняет демультиплексирование.

Назначение портов приложениям на каждом компьютере происходит независимо друг от друга. TCP может самостоятельно выбирать порт, с которым будет работать приложение, или приложение укажет, с каким портом на данном компьютере оно будет работать. Однако, как правило, часто используемые приложения - сервисы используют одни и те же номера портов, которые уже стали общеизвестными, например, такие как HTTP, FTP, SMTP и др., для того, чтобы к данному процессу на компьютере можно было присоединиться, указывая только адрес машины. Например, Internet браузер, если ему не указать дополнительно, ищет по указанному адресу приложение, работающее с портом 80, - это наиболее распространенный порт для серверов WWW.

Кроме того, машина может быть снабжена несколькими сетевыми интерфейсами, тогда она должна осуществлять мультиплексирование типа п х т, т. е. между несколькими прикладными программами и сетевыми интерфейсами.

### Установление соединения и передача данных

Соединение определяется вызовом команды OPEN с аргументами в виде номера локального порта и гнезда (IP-адрес + порт) удаленного процесса. Функция OPEN вызывается и в том случае, когда данный процесс намерен передавать информацию (активный OPEN), и когда процесс ожидает поступления информации (пассивный OPEN). Функция возвращает идентификатор соединения, по которому пользователь может ссылаться в своих последующих вызовах. Идентификатор соединения указывает на структуру данных, в которой хранятся переменные и информация данного TCP-соединения. Эта структура данных называется Управляющая Структура Передачи - Transmission Control Block (TCB).

ТСВ хранит такие параметры соединения, как адреса локального и удаленного гнезд, указатели на полученные и отправляемые пользовательские данные, указатели на очередь блоков для повторной отправки, номер текущего сегмента и т. д., то есть всю информацию, используемую данным соединением.

Как уже отмечено выше, открытие соединения может быть активным и пассивным. Пассивное открытие обозначает, что процесс ожидает поступления сигнала открытия соединения и не пытается открыть канал самостоятельно. Иными словами, канал, открытый с одного конца как пассивный, ожидает инициирующего сигнала от какого-либо из хостов. Этот тип открытия канала используется процессами, которые предоставляют свой сервис через заранее известный номер своего порта (например, HTTP, SMTP и т. д.) и работают с механизмом общеизвестных гнезд.

Процесс может вызвать функцию пассивного открытия канала и ждать получения сигнала активного открытия канала от другого процесса, и только после получения такого сигнала соединение будет установлено. Соединение будет так же установлено, если два процесса активно откроют канал навстречу друг другу. Эта гибкость в установлении соединения особенно важна в распределенных сетях, когда компьютеры работают асинхронно.

Только в двух случаях принципиально важно, чтобы гнездо на данном компьютере было открыто как пассивное, а на другой стороне как активное:
1. Когда локальное пассивное открытие соединения полностью определяет гнездо на другой стороне.
2. Локальное пассивное открытие гнезда не предполагает каких-либо ограничений на гнездо с другой стороны, т. е. любое гнездо может присоединиться к данному сервису.

Если у вас на одном гнезде открыто пассивно, с соответствующими записями ТСВ, несколько соединений, то при открытии активного соединения на другом конце будет задействовано ТСВ, соответствующее параметрам, заданным активным гнездом. Если такого не существует, выбирается любое другое открытое гнездо.

Процедура установления соединения использует специальный флаг синхронизации - SYN и состоит из трех этапов обмена сообщениями - так называемое "трехходовое квитирование". Использование именно трех тактов квитирующих сообщений всегда достаточно, чтобы синхронизировать потоки данных.

Инициализация соединения начинается с обмена пакетами, которые отправляются при открытии канала пользователем, например, командой OPEN, и содержат флаг SYN и свой начальный порядковый номер пакетов данных. После этого гнезда ожидают пакет с ТСВ-партнера. Соединение считается установленным, когда в обоих направлениях синхронизируются нумерующие последовательности передаваемых пакетов, т. е. и клиент и сервер "знают", пакет с каким номером поступит с противоположного конца соединения.

Соединение закрывается, когда гнезда обмениваются пакетами, содержащими команду FIN. При этом все ресурсы системы, занятые ТСВ-данных соединений, должны быть освобождены.

Вообще говоря, TCP сам определяет, как группировать и когда отправлять очередной блок данных. Однако в некоторых случаях, пользователю необходимо быть уверенным, что все данные, переданные на уровень TCP, отправлены. Для этих целей существует функция "проталкивания пакета" - PUSH-функция. Вызов этой функции позволяет проконтролировать отправку всех буферизированных TCP-протоколом данных.

Примечание:
Под словом "пользователь" здесь и далее будет пониматься пользовательский процесс или приложение, которое работает с TCP.

Пользователь, отправляющий пакет вызовом SEND, указывает, передаются ли в сегменте или в предшествующих сегментах данные немедленно, или при передаче будет использоваться механизм кэширования данных, тогда данные будут отправляться в соответствии с установками системы. Когда же TCP получает пакет с флагом PUSH, а этот флаг устанавливается PUSH-функцией, вся кэшированная информация, вне зависимости от того, сформирована она одним вызовом команды SEND или несколькими, будет немедленно отправлена получателю.

Назначение PUSH-функции и PUSH-флага состоит только в "проталкивании" данных к пользователю, минуя механизм кэширования. Команда PUSH не производит никаких дополнительных группировок или других действий над данными.

Следует отметить, что существует взаимосвязь между PUSH-функцией и использованием буферов данных, используемых как TCP, так и пользовательским интерфейсом. Всякий раз, когда с данными, помещенными в пользовательский буфер получателя, ассоциирован PUSH-флаг, буфер немедленно передается пользователю, даже если он не заполнен до конца. Если данные заполнили буфер до получения PUSH-флага, эти данные передадутся пользователю в размере целого буфера.

### Механизмы обеспечения достоверности передаваемых данных

Протокол ТСР должен уметь работать с поврежденными, потерянными, дублированными или поступившими с изменением порядка пакетами. Это достигается благодаря механизму присвоения порядкового номера каждому передаваемому пакету данных и механизму проверок получения пакетов подтверждения доставки.

Когда TCP передает сегмент данных, копия этих данных помещается в очередь повтора передачи и запускается таймер ожидания подтверждения. Когда система получает подтверждение - сегмент TCP, содержащий управляющий флаг АСК, что этот пакет данных получен, она удаляет его из очереди. Сегмент подтверждения получения содержит номер полученного сегмента, на основании которого и происходит контроль доставки данных адресату. Если подтверждение не поступило до истечения срока таймера, пакет отправляется еще раз. Уведомление TCP о получении пакета данных еще не означает, что он был доставлен конечному пользователю. Оно только означает, что TCP выполнил возложенные на него функции.

При передаче информации каждому байту данных присваивается порядковый номер, поэтому, в какой бы последовательности эти пакеты не достигали точки назначения, они всегда будут собраны в изначально заданной последовательности. Порядковый номер первого байта данных в передаваемом сегменте называется порядковым номером сегмента. Нумерация проводится "с головы состава", т. е. от заголовка пакета. TCP-пакет также содержит "подтверждающий номер" (acknowledgment number), который представляет собой номер следующего ожидаемого пакета данных передачи в обратном направлении. Иными словами, номер обозначает: "до сих пор я все получил". Механизм с использованием "подтверждающего номера" позволяет исключать дублирование пакетов при повторной отправке недоставленных данных.

Кроме определения порядка следования информационных пакетов, "порядковый номер" играет большую роль в механизме синхронизации соединения и контроле потерянных пакетов при разрывах соединения. Однако необходимо помнить, что величина счетчика - нумератора все же ограничена. Пакеты могут нумероваться числами от 0 до 2(32-1). Таким образом, все арифметические операции со счетчиком пакетов производятся по модулю 232. Это не означает, что гнезда, в процессе соединения, могут обмениваться только ограниченным количеством пакетов. Поскольку в процессе обмена получатель и отправитель знают предыдущий, последующий номера пакетов и длину пакета, а эти величины хранятся в структуре ТСВ при образовании соединения, все операции сравнения по модулю 232 проводятся корректно.

Здесь стоит сказать несколько слов о механизме предотвращения появления в сети пакетов с одинаковыми номерами. Они могут появиться, например, при установлении и быстром сбросе соединения или при сбросе соединения и его быстром восстановлении, т. е. когда номер испорченного пакета может сразу использоваться новым пакетом данных. Механизм предотвращения подобных ситуаций основан на генерировании начального числа последовательности пакетов, а поскольку счетчик циклический, то не все ли равно, с какого места начинать отсчет.

Так, при установлении нового соединения генерируется 32-битное число ISN (Initial Sequence Number). Генератор использует 32 младших разряда машинного таймера, который меняется каждые 4 микросекунды (полный цикл - 4,55 часа). Это число и служит отсчетом нумератора пакетов. Кроме того, каждая дейтаграмма в сети имеет ограниченное время жизни MSL - Maximum Life Time, которое значительно меньше периода генератора. Таким образом, в сети гарантируется невозможность возникновения конфликтов пакетов с одинаковыми номерами.

Поврежденные пакеты отсеиваются механизмом проверки величины контрольной суммы данных, которая размещается в каждом передаваемом пакете.

### Механизм контроля потока данных

Протокол TCP позволяет получателю последовательности пакетов регулировать передаваемый отправителем поток данных. Этот механизм основан на том, что при передаче флага подтверждения получения пакета (АСК) в ТСР-сегменте передается размер буфера данных, который может быть передан отправителем, не дожидаясь разрешения на отправку очередной порции данных от получателя. Иными словами - передается размер свободного места в стеке протокола, куда записываются только что принятые и ожидающие дальнейшей обработки данные. Из стека данные обрабатываются и передаются соответствующим процессам. Этот механизм позволяет избегать "пробок" при передаче данных между системами различной производительности.

"Окно" задается в количестве байт, отсчитываемых от номера байта, заданного в поле номера пакета "подтвержденного получения" (acknowledgment number) данных. Нулевой размер окна означает для отправителя команду приостановить передачу до готовности принимать данные получателем. Необходимо заметить, что в этом случае отправитель посылает однобайтные пакеты и на основании информации пакетов подтверждения возобновляет или нет дальнейшую передачу данных.

Безусловно, большой размер окна позволяет передавать данные быстрее, поскольку отправителю пакета не нужно ждать сигнала готовности приема от получателя. Однако в случае сбоя передачи, соответственно, возрастет объем данных, которые нужно отправить заново. При небольшом же размере окна сбойные сегменты данных можно локализовать с минимальными потерями.

Механизм контроля потока данных позволяет TCP влиять на изменение размера "окна" передачи. Это, в свою очередь, помогает значительно оптимизировать скорость достоверного обмена данных между процессами в гетерогенных сетях Internet.

### Флаг важности пакета, средства обеспечения безопасности протокола

Протокол TCP наследует все параметры секретности и приоритетности пакета, используемые IP и позволяет работать с ними для обеспечения собственной безопасности. В TCP-спецификации термин "секретность и изолированность" обозначает безопасность соединения, изолированность потоков данных и другие ограничения, которые обеспечивает IP.

Кроме того, TCP поддерживает некоторые дополнительные механизмы, которые поддерживаются специальным аппаратным и программным обеспечением TCP.

Для того чтобы TCP мог полностью реализовать свои возможности работы с иерархией приоритетных пакетов и информацией различного уровня секретности, необходима также поддержка этих возможностей и со стороны протоколов высокого уровня, и самих пользовательских приложений, и операционных систем.

Кроме наследуемых от IP-параметров, TCP имеет в своем распоряжении механизм работы с флагом важности пакетов - URG. Этот механизм позволяет отправителю "настоятельно сообщать" получателю о том, что тот или иной пакет содержит срочную информацию и позволяет получателю сигнализировать, когда вся срочная информация им получена. Такой механизм уведомления, т. е. манипулирование с URG-флагом TCP-пакета используется, например, при обработке асинхронных событий.

### Состав и предназначение полей заголовка

ТСР-сегменты отправляются как IP-дейтаграммы. Заголовок TCP, следующий за IP-заголовком, содержит информацию TCP-протокола (рис. 2.13).

**Source Port** (16 бит). Порт отправителя.

**Destination Port** (16 бит). Порт получателя.

**Sequence Number** (32 бита). Номер кадра. Номер кадра первого октета данных в этом сегменте (за исключением пакета, где присутствует флаг SYN). Если в пакете присутствует флаг SYN, то номер данного пакета становится номером начала последовательности (ISN) и номером первого октета данных становится номер ISN+1.

**Acknowledgment Number** (32 бита). Поле номера кадра подтвержденного получения. Если пакет содержит установленный контрольный бит АСК, то это поле содержит номер следующего пакета данных отправителя, который ожидает получатель. При установленном соединении пакет подтверждения отправляется всегда.

**Data Offset** (4 бита). Поле величины смещения данных. Оно содержит количество 32-битных слов заголовка TCP-пакета. Это число определяет смещение расположения данных в пакете.

**Reserved** (6 бит). Резервное поле. Поле зарезервировано.

Флаги управления (слева направо):

URG: Флаг срочности
АСК: Флаг пакета, содержащего подтверждение получения
PSH: Флаг форсированной отправки
RST: Переустановка соединения
SYN: Синхронизация чисел последовательности
FIN: Флаг окончания передачи со стороны отправителя

**Window** (16 бит). Окно. Это поле содержит количество байт данных, которое отправитель данного сегмента может принять, отсчитанное от номера байта, указанного в поле Acknowledgment Number.

**Checksum** (16 бит). Поле контрольной суммы. Это поле содержит 16 бит суммы побитных дополнений 16-битных слов заголовка и данных. Если сегмент содержит нечетное число байт заголовка и данных, последний байт дополняется справа нулями. При вычислении контрольной суммы поле контрольной суммы полагается равным нулю.

**Urgent Pointer** (16 бит). Поле указателя срочных данных. Это поле содержит значение счетчика пакетов, начиная с которого следуют пакеты повышенной срочности. Это поле принимается во внимание только в сегментах с установленным флагом URG.

**Options**. Поле дополнительных параметров: может быть переменной длины.

**Padding.** Заполнение: переменная длина. Заполнение (нулями) TCP-заголовка используется для выравнивания его по 32-битному слову.

### Псевдозаголовок

Между TCP-заголовком и IP-заголовком располагается так называемый псевдозаголовок (рис. 2.14). Он состоит из IP-адреса отправителя (Source Address), IP-адреса получателя (Destination Address), типа протокола (PTCL) и длины TCP-пакета (TCP Length). Он предназначен для "страховки" неправильной маршрутизации TCP-пакета. Информация, расположенная в этом заголовке передается TCP от IP-протокола как аргумент или результат обработки вызова IP-функции.

Более подробное описание протокола TCP можно найти в RFC-793, RFC-1180.

**1.2 Адресация в сети Internet.**

**1.2.1 Типы адресов.**

Типы адресов:

1. **Физический (MAC-адрес)**
2. **Сетевой (IP-адрес)**
3. **Символьный (DNS-имя)**

Компьютер в сети TCP/IP может имееть адреса трех уровней (но не менее двух):

* Локальный адрес компьютера. Для узлов, входящих в локальные сети - это МАС-адрес сетевого адаптера. Эти адреса назначаются производителями оборудования и являются уникальными адресами.
* 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.
* Символьный идентификатор-имя (DNS), например, [www.kstu.ru](http://www.kstu.ru).

**1.2.2 IP-адреса**

**IPv4** - адрес является уникальным 32-битным идентификатором IP-интерфейса в Интернет.

**IPv6** - адрес является уникальным 128-битным идентификатором IP-интерфейса в Интернет, иногда называют **Internet-2,** адресного пространства IPv4 уже стало не хватать, поэтому постепенно вводят новый стандарт.

IP-адреса принято записывать разбивкой всего адреса по октетам (8), каждый октет записывается в виде десятичного числа, числа разделяются точками. Например, адрес

10100000010100010000010110000011
записывается как

10100000.01010001.00000101.10000011 = 160.81.5.131



Перевод адреса из двоичной системы в десятичную

IP-адрес хоста состоит из номера IP-сети, который занимает старшую область адреса, и номера хоста в этой сети, который занимает младшую часть.

160.81.5.131 - IP-адрес

160.81.5. - номер сети

131 -  номер хоста

**1.3 Базовые протоколы (IP, TCP, UDP)**

**1.3.1 Стек протоколов TCP/IP**

TCP/IP - собирательное название для набора (стека) сетевых протоколов разных уровней, используемых в Интернет. Особенности TCP/IP:

* Открытые стандарты протоколов, разрабатываемые независимо от программного и аппаратного обеспечения;
* Независимость от физической среды передачи;
* Система уникальной адресации;
* Стандартизованные протоколы высокого уровня для распространенных пользовательских сервисов.



Стек протоколов TCP/IP

Стек протоколов TCP/IP делится на 4 уровня:

* Прикладной,
* Транспортный,
* Межсетевой,
* Физический и канальный.

Позже была принята 7-ми уровневая модель ISO, но она не используется.

Данные передаются в пакетах. Пакеты имеют заголовок и окончание, которые содержат служебную информацию. Данные,  более верхних уровней вставляются, в пакеты нижних уровней.



Пример инкапсуляции пакетов в стеке TCP/IP

**1.3.2 Физический и канальный уровень.**

Стек TCP/IP не подразумевает использования каких-либо определенных протоколов уровня доступа к среде передачи и физических сред передачи данных. От уровня доступа к среде передачи требуется наличие интерфейса с модулем IP, обеспечивающего передачу IP-пакетов. Также требуется обеспечить преобразование IP-адреса узла сети, на который передается IP-пакет, в MAC-адрес. Часто в качестве уровня доступа к среде передачи могут выступать целые протокольные стеки, тогда говорят об IP поверх ATM, IP поверх IPX, IP поверх X.25 и т.п.

**1.3.3 Межсетевой уровень и протокол IP.**

Основу этого уровня составляет IP-протокол.

**IP (Internet Protocol)** – интернет протокол.

Первый стандарт IPv4 определен в RFC-760 (DoD standard Internet Protocol J. Postel Jan-01-1980)

Последняя версия IPv4 - [RFC-791](http://www.ipm.kstu.ru/it/doc/rfc/rfc791.txt) (Internet Protocol J. Postel Sep-01-1981).

Первый стандарт IPv6 определен в RFC-1883 (Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden December 1995)

Последняя версия IPv6 - [RFC-2460](http://www.ipm.kstu.ru/it/doc/rfc/rfc2460.txt) (Internet Protocol, Version 6 (IPv6) Specification S. Deering, R. Hinden December 1998).

Основные задачи:

* Адресация
* Маршрутизация
* Фрагментация датаграмм
* Передача данных

Протокол IP доставляет блоки данных от одного IP-адреса к другому.

 *Программа, реализующая функции того или иного протокола, часто называется модулем, например, “IP-модуль”, “модуль TCP”.*

Когда модуль IP получает IP-пакет с нижнего уровня, он проверяет IP-адрес назначения.

* Если IP-пакет адресован данному компьютеру, то данные из него передаются на обработку модулю вышестоящего уровня (какому конкретно - указано в заголовке IP-пакета).
* Если же адрес назначения IP-пакета - чужой, то модуль IP может принять два решения: первое - уничтожить IP-пакет, второе - отправить его дальше к месту назначения, определив маршрут следования - так поступают маршрутизаторы.

Также может потребоваться, на границе сетей с различными характеристиками, разбить IP-пакет на фрагменты

(**фрагментация**), а потом собрать в единое целое на компьютере-получателе.

Если модуль IP по какой-либо причине не может доставить IP-пакет, он уничтожается. При этом модуль IP может отправить компьютеру-источнику этого IP-пакета уведомление об ошибке; такие уведомления отправляются с помощью протокола **ICMP**, являющегося неотъемлемой частью модуля IP. Более никаких средств контроля корректности данных, подтверждения их доставки, обеспечения правильного порядка следования IP-пакетов, предварительного установления соединения между компьютерами протокол IP не имеет. Эта задача возложена на транспортный уровень.



Структура дейтограммы IP. Слова по 32 бита.

**Версия -** версия протокола IP (например, 4 или 6)

**Длина заг.** - длина заголовка IP-пакета.

**Тип сервиса** (TOS - type of service) - Тип сервиса (подробнее рассмотрен в лекции 8).

TOS играет важную роль в маршрутизации пакетов. Интернет не гарантирует запрашиваемый TOS, но многие маршрутизаторы учитывают эти запросы при выборе маршрута (протоколы OSPF и IGRP).

**Идентификатор дейтаграммы, флаги (3 бита)  и указатель фрагмента** - используются для распознавания пакетов, образовавшихся путем  фрагментации исходного пакета.

**Время жизни (TTL - time to live)** - каждый маршрутизатор уменьшает его на 1, что бы пакеты не блуждали вечно.

**Протокол** - Идентификатор протокола верхнего уровня указывает, какому протоколу верхнего уровня принадлежит пакет (например: TCP, UDP).

Коды некоторые протоколов  [RFC-1700](http://www.ipm.kstu.ru/it/doc/rfc/rfc1700.txt)  (1994)

|  |  |  |
| --- | --- | --- |
| **Код** | **Протокол** | **Описание**  |
| 0 | - | Зарезервировано  |
| 1 | ICMP | Протокол контрольных сообщений |
| 2 | IGMP | Групповой протокол управления |
| 4 | IP | IP-поверх-IP (туннели)  |
| 6 | TCP | Протокол управления передачей |
| 8 | EGP | Протокол внешней маршрутизации |
| 9 | IGP | Протокол внутренней маршрутизации  |
| 17 | UDP | Протокол дейтограмм пользователя |
| 35 | IDRP | Междоменный протокол маршрутизации  |
| 36 | XTP | Xpress транспортный протокол  |
| 46 | RSVP | Протокол резервирования ресурсов канала |
| 88 | IGRP | внутренний протокол маршрутизации |
| 89 | OSPFIGP | внутренний протокол маршрутизации  |
| 97 | ETHERIP | Ethernet-поверх-IP |
| 101-254 | - | не определены |
| 255 | - | зарезервировано  |

1.3.3.1 Маршрутизация.

Протокол IP является маршрутизируемый, для его маршрутизации нужна маршрутная информация.

Маршрутная информация, может быть:

* Статической (маршрутные таблицы прописываются вручную)
* Динамической (маршрутную информацию распространяют специальные протоколы)

Протоколы динамической маршрутизации:

* RIP (Routing Information Protocol) - протокол передачи маршрутной информации, маршрутизаторы динамически создают маршрутные таблицы.
* OSPF (Open Shortest Path First) - протокол "Открой кротчайший путь первым", является внутренним протоколом маршрутизации.
* IGP (Interior Gateway Protocols) - внутренние протоколы маршрутизации, распространяет маршрутную информацию внутри одной автономной системе.
* EGP (Exterior Gateway Protocols) - внешние протоколы маршрутизации, распространяет маршрутную информацию между автономными системами.
* BGP (Border Gateway Protocol) - протокол граничных маршрутизаторов.

1.3.3.2 Протокол ICMP

**ICMP (Internet Control Message Protocol)** - расширение протокола IP, позволяет передавать сообщения об ошибке или проверочные сообщения.

1.3.3.3 Другие служебные IP-протоколы

IGMP (Internet Group Management Protocol) - позволяет организовать многоадресную рассылку средствами IP.

RSVP (Resource Reservation Protocol) - протокол резервирования ресурсов.

ARP (Address Resolution Protocol) - протокол преобразования IP-адреса и адреса канального уровня.

**1.3.4 Транспортный уровень**

Протоколы транспортного уровня обеспечивают прозрачную доставку данных между двумя прикладными процессами. Процесс, получающий или отправляющий данные с помощью транспортного уровня, идентифицируется на этом уровне номером, который называется номером порта. Таким образом, роль адреса отправителя и получателя на транспортном уровне выполняет номер порта (или проще - порт).

Анализируя заголовок своего пакета, полученного от межсетевого уровня, транспортный модуль определяет по номеру порта получателя, какому из прикладных процессов направлены данные, и передает эти данные соответствующему прикладному процессу. Номера портов получателя и отправителя записываются в заголовок транспортным модулем, отправляющим данные; заголовок транспортного уровня содержит также и другую служебную информацию; формат заголовка зависит от используемого транспортного протокола.

На транспортном уровне работают два основных протокола: UDP и TCP.

1.3.4.1 Протокол надежной доставки сообщений TCP

**TCP (Transfer Control Protocol)** – протокол контроля передачи, протокол TCP применяется в тех случаях, когда требуется гарантированная доставка сообщений.

Первая и последняя версия TCP - [RFC-793](http://www.ipm.kstu.ru/it/doc/rfc/rfc793.txt) (Transmission Control Protocol J. Postel Sep-01-1981).

Основные особенности:

* Устанавливается соединение.
* Данные передаются **сегментами**. Модуль TCP нарезает большие сообщения (файлы) на пакеты, каждый из которых передается отдельно, на приемнике наоборот файлы собираются. Для этого нужен **порядковый номер (Sequence Number - SN)** пакета.
* Посылает запрос на следующий пакет, указывая его номер в поле **"Номер подтверждения" (AS).** Тем самым, подтверждая получение предыдущего пакета.
* Делает проверку целостности данных, если пакет битый посылает повторный запрос.



Структура дейтограммы TCP. Слова по 32 бита.

**Длина заголовка -** задается словами по 32бита.

**Размер окна** - количество байт, которые готов принять получатель без подтверждения.

**Контрольная сумма** - включает псевдо заголовок, заголовок и данные.

**Указатель срочности** - указывает последний байт срочных данных, на которые надо немедленно реагировать.

**URG -** флаг срочности, включает поле "Указатель срочности", если =0 то поле игнорируется.

**ACK -** флаг подтверждение, включает поле "Номер подтверждения, если =0 то поле игнорируется.

**PSH -** флаг требует выполнения операции push, модуль TCP должен срочно передать пакет программе.

**RST -** флаг прерывания соединения, используется для отказа в соединении

**SYN -** флаг синхронизация порядковых номеров, используется при установлении соединения.

**FIN -** флаг окончание передачи со стороны отправителя

1.3.4.2 Протокол UDP

**UDP (Universal Datagram Protocol)** **-** универсальный протокол передачи данных, более облегченный транспортный протокол, чем TCP.

Первая и последняя версия UDP - [RFC-768](http://www.ipm.kstu.ru/it/doc/rfc/rfc768.txt) (User Datagram Protocol J. Postel Aug-28-1980).

Основные отличия от TCP:

* Отсутствует соединение между модулями UDP.
* Не разбивает сообщение для передачи
* При потере пакета запрос для повторной передачи не посылается

UDP используется если не требуется гарантированная доставка пакетов , например, для потокового видео и аудио, DNS (т.к. данные небольших размеров). Если проверка контрольной суммы выявила ошибку или если процесса, подключенного к требуемому порту, не существует, пакет игнорируется (уничтожается). Если пакеты поступают быстрее, чем модуль UDP успевает их обрабатывать, то поступающие пакеты также игнорируются.



Структура дейтограммы UDP. Слова по 32 бита.

Не все поля UDP-пакета обязательно должны быть заполнены. Если посылаемая дейтаграмма не предполагает ответа, то на месте адреса отправителя могут помещаться нули.

1.3.4.2 Протокол реального времени RTP

**RTP (Real Time Protocol)** - транспортный протокол для приложений реального времени.

**RTCP (Real Time Control Protocol)** - транспортный протокол обратной связи для приложения RTP..

**1.4 Назначение портов**

По номеру порта транспортные протоколы определяют, какому приложению передать содержимое пакетов.

Порты могут принимать значение от 0-65535 (два байта 2^16).

Номера портам присваиваются таким образом: имеются стандартные номера (например, номер 21 закреплен за сервисом FTP, 23 - за telnet, 80 - за HTTP), а менее известные приложения пользуются произвольно выбранными локальными номерами (как правило, больше>1024), некоторые из них также зарезервированы.

Некоторые заданные порты  [RFC-1700](http://www.ipm.kstu.ru/it/doc/rfc/rfc1700.txt)  (1994)

|  |  |  |
| --- | --- | --- |
| **Порт** | **Служба** | **Описание**  |
| 0 | - | Зарезервировано |
| 13 | Daytime | Синхронизация времени |
| 20 | ftp-data | Канал передачи данных для FTP |
| 21 | ftp | Передача файлов |
| 23 | telnet | Сетевой терминал |
| 25 | SMTP | Передача почты |
| 37 | time | Синхронизация времени |
| 43 | Whois | Служба Whois |
| 53 | DNS | Доменные имена |
| 67 | bootps  | BOOTP и DHCP - сервер |
| 68 | bootps  | BOOTP и DHCP - клиент |
| 69 | tftp | Упрощенная передача почты |
| 80 | HTTP | Передача гипертекста |
| 109 | POP2 | Получение почты |
| 110 | POP3 | Получение почты |
| 119 | NNTP | Конференции |
| 123 | NTP | Синхронизация времени |
| 137 | netbios-ns | NETBIOS - имена |
| 138 | netbios-dgm | NETBIOS Datagram Service |
| 139 | netbios-ssn | NETBIOS Session Service |
| 143 | imap2 | Получение почты |
| 161 | SNMP | Протокол управления |
| 210 | z39.50 | Библиотечный протокол |
| 213 | IPX  | IPX - протокол |
| 220 | imap3 | Получение почты |
| 443 | HTTPs | HTTP  с шифрованием |
| 520 | RIP | Динамическая маршрутизация |
| **Диапазон 1024-65535** |
| 1024 | - | Зарезервировано |
| 6000-6063 | X11 | Графический сетевой терминал |

**Опции IP-протокола**



Рис. 4.4.1.2. Формат описания опций

Флаг *копия* равный 1 говорит о том, что опция должна быть скопирована во все фрагменты дейтограммы. При равенстве этого флага 0 опция копируется только в первый фрагмент. Ниже приведены значения разрядов 2-битового поля *класс опции*:

|  |  |
| --- | --- |
| Значение поля *класс опции*  | Описание |
| 0 | Дейтограмма пользователя или сетевое управление |
| 1 | Зарезервировано для будущего использования |
| 2 | Отладка и измерения (диагностика) |
| 3 | Зарезервировано для будущего использования |

В таблице, которую вы найдете ниже, приведены значения классов и номеров опций.

|  |  |  |  |
| --- | --- | --- | --- |
| Класс опции | Номер опции | Длина описания | Назначение |
| 0 | 0 | - | Конец списка опций. Используется, если опции не укладываются в поле заголовка (смотри также поле "заполнитель") |
| 0 | 1 | - | Никаких операций (используется для выравнивания октетов в списке опций) |
| 0 | 2 | 11 | Ограничения, связанные с секретностью (для военных приложений) |
| 0 | 3 | \* | Свободная маршрутизация. Используется для того, чтобы направить дейтограмму по заданному маршруту |
| 0 | 7 | \* | Запись маршрута. Используется для трассировки |
| 0 | 8 | 4 | Идентификатор потока. Устарело. |
| 0 | 9 | \* | Жесткая маршрутизация. Используется, чтобы направить дейтограмму по заданному маршруту |
| 2 | 4 | \* | Временная метка Интернет |

\* в колонке "длина" - означает - переменная.

Наибольший интерес представляют собой опции *временные метки* и *маршрутизация*. Опция *записать маршрут* (RR) создает дейтограмму, где зарезервировано место, куда каждый маршрутизатор по дороге должен записать свой IP-адрес (например, утилита traceroute). Формат опции *записать маршрут* в дейтограмме представлен ниже на рис. 4.4.1.3 (предусмотрено место для записи 9 IP-адресов, к сожаления, реализация RR не является обязательной):



Рис. 4.4.1.3 Формат опций *записать маршрут*

Поле *код* содержит номер опции (7 в данном случае). Поле *длина* определяет размер записи для опций, включая первые 3 октета. *Указатель* отмечает первую свободную позицию в списке IP-адресов (куда можно произвести запись очередного адреса). Интересную возможность представляет опция *маршрут отправителя*, которая открывает возможность посылать дейтограммы по заданному отправителем маршруту. Это позволяет исследовать различные маршруты, в том числе те, которые недоступны через узловые маршрутизаторы. Существует две формы такой маршрутизации: *Свободная маршрутизация* и *Жесткая маршрутизация* (маршрутизация отправителя). Форматы для этих опций показаны ниже:



Рис. 4.4.1.3а. Формат опций маршрутизации

*Жесткая маршрутизация* означает, что адреса определяют точный маршрут дейтограммы. Проход от одного адреса к другому может включать только одну сеть. *Свободная маршрутизация* отличается от предшествующей возможностью прохода между двумя адресами списка более чем через одну сеть. Поле *длина* задает размер списка адресов, а *указатель* отмечает адрес очередного маршрутизатора на пути дейтограммы.

IP-слой имеет маршрутные таблицы, которые просматриваются каждый раз, когда IP получает дейтограмму для отправки. Когда дейтограмма получается от сетевого интерфейса, IP первым делом проверяет, принадлежит ли IP-адрес места назначения к списку локальных адресов, или является широковещательным адресом. Если имеет место один из этих вариантов, дейтограмма передается программному модулю в соответствии с кодом в поле протокола. IP-процессор может быть сконфигурирован как маршрутизатор, в этом случае дейтограмма может быть переадресована в другой узел сети. Маршрутизация на IP-уровне носит пошаговый характер. IP не знает всего пути, он владеет лишь информацией - какому маршрутизатору послать дейтограмму с конкретным адресом места назначения.

Просмотр маршрутной таблицы происходит в три этапа:

1. Ищется полное соответствие адресу места назначения. В случае успеха, пакет посылается соответствующему маршрутизатору или непосредственно интерфейсу адресата. Связи точка-точка выявляются именно на этом этапе.
2. Ищется соответствие адресу сети места назначения. В случае успеха система действует также как и в предшествующем пункте. Одна запись в таблице маршрутизации соответствует всем ЭВМ, входящим в данную сеть.
3. Осуществляется поиск маршрута по умолчанию и, если он найден, дейтограмма посылается в соответствующий маршрутизатор.

Для того чтобы посмотреть, как выглядит простая маршрутная таблица, воспользуемся командой netstat -rn (ЭВМ Sun. Флаг -r выводит на экран маршрутную таблицу, а -n отображает IP-адреса в цифровой форме. С целью экономии места таблица в несколько раз сокращена).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| routing tables destination | gateway | flags | refcnt | use | interface |
| 193.124.225.72 | 193.124.224.60 | ughd | 0 | 61 | le0 |
| 192.148.166.1 | 193.124.224.60 | ughd | 0 | 409 | le0 |
| 193.124.226.81 | 193.124.224.37 | ughd | 0 | 464 | le0 |
| 192.160.233.201 | 193.124.224.33 | ughd | 0 | 222 | le0 |
| 192.148.166.234 | 193.124.224.60 | ughd | 1 | 3248 | le0 |
| 193.124.225.66 | 193.124.224.60 | ughd | 0 | 774 | le0 |
| 192.148.166.10 | 193.124.224.60 | ughd | 0 | 621 | le0 |
| 192.148.166.250 | 193.124.224.60 | ughd | 0 | 371 | le0 |
| 192.148.166.4 | 193.124.224.60 | ughd | 0 | 119 | le0 |
| 145.249.16.20 | 193.124.224.60 | ughd | 0 | 130478 | le0 |
| 192.102.229.14 | 193.124.224.33 | ughd | 0 | 13206 | le0 |
| default | 193.124.224.33 | ug | 9 | 5802624 | le0 |
| 193.124.224.32 | 193.124.224.35 | u | 6 | 1920046 | le0 |
| 193.124.134.0 | 193.124.224.50 | ugd | 1 | 291672 | le0 |

Колонка destination - место назначение, Default - отмечает маршрут по умолчанию; Gateway - IP-адреса портов подключения (маршрутизаторов); REFCNT (reference count) - число активных пользователей маршрута; USE - число пакетов, посланных по этому маршруту; interface - условные имена сетевых интерфейсов. Расшифровка поля FLAGS приведено ниже:

|  |  |
| --- | --- |
| u | Маршрут работает (up). |
| g | Путь к маршрутизатору (gateway), если этот флаг отсутствует, адресат доступен непосредственно. |
| h | Маршрут к ЭВМ (host), адрес места назначения является полным адресом этой ЭВМ (адрес сети + адрес ЭВМ). Если флаг отсутствует, маршрут ведет к сети, а адрес места назначения является адресом сети. |
| d | Маршрут возник в результате переадресации. |
| m | Маршрут был модифицирован с помощью переадресации. |

Опция *временные метки* работает также как и опция *запись маршрута*. Каждый маршрутизатор на пути дейтограммы делает запись в одном из полей дейтограммы (два слова по 32 разряда; смотри раздел [4.4.15](http://book.itep.ru/4/44/ntp_4415.htm)). Формат этой опции отображен на рисунке 4.4.1.4.



Рис. 4.4.1.4 Формат опции "временные метки"

Смысл полей ***длина*** и ***указатель*** идентичен тому, что сказано о предыдущих опциях. 4-битовое поле ***переполнение*** содержит число маршрутизаторов, которые не смогли записать временные метки из-за ограничений выделенного места в дейтограмме. Значения поля ***флаги*** задают порядок записи временных меток маршрутизаторами:

Таблица 4.4.1.3.

|  |  |
| --- | --- |
| **Значение флага** | **Назначение** |
| 0 | Записать только временные метки; опустить IP-адреса. |
| 1 | Записать перед каждой временной меткой IP-адрес (как в формате на предыдущем рисунке). |
| 3 | IP-адреса задаются отправителем; маршрутизатор записывает только временные метки, если очередной IP-адрес совпадает с адресом маршрутизатора |

Временные метки должны содержать время в миллисекундах, отсчитанное от начала суток. Если маршрутизатору некуда положить свою временную метку (число меток превысило 9), он инкрементирует счетчик ***переполнение***.

Взаимодействие других протоколов с IP можно представить из схемы на рис. 4.4.1.5. В основании лежат протоколы, обеспечивающие обмен информацией на физическом уровне, далее следуют протоколы IP, ICMP, ARP, RARP, IGMP и протоколы маршрутизаторов. Чем выше расположен протокол, тем более высокому уровню он соответствует. Протоколы, имена которых записаны в одной и той же строке, соответствуют одному и тому же уровню. Но все разложить аккуратно по слоям невозможно - некоторые протоколы занимают промежуточное положение, что и отражено на схеме, (области таких протоколов захватывают два уровня. Здесь протоколы IP, ICMP и IGMP помещены на один уровень, для чего имеется не мало причин. Но иногда последние два протокола помещают над IP, так как их пакеты вкладываются в IP-дейтограммы. Так что деление протоколов по уровням довольно условно. На самом верху пирамиды находятся прикладные программы, хотя пользователю доступны и более низкие уровни (например, ICMP), что также отражено на приведенном рисунке (4.4.1.5).

**Формат TCP-сегмента**



Рис. 4.4.3.1 Формат TCP-сегмента

Поле ***опции*** зарезервировано на будущее и в заголовке может отсутствовать, его размер переменен и дополняется до кратного 32-бит с помощью поля *заполнитель*. Формат поля ***опции*** представлен на рис. 4.4.3.2. В настоящее время определены опции:

0   Конец списка опций.
1   Никаких операций. Используется для заполнения поля опции до числа октетов, кратного 4.
2   Максимальный размер сегмента (MSS).

В поле ***вид*** записывается код опции, поле ***LEN*** содержит число октетов в описании опции, включая поля *вид* и *LEN*. Определены также опции со значением вид=4,5,6,7. В предложении T/TCP (RFC-1644) описаны опции 11, 12 и 13. Поле ***данные*** может иметь переменную длину, верхняя его граница задается значением **MSS** (Maximum Segment Size). Значение MSS может быть задано при установлении соединения каждой из сторон независимо. Для Ethernet MSS=1452 байта.

**Формат опций для TCP-сегментов**



Рис. 4.4.3.2. Формат опций для TCP-сегментов

Поле *данные* в TCP-сегменте может и отсутствовать, характер и формат передаваемой информации задается исключительно прикладной программой, теоретически максимальный размер этого поля составляет в отсутствии опций 65495 байт (на практике, помимо MSS, нужно помнить, например, о значении MTU для Ethernet, которое немногим больше 1500 байт). TCP является протоколом, который ориентируется на согласованную работу ЭВМ и программного обеспечения партнеров, участвующих в обмене информацией. Установление связи клиент-сервер осуществляется в три этапа:

1. Клиент посылает SYN-сегмент с указанием номера порта сервера, который предлагается использовать для организации канала связи (active open).
2. Сервер откликается, посылая свой SYN-сегмент, содержащий идентификатор (**ISN** - Initial Sequence Number). Начальное значение ISN не равно нулю. Процедура называется *passive open*.
3. Клиент отправляет подтверждение получения SYN-сегмента от сервера с идентификатором равным ISN (сервера)+1.

Стандартная процедура установления связи представлена на рисунке 4.4.3.3 (под словом “стандартная” подразумевается отсутствие каких-либо отклонений от штатного режима, например, одновременного открывание соединения со стороны сервера и клиента). Если же соединение одновременно инициируется клиентом и сервером, в конечном итоге будет создан только один виртуальный канал.



Рис. 4.4.3.3. Алгоритм установления связи. В рамках представлены состояния клиента и сервера; пунктиром отмечены изменения cостояния после посылки сообщения (см. также рис. 4.4.3.4)

Префикс **S** на рисунке указывает на сервер, а **С** - на клиента. Параметры в скобках обозначают относительные значения ISN. После установления соединения ISN(S) = s\_seq\_1, а ISN(C) = c\_seq\_1.

Каждое соединение должно иметь свой неповторимый код ISN. Для реализации режима соединения прикладная программа на одном конце канала устанавливается в режим пассивного доступа ("passive open"), а операционная система на другом конце ставится в режим активного доступа ("active open"). Протокол TCP предполагает реализацию 11 состояний (established, closed, listen, syn\_sent, syn\_received и т.д.; см. также RFC-793), переход между которыми строго регламентирован. Машина состояний для протокола TCP может быть описана диаграммой, представленной на рис. 4.4.3.4. Здесь состояние closed является начальной и конечной точкой последовательности переходов. Каждое соединение стартует из состояния closed. Из диаграммы машины состояний видно, что ни одному из состояний не поставлен в соответствие какой-либо таймер. Это означает, что машина состояний TCP может оставаться в любом из состояний сколь угодно долго. Исключение составляет keep-alive таймер, но его работа является опционной, а время по умолчанию составляет 2 часа. Это означает, что машина состояния может оставаться 2 часа без движения. В случае, когда две ЭВМ (C и S) попытаются установить связь друг с другом одновременно, реализуется режим simultaneous connection (RFC-793). Обе ЭВМ посылают друг другу сигналы SYN. При поучении этого сигнала партнеры посылают отклики SYN+ACK. Обе ЭВМ должны обнаружить, что SYN и SYN+ACK относятся к одному и тому же соединению. Когда C и S обнаружат, что SYN+ACK соответствует посланному ранее SYN, они выключат таймер установления соединения и перейдут непосредственно в состояние syn\_recvd (смотри рис. 4.4.3.4).

В состоянии established пакет будет принят сервером, если его ISN лежит в пределах s\_ack, s\_ack+s\_wind (s\_wind - ширина окна для сервера; см. рис. 4.4.3.5). Аналогичный диапазон ISN для клиента выглядит как: c\_ack, c\_ack+c\_wind (c\_wind - ширина окна для клиента). c\_wind и s\_wind могут быть не равны. *Пакеты, для которых эти условия не выполняются, будут отброшены*.

Рассмотрим пример установления соединения для случая FTP-запроса (См. также [http://www.cis.ohio-state.edu/~dolske/gradwork/cis694q](http://www.cis.ohio-state.edu/~dolske/gradwork/cis694q/)). Пусть клиент **С** запускает процесс установления FTP-соединения с сервером **s**. Обычный порядок установления соединения показан ниже (см. рис. 4.4.3.3):

c -> s:syn(ISNc)
s -> c:syn(ISNs), ack(ISNc)
c -> s: ack(ISNs) (Связь установлена)
c -> s: данные
и/или
s -> c: данные

ISN - идентификатор пакета, посылаемого клиентом (С) или сервером (S). Клиент, послав SYN серверу S, переходит в состояние *syn\_sent*. При этом запускается таймер установления соединения.

|  |
| --- |
| Как при установлении соединения, так и при его разрыве приходится сталкиваться с проблемой двух армий. Представим себе, что имеется две армии А и Б, причем Б больше по численности чем А. Армия Б разделена на две части, размещенные по разные стороны от армии А. Если две части армии Б одновременно нападут на армию А, победа гарантирована. В то же время нападение на А одной из частей армии Б обрекает ее на поражение. Но как обеспечить одновременность? Здесь предполагается, что радио еще не изобретено и передача сообщений осуществляется вестовыми, которые в нашем случае могут быть перехвачены врагом. Как убедиться, что вестовой дошел? Первое, что приходит в голову, это послать другого вестового с подтверждением. Но он также с некоторой вероятностью может быть перехвачен. А отправитель не будет знать, дошел ли он. Ведь если сообщение перехвачено, отправитель первичного запроса не выдаст команды на начало, так как не уверен, дошло ли его первое сообщение. Возникает вопрос, существует ли алгоритм, который бы гарантировал надежность синхронизации решений путем обмена сообщениями при ненадежной доставке? Повысит ли достоверность увеличение числа обменов между партнерами? Ответом на этот вопрос будет - нет, не существует. В этом читатель, порассуждав логически, может убедиться самостоятельно. Не трудно видеть, что схожие проблемы возникают в любом протоколе, работающем через установление соединения. Чаще всего эта проблема решается путем таймаутов и повторных попыток (это, слава богу, не война и все обходится без людских жертв). |

Сервер, получив **SYN**, откликается посылкой другого SYN. Когда **С** получает SYN от **S** (но не получает ACK, например, из-за его потери или злого умысла), он предполагает, что имеет место случай одновременного открытия соединения. В результате он посылает **syn\_ack**, отключает таймер установления соединения и переходит в состояние syn\_received. Сервер получает syn\_ack от C, но не посылает отклика. Тогда С ожидает получения syn\_ack в состоянии syn\_received. Так как время пребывания в этом состоянии не контролируется таймером, **С** может остаться в состоянии syn\_received вечно. Из-за того, что переходы из состояния в состояние не всегда четко определены, протокол TCP допускает и другие виды атак (некоторые из них описаны в разделе [“Сетевая безопасность”](http://book.itep.ru/6/secur_6.htm)), там же рассмотрены алгоритмы задания и изменения ISN.

Хотя TCP-соединение является полнодуплексным, при рассмотрении процесса разрыва связи проще его рассматривать как два полудуплексных канала, каждый из которых каналов ликвидируется независимо. Сначала инициатор разрыва посылает сегмент с флагом **FIN**, сообщая этим партнеру, что не намерен более что-либо передавать (FIN посылается, как правило в результате вызова приложением функции ***close***). Когда получение этого сегмента будет подтверждено (ACK), данное направление передачи считается ликвидированным (реализуется полузакрытие соединения). При этом передача информации в противоположном направлении может беспрепятственно продолжаться. Когда партнер закончит посылку данных, он также пошлет сегмент с флагом FIN. По получении отклика ACK виртуальный канал считается окончательно ликвидированным.

|  |
| --- |
| Таким образом, для установление связи требуется обмен тремя сегментами, а для разрыва - четырьмя. Но протокол допускает совмещение первого ACK и второго FIN в одном сегменте, сокращая полное число закрывающих сегментов с четырех до трех. |

Партнер, пославший флаг FIN первым, производит *активное закрытие соедиения*, а противоположный партнер (получивший FIN) отвечает на него своим FIN, осуществляя *пассивное закрытие соединения*. Инициатором посылки первого FIN может любая из сторон, но чаще это делается клиентом (например, путем ввода команды quit). Полузакрытие используется, например при реализации команды **rsh** (запуск операций в удаленном узле).

|  |
| --- |
| Машина состояний для протокола TCP не предусматривает изменения состояний при посылке или получении обычных пакетов, содержащих данные. |

Всего в машине конечных состояний протокола TCP имеется 11 состояний (CLOSED, LISTEN, SYN\_RCVD, SYN\_SENT и т.д., введены в RFC-793). Состояние CLOSED является начальной и конечной точкой диаграммы. ESTABLISHED указывает на то, что система находится в состоянии с установленным соединением. Четыре состояния в левом углу помещены в границы зеленой зоны и соответствуют активному закрытию. Состояния CLOSE\_WAIT и LAST\_ACK относятся к пассивному закрытию. Переход из состояния SYN\_RCVD в LISTEN возможно, если переход в SYN\_RCVD осуществлен из состояния LISTEN, а не из состояния SYN\_SENT (одновременное открытие двух соединений, получение RST вместо финального ACK).

**Некоторые проблемы ТСР**

Существуют и другие, могущие показаться забавными проблемы. Каждый сегмент в TCP-протоколе снабжается 32-битным идентификатором. Время жизни IP-пакета (TTL) определяется по максимуму 255 шагами или 255 секундами в зависимости оттого, что раньше наступит. Трудно предсказуемая ситуация может произойти, когда канал ликвидирован, затем создан снова (для той же комбинации IP-адресов и портов), а какой-то пакет из предшествующей сессии, погуляв по Интернет, придет уже во время следующей. Есть ли гарантия, что он будет верно идентифицирован? Одной из мер, упомянутых ранее, можно считать использование ограничения по максимальному времени жизни сегмента (**MSL**) или TTL, хотя снижение значения TTL не всегда возможно - ведь IP-пакетами пользуется не только TCP-протокол и нужна очень гибкая система задания его величины. Во многих приложениях MSL=30 сек (рекомендуемое значение 2 мин слишком велико). Технический прогресс ставит и некоторые новые проблемы. Высокопроизводительные каналы (1 Гбит/с) уже сегодня могут исчерпать разнообразие идентификационных кодов пакетов за один сеанс связи. Появление же двух пакетов с равными идентификаторами может породить неразрешимые трудности. Для передачи мегабайтного файла по гигабитному каналу требуется около 40 мсек (при этом предполагается, что задержка в канале составляет 32 мсек (RTT=64 мсек)). Собственно передача этой информации занимает 8 мсек. Из этих цифр видно, что традиционные протоколы, размеры окон и пр. могут свести на нет преимущества скоростного (дорогостоящего) канала. Пропускная способность такого канала определяется уже не его полосой, а задержкой. Понятно также, что необходимо расширить поле размера окна с 16 до 32 бит. Чтобы не изменять формат TCP-сегментов, можно сделать код размера окна в программе 32-разрядным, сохранив соответствующее поле в сегменте неизменным. Размер окна в этом случае задается как бы в формате с плавающей запятой. При установлении канала определяется масштабный коэффициент n (порядок) лежащий в интервале 0-14. Передача этого коэффициента (один байт) осуществляется сегментом SYN в поле опций. В результате размер окна оказывается равным 65535\*2n. Если один из партнеров послал ненулевой масштабный коэффициент, но не получил такого коэффициента от своего партнера по каналу, то **n** считается равным нулю. Эта схема позволит сосуществовать старым и новым системам. Выбор **n** возлагается на TCP-модуль системы.

Для того чтобы точнее отслеживать вариации RTT, предлагается помещать временные метки в каждый посылаемый сегмент. Так как в TCP используется одно подтверждение ACK на несколько сегментов, правильнее будет сказать, что RTT измеряется при посылке каждого ACK. Способность и готовность партнеров работать в таком режиме временных меток определяется на фазе установления канала. Более точное вычисление RTT позволяет не только корректно выбрать временные постоянные для таймеров, правильно вычислить задержку TIME\_WAIT (TIME\_WAIT=8×RTO), но и отфильтровать "старые" сегменты. Идеология временных меток используется и в алгоритме **PAWS** (Protection Against Wrapped Sequence Numbers) для защиты против перепутывания номеров сегментов.

Предлагаемое усовершенствование TCP - T/TCP модифицирует алгоритмы выполнения операций. T/TCP вводит новую 32-битную системную переменную - число соединений (CC). СС позволяет сократить число пересылаемых сегментов при установлении канала, а также отфильтровывать "старые" сегменты, не принадлежащие данной сессии (установленной связи). Время отклика клиента в рамках указанных алгоритмов сокращается до суммы RTT и времени обработки запроса процессором. Данные пришедшие до SYN-сегмента должны буферизоваться для последующей обработки, а не отбрасываться.

Ethernet (10 Мбит/c) в идеальных условиях позволяет осуществить обмен в рамках протокола TCP (например, при FTP-сессии) со скоростью 1,18 Мбайт/с.

Как уже отмечалось, максимальная длина сегмента (MSS - Maximum Segment Size) в TCP-обменах величина переменная. Длина сегмента определяет длину кадра, в который он вложен. Для локальных Ethernet-сетей MSS=1460 октетов. Чем длиннее кадр, тем выше пропускная способность сети (меньше накладные расходы на заголовок кадра). С другой стороны, при передаче дейтограмм по внешним каналам, где размер пакета не столь велик, большое значение MSS приведет к фрагментации пакетов, которая замедлит обмен, поэтому администратор сети должен взвешивать последствия, задавая значения размера сегментов. Если MSS явно не задан, устанавливается значение по умолчанию (536 байт), что соответствует 576-байтной IP-дейтограмме. Для нелокальных адресов - это, как правило, разумный выбор.

Ликвидация связи требует посылки четырех сегментов. TCP-протокол допускает возможность, когда один из концов канала объявляет о прекращении посылки данных (посылает FIN-сегмент), продолжая их получать (режим частичного закрытия - *half-close*). Посылка сегмента FIN означает выполнение операции *active close*. Получатель FIN-сегмента должен послать подтверждение его получения. Когда противоположный конец, получивший FIN, закончит пересылку данных, он пошлет свой FIN-сегмент. Прием подтверждения на получение этого сегмента означает закрытие данного канала связи. Возможно прерывание связи и с помощью посылки RST-сегмента. В этом случае все буферы и очереди очищаются немедленно и часть информации будет потеряна.