1 Лабораторная работа № 1. Стек TCP/IP

Цель работы. Получить основные теоретические сведения по стеку TCP/IP.

Теоретическая справка.

В настоящее время в сетях используется несколько стеков коммуникационных протоколов. Наиболее популярны следующие стеки:

- TCP/IP;
- IPX/SPX;
- NetBIOS/SMB;
- DECnet;
- SNA;
- OSI.

Все эти стеки, кроме SNA на нижних уровнях — физическом и канальномиспользуют одни и те же хорошо стандартизованные протоколы Ethernet, Token Ring, FDDI и ряд других, которые позволяют задействовать во всех сетях одну и ту же аппаратуру. Зато на верхних уровнях все стеки работают по своим протоколам. Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков [1].

Стек TCP/IP был разработан для связи экспериментальной сети ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней для локальных сетей — это Ethernet, Token Ring, FDDI, для глобальных — протоколы работы на аналоговых коммутируемых и выделенных линиях (SLIP, PPP) протоколы территориальных сетей X.25 и ISDN.

Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному уровням, соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки. Стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие протоколы, как протокол пересылки файлов FTP, протокол эмуляции терминала telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы службы WWW и другие.

Уровни.

Сетевые протоколы обычно разрабатываются по уровням, причем каждый уровень отвечает за собственную фазу коммуникаций. Семейства протоколов, такие как TCP/IP, это комбинации различных протоколов на различных уровнях. TCP/IP состоит из четырех уровней, как показано в таблице 1 [1].

Таблица 1 – Уровни протокола TCP/IP

Прикладной	Telnet, FTP, e-mail и т.д.
Транспортный	TCP,UDP
Сетевой	IP, ICMP, IGMP
Канальный	драйвер устройства и интерфейсная плата

Каждый уровень несет собственную функциональную нагрузку.

1. Канальный уровень (link layer). Его называют уровнем сетевого интефейса. Обычно включает в себя драйвер устройства в операционной системе и соответствующую сетевую интерфейсную плату в компьютере. Вместе они обеспечивают аппаратную поддержку физического соединения с сетью (с кабелем или с другой средой передачи).

2. Сетевой уровень (network layer), иногда называемый уровнем межсетевого взаимодействия, отвечает за передачу пакетов по сети. Маршрутизация пакетов осуществляется на этом уровне. IP (Internet Protocol - протокол Internet), ICMP (Internet Control Message Protocol - протокол управления сообщениями Internet) и

IGMP (Internet Group Management Protocol - протокол управления группами Internet) обеспечивают сетевой уровень в семействе протоколов TCP/IP.

3. Транспортный уровень (transport layer) отвечает за передачу потока данных между двумя компьютерами и обеспечивает работу прикладного уровня, который находится выше. В семействе протоколов TCP/IP существует два транспортных протокола - TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). TCP осуществляет передачу данных между двумя компьютерами. Он обеспечивает деление данных, передающихся от одного приложения к другому, на пакеты подходящего для сетевого уровня размера, подтверждение принятых пакетов, установку тайм-аутов, в течение которых должно прийти подтверждение на пакет, и так далее. Так как надежность передачи данных гарантируется на транспортном уровне, на прикладном уровне эти детали игнорируются. UDP предоставляет более простой сервис для прикладного уровня. Он просто отсылает пакеты, которые называются датаграммами (datagram) от одного компьютера к другому. За надежность передачи данных, при использовании датаграмм отвечает прикладной уровень.

4. Прикладной уровень (application layer) определяет детали каждого конкретного приложения. Существует несколько приложений TCP/IP, которые присутствуют практически в каждой реализации:

– Telnet - удаленный терминал;

– FTP, File Transfer Protocol - протокол передачи файлов;

– SMTP, Simple Mail Transfer Protocol - простой протокол передачи электронной почты;

– SNMP, Simple Network Management Protocol - простой протокол управления сетью [1].

Полезным свойством протокола TCP/IP является его способность фрагментировать пакеты. Сложная составная сеть часто состоит из сетей, построенных на совершенно разных принципах. В каждой из этих сетей может быть установлена собственная величина максимальной длины единицы передаваемых данных (кадра). В таком случае при переходе из одной сети, имеющей большую

максимальную длину, в другую, с меньшей максимальной длиной, может возникнуть необходимость разделения передаваемого кадра на несколько частей. Протокол IP стека TCP/IP решает эту задачу.

Другой особенностью технологии TCP/IP является гибкая система адресации, позволяющая более просто по сравнению с другими протоколами аналогичного назначения включать в интерсеть (объединенную или составную сеть) сети других технологий. Это свойство также способствует применению стека TCP/IP для построения больших гетерогенных сетей.

Недостаток использования этого протокола - требования к ресурсам и сложность администрирования IP - сетей. Для реализации функциональных возможностей протоколов стека TCP/IP требуются большие вычислительные затраты. Гибкая система адресации и отказ от широковещательных рассылок приводят к наличию в IP-сети различных централизованных служб типа DNS, DHCP и т. п. Каждая из этих служб упрощает администрирование сети и конфигурирование оборудования, но в то же время сама требует внимания со стороны администраторов.

В стеке TCP/IP используются три типа адресов - локальные (называемые также аппаратными), IP - адреса и символьные доменные имена.

В терминологии TCP/IP под локальным адресом понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес — это MAC - адрес. MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC - адрес назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC - адрес имеет формат 6 байт, например 11-A0-17-3D-BC-01. Однако протокол IP может работать и над протоколами более высокого уровня, например над протоколом IPX или X.25. В

этом случае локальными адресами для протокола IP соответственно будут адреса IPX и X.25. Следует учесть, что компьютер в локальной сети может иметь несколько локальных адресов даже при одном сетевом адаптере. Некоторые сетевые устройства не имеют локальных адресов (глобальные порты маршрутизаторов, предназначенные для соединений типа «точка-точка»).

Символьные доменные имена. Символьные имена в IP - сетях называются доменными и строятся по иерархическому признаку.

Составляющие полного символьного имени в IP - сетях разделяются точкой и перечисляются в следующем порядке - сначала простое имя конечного узла, затем имя группы узлов (например, имя организации), затем имя более крупной группы (поддомена) и так до имени домена самого высокого уровня (например, домена объединяющего организации по географическому принципу (RU — Россия, UK — Великобритания, SU — США). В сетях TCP/IP используется специальная распределенная служба Domain Name System (DNS), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также DNS – именами [1].

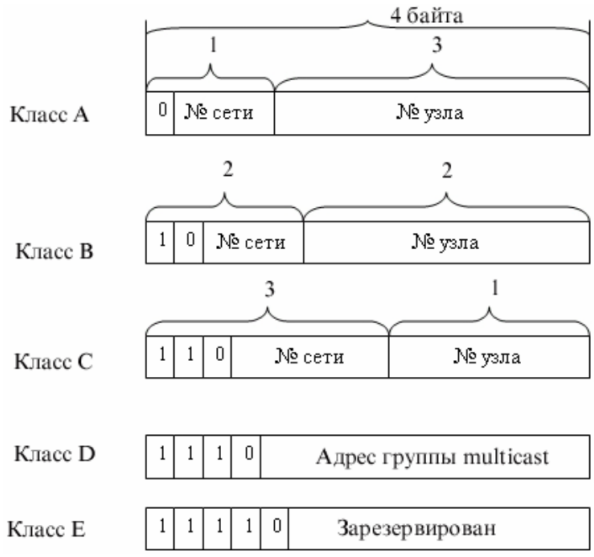

Рисунок 1 – Маски классов сетей

IP - адрес имеет длину 4 байта и обычно записывается в виде четырех чисел, представляющих значения каждого байта в десятичной форме и разделенных точками. Адрес состоит из двух логических частей — номера сети и номера узла в

сети. Какая часть адреса относится к номеру сети, а какая — к номеру узла, определяется значениями первых бит адреса. Значения этих бит являются также признаками того, к какому классу относится тот или иной IP - адрес.

Для установки границы между номером сети и номером узла используются маски. Маска — это число, которое используется в паре с IP - адресом (двоичная запись маски содержит единицы в тех разрядах, которые должны в IP - адресе интерпретироваться как номер сети). Поскольку номер сети является цельной частью адреса, единицы в маске также должны представлять непрерывную последовательность. Для стандартных классов сетей маски имеют следующие значения:

– класс A - 11111111.00000000.00000000. 00000000 (255.0.0.0);

– класс B - 11111111.11111111.00000000. 00000000 (255.255.0.0);

– класс C - 11111111.11111111.11111111.00000000 (255.255.255.0).

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8, чтобы повторять деление адреса на байты.

Пример. Для IP-адреса 129.64.134.5 указана маска 255.255.128.0, то есть в двоичном виде:

– IP - адрес 129.64.134.5 - 10000001. 01000000.10000110. 00000101;

– маска 255.255.128.0 - 11111111.11111111.10000000.00000000.

Если игнорировать маску, то в соответствии с системой классов адрес 129.64.134.5 относится к классу B, а значит, номером сети являются первые 2 байта — 129.64.0.0, а номером узла — 0.0.134.5.

Если же использовать для определения границы номера сети маску, то 17 последовательных единиц в маске, «наложенные» на IP-адрес, определяют в качестве номера сети в двоичном выражении число: 10000001.01000000.10000000. 00000000 или в десятичной форме записи — номер сети 129.64.128.0, а номер узла 0.0.6.5. IP - пакет состоит из заголовка и поля данных. Заголовок, как правило, имеющий длину 20 байт и имеет структуру, показанную на рисунке 2.

Поле «Номер версии» (Version), занимающее 4 бит, указывает версию протокола IP. Сейчас используется версия 4 (IPv4) (новая версия 6 (IPv6)).

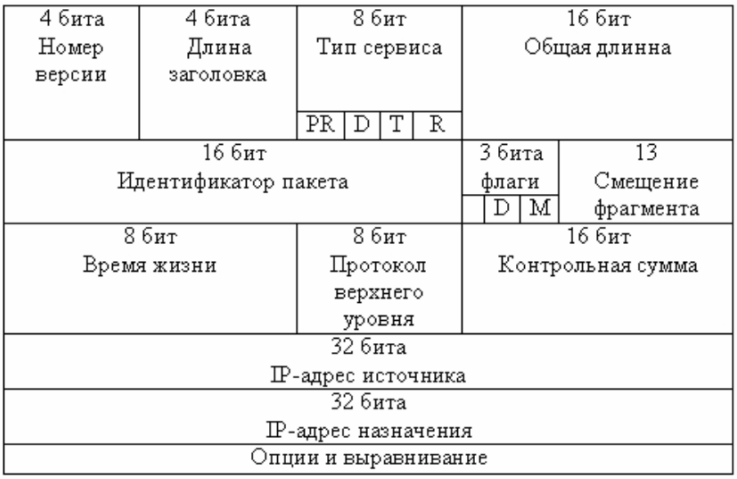

Рисунок 2 – Структура заголовка

Поле «Длина заголовка» (IHL) IP - пакета занимает 4 бит и указывает значение длины заголовка, измеренное в 32-битовых словах. Обычно заголовок имеет длину в 20 байт (пять 32-битовых слов), но при увеличении объема служебной информации эта длина может быть увеличена за счет использования дополнительных байт в поле Опции (IP Options) [1].

Поле «Тип сервиса» (Type of Service) занимает один байт и задает приоритетность пакета и вид критерия выбора маршрута. Первые три бита этого поля образуют подполе приоритета пакета (Precedence). Приоритет может иметь значения от самого низкого - 0 (нормальный пакет) до самого высокого - 7 (пакет управляющей информации). Маршрутизаторы и компьютеры могут принимать во внимание приоритет пакета и обрабатывать более важные пакеты в первую очередь. Поле Тип сервиса содержит также три бита, определяющие критерий выбора маршрута. Реально выбор осуществляется между тремя альтернативами - малой задержкой, высокой достоверностью и высокой пропускной способностью. Установленный бит D (delay) говорит о том, что маршрут должен выбираться для минимизации задержки доставки данного пакета, бит T — для максимизации пропускной способности, а бит R — для максимизации надежности доставки. Во многих сетях улучшение одного из этих параметров связано с ухудшением другого,

кроме того, обработка каждого из них требует дополнительных вычислительных затрат. Зарезервированные биты имеют нулевое значение.

Поле «Общая длина» (Total Length) занимает 2 байта и означает общую длину пакета с учетом заголовка и поля данных. Максимальная длина пакета ограничена разрядностью поля, определяющего эту величину, и составляет 65535 байт, однако в большинстве хост-компьютеров и сетей столь большие пакеты не используются. При передаче по сетям различного типа длина пакета выбирается с учетом максимальной длины пакета протокола нижнего уровня, несущего IP - пакеты. Если это кадры Ethernet, то выбираются пакеты с максимальной длиной в 1500 байт, умещающиеся в поле данных кадра Ethernet. В стандарте предусматривается, что все хосты должны быть готовы принимать пакеты вплоть до 576 байт длиной (приходят ли они целиком или по фрагментам). Хостам рекомендуется отправлять пакеты размером более чем 576 байт, только если они уверены, что принимающий хост или промежуточная сеть готовы обслуживать пакеты такого размера.

Поле «Идентификатор пакета» (Identification) занимает 2 байта и используется для распознавания пакетов, образовавшихся путем фрагментации исходного пакета. Все фрагменты должны иметь одинаковое значение этого поля.

Поле «Флаги» (Flags) занимает 3 бита и содержит признаки, связанные с фрагментацией. Установленный бит DF (Do not Fragment) запрещает маршрутизатору фрагментировать данный пакет, а установленный бит MF (More Fragments) говорит о том, что данный пакет является промежуточным (не последний) фрагментом. Оставшийся бит зарезервирован.

Поле «Смещение фрагмента» (Fragment Offset) занимает 13 бит и задает смещение в байтах поля данных этого пакета от начала общего поля данных исходного пакета, подвергнутого фрагментации. Используется при сборке/разборке фрагментов пакетов при передачах их между сетями с различными величинами MTU. Смещение должно быть кратно 8 байт.

Поле «Время жизни» (Time to Live) занимает один байт и означает предельный срок, в течение которого пакет может перемещаться по сети. Время

жизни данного пакета измеряется в секундах и задается источником передачи. На маршрутизаторах и в других узлах сети по истечении каждой секунды из текущего времени жизни вычитается единица. Единица вычитается и в том случае, когда время задержки меньше секунды. Время жизни можно считать равным максимальному числу узлов, которые разрешено пройти данному пакету до того, как он достигнет места назначения. Если параметр времени жизни станет нулевым до того, как пакет достигнет получателя, этот пакет будет уничтожен.

Идентификатор протокола верхнего уровня (Protocol) занимает один байт и указывает, какому протоколу верхнего уровня принадлежит информация, размещенная в поле данных пакета (например, это могут быть сегменты протокола TCP, дейтаграммы UDP, пакеты ICMP или OSPF). Значения идентификаторов для различных протоколов приводятся в документе RFC «Assigned Numbers».

Контрольная сумма (Header Checksum) занимает 2 байта и рассчитывается только по заголовку. Поскольку некоторые поля заголовка меняют свое значение в процессе передачи пакета по сети (например, время жизни), контрольная сумма проверяется и повторно рассчитывается при каждой обработке IP - заголовка. Контрольная сумма - 16 бит подсчитывается как дополнение к сумме всех 16-битовых слов заголовка. При вычислении контрольной суммы значение самого поля «контрольная сумма» устанавливается в нуль. Если контрольная сумма неверна, то пакет будет отброшен, как только ошибка будет обнаружена.

Поля «IP - адрес источника» (Source IP Address) и «IP - адрес назначения» (Destination IP Address) имеют одинаковую длину - 32 бита и одинаковую структуру.

Поле «Опции» (IP Options) является необязательным и используется обычно только при отладке сети. Механизм опций предоставляет функции управления, которые необходимы или просто полезны при определенных ситуациях, однако он не нужен при обычных коммуникациях. Это поле состоит из нескольких подполей, каждое из которых может быть одного из восьми предопределенных типов. В этих подполях можно указывать точный маршрут прохождения маршрутизаторов, регистрировать проходимые пакетом маршрутизаторы, помещать данные системы безопасности, а также временные отметки. Так как число подполей может быть

произвольным, то в конце поля Опции должно быть добавлено несколько байт для выравнивания заголовка пакета по 32-битной границе.

Поле «Выравнивание» (Padding) используется для того, чтобы убедиться в том, что IP-заголовок заканчивается на 32-битной границе. Выравнивание осуществляется нулями.

Каждый интерфейс в объединенной сети должен иметь уникальный IP адрес. Эти адреса представляют из себя тридцатидвухбитовые числа. Существует определенная структура адреса Internet. Эти 32-битные адреса обычно записываются как 4 десятичных числа, по одному на каждый байт адреса. Такая форма записи называется "десятичной записью с точками" (dotted-decimal) [1].

Пример. Адрес сети класса B может быть записан как 140.252.13.33.

Определить класс адреса, или класс сети, можно по первому числу в адресе (таблица 2).

Таблица 2 - Пять классов адресов

Класс	Диапазон IP адресов в разных классах сетей
A	0.0.0.0 - 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 247.255.255.255

Так как каждый интерфейс, подключенный к сети, должен иметь уникальный адрес, встает вопрос распределения IP адресов в глобальной сети Internet. Этим занимается сетевой информационный центр (Internet Network Information Center или InterNIC). InterNIC назначает только сетевые идентификаторы (ID). Назначением идентификаторов хостов в сети занимаются системные администраторы.

Существует три типа IP адресов - персональный адрес (unicast) - указывает на один хост, широковещательный адрес (broadcast) - указывает на все хосты в указанной сети, и групповой адрес (multicast) - указывает на группу хостов, принадлежащей к группе адресации.

Порядок выполнения работы.

1. Изучить назначение протокола TCP/IP.
2. Изучить уровни протокола TCP/IP.
3. Изучить систему адресации протокола TCP/IP.
4. Изучить структуру заголовка пакета IP.
5. Изучить описание полей заголовка IP.
6. Оформить отчет.

Содержание отчета по лабораторной работе.

1. Название и цель работы.
2. Основные теоретические пункты общих сведений.
3. Выводы по выполненной работе.
4. Список использованных источников.

Контрольные вопросы.

1. Назначение протокола TCP/IP.
2. Какие стандарты поддерживает протокол TCP/IP ?
3. Какие уровни представлены в протоколе TCP/IP ?
4. Какую функциональную нагрузку несет канальный уровень ?
5. Какую функциональную нагрузку несет сетевой уровень ?
6. Какую функциональную нагрузку несет транспортный уровень ?
7. Какую функциональную нагрузку несет прикладной уровень ?
8. Как устроена система адресации в протоколе TCP/IP ?
9. Что понимается под локальным адресом в протоколе TCP/IP ?
10. Какое назначение IP - адреса ?
11. Что такое символьные доменные имена ?
12. Какую длину и структуру имеет IP - адрес ?
13. Что представляют собой маски классов сетей ?
14. Из чего состоит IP - пакет ?
15. Какие поля (и их назначение) используются в пакете ?