Общие принципы построения компьютерных сетей и основные определения

Под термином «Сеть» будем понимать систему связи со многими источниками и/или получателями сообщений. Места, где пути распространения сигналов в сети разветвляются или оканчиваются, называются узлами сети.

Компьютерная сеть – это сеть, в которой источниками и получателями сообщений являются компьютеры. Можно назвать несколько близких понятий, а именно, — вычислительная сеть, сеть передачи данных, распределённая система, различие между которыми определяется акцентами.

Классификация компьютерных сетей

Компьютерные сети как сложные и многопрофильные объекты принято классифицировать, исходя из разных точек зрения. Наиболее популярными являются следующие принципы классификации:

По «диаметру», т. е. расстоянию между наиболее удалённым узлами сети:

Сотни метров — LAN (Local Area Network) или ЛВС (Локальная Вычислительная Сеть);

Километры — MAN/CAN (Metropolitan/Campus Area Network) или РВС (Региональная Вычислительная Сеть);

Сотни и тысячи километров — WAN (Wide Area Network) или ГВС (Глобальная Вычислительная Сеть).

Поскольку современные компьютерные сети практически всегда имеют выход в глобальную сеть Internet, классификация сетей по этому принципу носит довольно условный характер.

По физической топологии (звезда, кольцо, общая шина, сотовая, иерархическая (древовидная), комбинированная), показывающей физическое соединение линий связи между узлами сети.

По логической топологии (звезда, кольцо, общая шина), показывающей способ обмена сигналами.

Физическая и логическая топологии слабо связаны между собой. Например, популярной технологии Ethernet на витой паре соответствует физическая топология звезда и логическая топология общая шина.

По виду кабельной системы – витая пара, оптический кабель, коаксиальный кабель, беспроводные сети.

По способу организации соединения и передачи информации сети делятся на сети с коммутацией

- каналов (например, телефонная сеть общего пользования),
- сообщений (информация перемещается от узла к узлу целиком)
- пакетов (пакеты внутри сети перемещаются независимо друг от друга и собираются целиком в узле назначения).

По стекам протоколов – наборам правил формирования и передачи пакетов. Например, стек TCP/IP, стек IPX/SPX, X25 и пр. Стек отличается от совокупности тем, что стек подразумевает не только набор правил, но и определяет последовательность их применения.

По сетевым операционным системам, т. е. программным продуктам, обслуживающим запросы пользователей на ресурсы сети и обеспечивающим функционирование сети, её администрирование. Например, MS Windows, Novell NetWare, UNIX/Linux и пр.

По способу предоставления ресурсов

- одноранговые (все компьютеры могут быть и источниками и потребителями ресурсов сети),
- клиент – сервер (выделенные компьютеры являются источниками ресурсов – серверами, а остальные – клиентами, т. е. потребителями ресурсов).

Ресурсами сети могут быть устройства (принтеры, модемы, диски и пр.), файлы (текстовые, звуковые, видео и пр.), службы/сервисы (WWW, E-mail, базы данных и пр.).

Международные организации. Модель OSI

Глобальность охвата и интернациональный характер развития компьютерных сетей делает роль международных организаций в вопросах стандартизации определяющей. При этом, в большинстве случаев, принимаемые стандарты носят характер рекомендаций, однако «де факто» становятся обязательными и соблюдаются всеми производителями сетевого оборудования и программного обеспечения. Механизм создания рекомендаций, кроме собственных разработок, включает в себя и рассмотрение инициативных предложений крупных компаний, самостоятельно разрабатывающих и продвигающих те или иные сетевые технологии. Отличительной чертой рекомендация является их непрерывная модернизация, отслеживающая новейшие достижения в этой области.

Наиболее авторитетными организациями в области сетевых технологий являются:

ITU-T (International Telecommunications Union sector Telecommunication) Международный союз электросвязи, сектор телекоммуникаций. До 1993 года организация называлась CCITT (Consultative Committee for International Telephone and telegraphy), или в русском переводе МККТТ (Международный Консультативный Комитет по Телефонии и Телеграфии). Кроме сектора T (Telecommunication), важными являются секторы R (распределения радиочастот) и D (развития).

ISO (International Organization for Standardization) Международная организация по стандартизации. Эта организация объединяет национальные институты стандартов из 89 стран (ANSI — США, DIN – Германия, BSI – Великобритания и др.).

IEEE (Institute of Electrical and Electronics Engineers) Институт инженеров по электротехнике и радиоэлектронике – национальный «профсоюз» «электрических» учёных и инженеров США.

Модель OSI (Open System Interconnection) — взаимодействия открытых систем была опубликована в 1983 г. по результатам совместных работ ISO и ITU-T. Согласно этой модели все процессы в сетях рассматриваются на семи (поэтому модель иногда называют «семиуровневой») относительно независимых уровнях для наилучшей реализации на каждом уровне по отдельности.

Обмен данными между двумя компьютерами в сети согласно семиуровневой модели иллюстрирует рисунок 1.2.1.

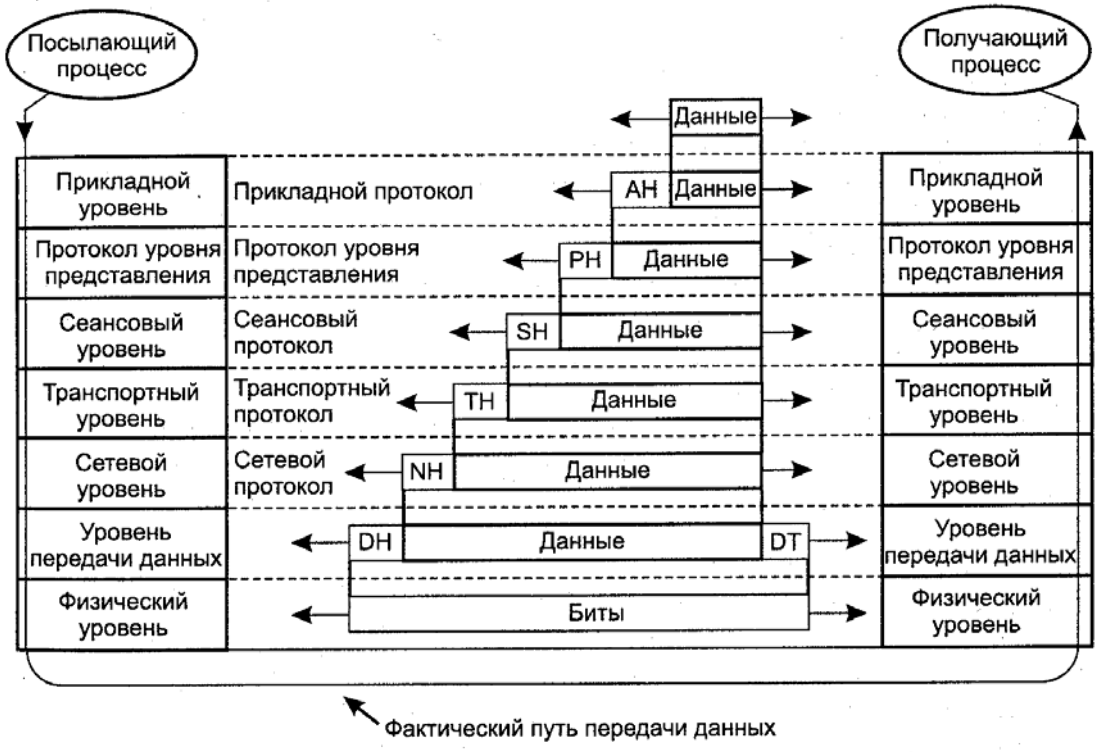


Рис. 1.2.1. Модель OSI.

На этом рисунке использованы следующие обозначения: AH (application header) заголовок прикладного уровня, PH (presentation) – заголовок уровня представлений, SH (session) – заголовок сеансового уровня, TH (transport) – заголовок транспортного уровня, NH

(network) – заголовок сетевого уровня, DH (data link) – заголовок канального уровня, DT (data link tail) – хвостовик кадра канального уровня.

Основной принцип построения модели, обеспечивающий независимость уровней, состоит в том, что пакет вышележащего уровня на нижележащем уровне рассматривается как данные, а вся необходимая для работы информация добавляется в виде заголовка/хвостовика.

При невозможности формирования пакета на нижележащем уровне из-за ограничений на размер пакета используется фрагментация (дробление) пакетов. Пример фрагментации показан на рисунке 1.2.2, где для обозначения данных используется буква M (message), заголовка – H (header) и хвостовика – T (tail).

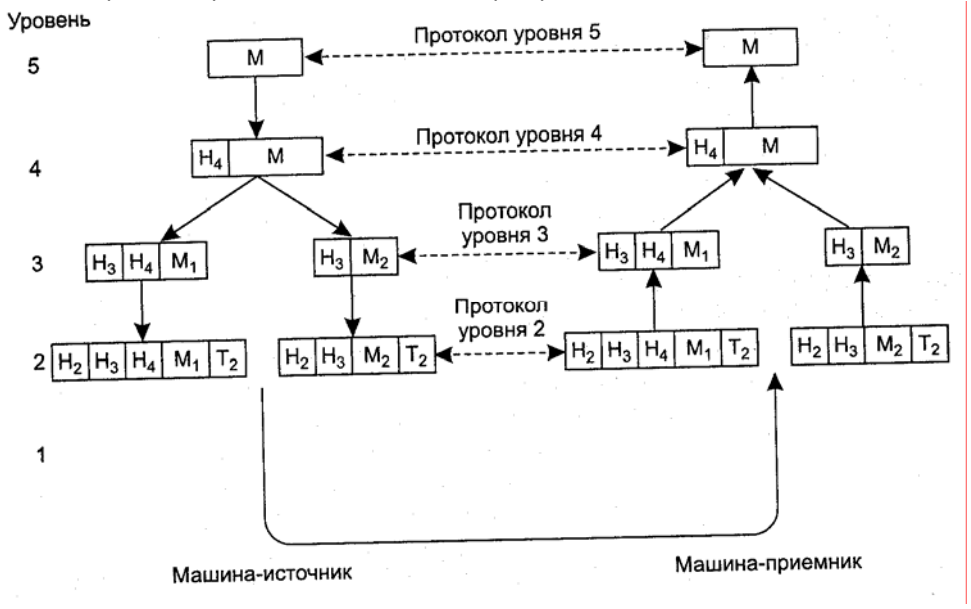


Рис. 1.2.2. Фрагментация.

На узлах внутри сети действуют три нижних уровня, как это показано на рисунке 1.2.3, где PDU (protocol data unit) означает пакет протокола соответствующего уровня.

При описании сетей принято использовать следующие термины:

Протокол – правило, определяющее состав пакета и последовательность действий на соответствующем уровне.

Интерфейс – способ передачи данных с уровня на уровень.

Стек протоколов – упорядоченная совокупность протоколов нескольких уровней.

Служба (service) отличается от протокола тем, что оговаривается только результат без подробной регламентации процесса выполнения.

Технология чаще всего используется для обозначения протоколов нижних уровней (физического и канального), например, Ethernet или ATM.

Инкапсуляция — преобразование пакета верхнего уровня одного стека в пакет нижнего уровня другого стека, например, при использовании IP поверх ATM.

Основные задачи уровней:

Физический (Physical) – стандартизация электрических и временных характеристик сигналов, физических параметров линий связи и разъёмов.

Канальный (Data Link) – доставка пакета на следующий узел сети (адресация, обнаружение/исправление ошибок).

Сетевой (Network) – доставка пакета в узел назначения (адресация, маршрутизация, проверка целостности данных).

Транспортный (Transport) – сборка всех пакетов в узле назначения.

Сеансовый (Session) – идентификация, начало/окончание сеанса передачи, аварийные режимы.

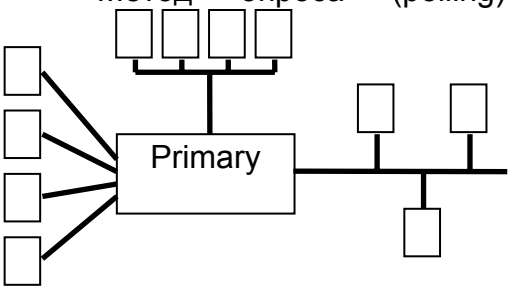
Представлений (Presentation) – преобразование данных к удобному для передачи по сети виду (например, шифрование данных по протоколу SSL (Secure Socket Layer)).

Прикладной (Application) – организация доступа к ресурсам сети. Например, получение файла – FTP (File Transfer Protocol), доступ к терминалу – Telnet и пр.

Методы доступа

Важным аспектом сетевых структур являются методы доступа к сетевой среде, т. е. принципы, используемые компьютерами для обращения к ресурсам сети. Основные методы доступа к сетевой среде основаны на логической топологии сети.

Метод опроса (polling) ассоциирован с логической топологией «звезда»



Первичный узел (primary) сети последовательно опрашивает вторичные (S – secondary) узлы об их состоянии и предоставляет требуемый сетевой ресурс. Метод реализуется в специальных сетях (телеметрических, сетях систем управления производством и технологическими процессами и т. п.).

Метод посылки маркера (token passing) соответствует логической топологии «кольцо». Идею метода посылки маркера иллюстрирует пример пересылки пакета А от станции 1 к станции 3, где пакет с точкой внутри – пакет с отметкой (флагом) получения.

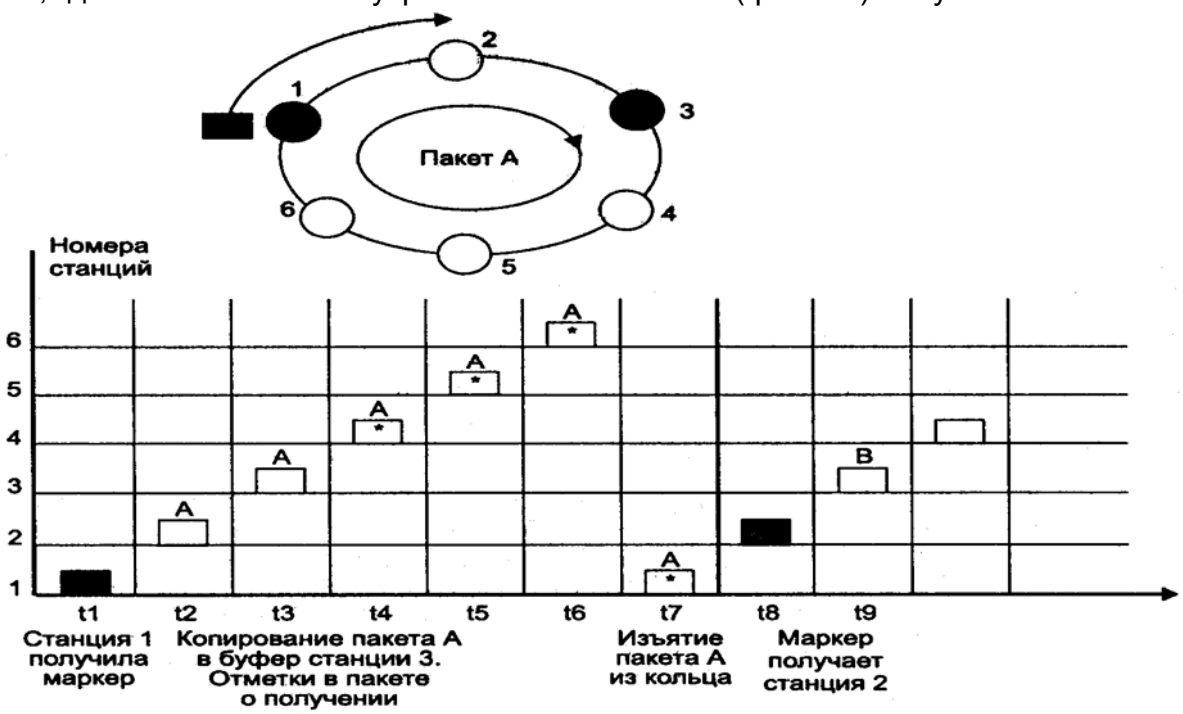


Рис. 1.3.2. Посылка маркера

Наиболее ярко этот метод реализован в технологиях Token Ring/Token Bus (IEEE 802.5/802.4) и FDDI.

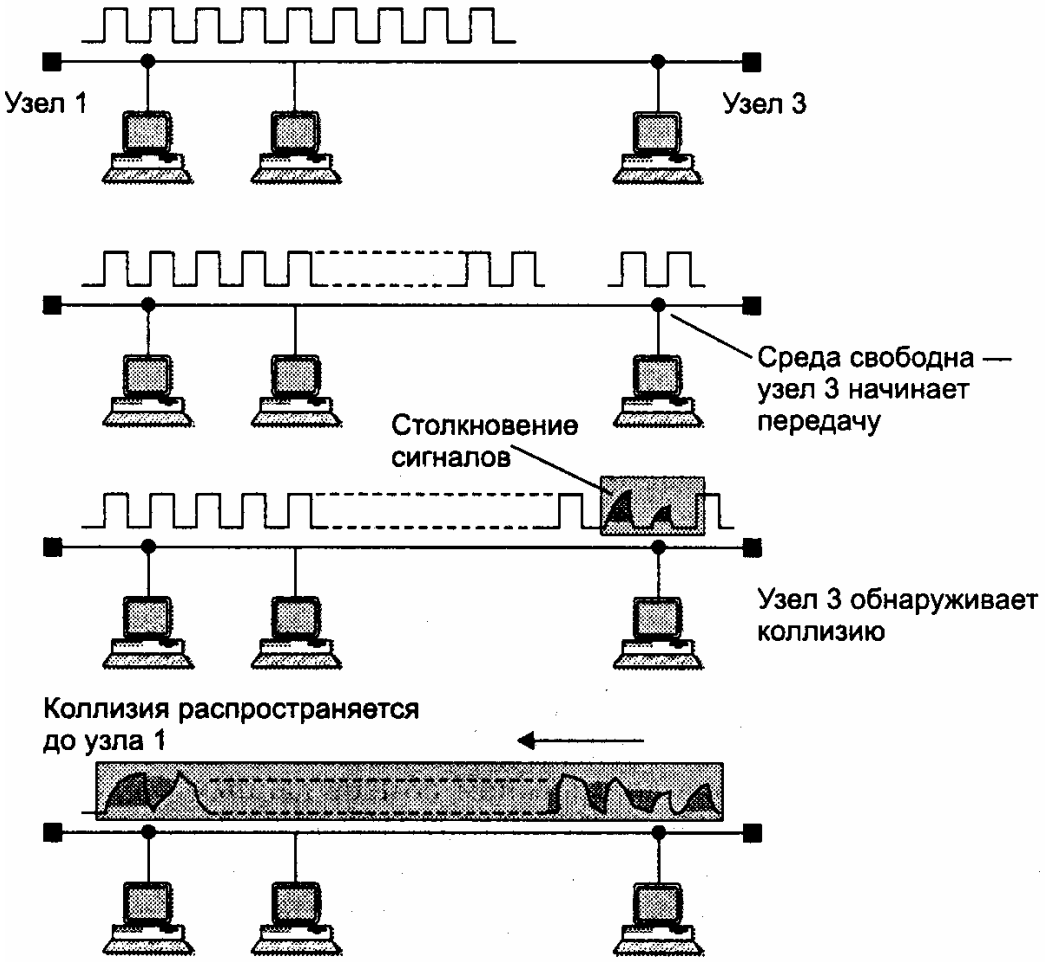
Технология Token Ring была разработана в 1984 г. фирмой IBM и обеспечивала скорость 4 Мбит/с (в современных реализациях эта скорость увеличена до 16 Мбит/с). В 1998 г. были предложены высокоскоростные версии технологии под названием High-Speed Token Ring для скоростей 100 или 155 Мбит/с. В качестве физической линии может использоваться либо коаксиальный кабель с волновым сопротивлением 70 Ом (максимальная длина кольца — 4000 м), либо экранированная витая пара STP (Shielded Twisted Pair) с расстоянием между концентратором и конечным узлом до 100 м, либо неэкранированная витая пара UTP (Unshielded Twisted Pair) с расстоянием между концентратором и конечным узлом до 45 м, либо волоконно-оптический кабель. Технология позволяет поддерживать до 260 компьютеров в сети.

Технология FDDI (Fiber Distributed Data Interface – оптоволоконный распределённый доступ к данным) разработана ANSI в 1986-8 гг. и предусматривает соединение до

500 компьютеров двойным (для повышения надёжности) кольцом оптоволокна длинной до 100 км со скоростью обмена 100 Мбит/с.

Метод конкуренции (competition) связан с логической топологией «общая шина».

Наиболее распространённая версия метода имеет название CSMA/CD (Carrier Sensing Multiple Access with Collision Detection) – прослушивание «несущей», множественный доступ, обнаружение коллизий (столкновений).



Процедура разрешения коллизий состоит в использовании случайной задержки при повторной передаче. При каждой следующей попытке интервал задержек увеличивается (например, в технологии Ethernet вдвое). Количество попыток ограничено (в технологии Ethernet их не более 16).

Для предотвращения неустранимых коллизий необходимо, чтобы длительность самого короткого кадра была больше двойного времени прохождения сигнала между крайними узлами сети.

Важным для этого метода является понятие коллизионного домена (collision domain), т. е. совокупности узлов, распознающих коллизию независимо от того, в каком узле эта коллизия возникла.

ISDN

Технология ISDN (Integrated Services Digital Network) – цифровая сеть с интеграцией услуг явилась результатом развития идеи «оцифровки» телефонных сетей общего пользования вплоть до потребителя, которому весь спектр услуг (телефонные переговоры, факсимильные сообщения, охранная и пожарная сигнализация, компьютерная передача данных и т. д.) предоставляется посредством цифровых сигналов. У истоков ISDN в 70-е гг. прошлого века под эгидой ITU-T (CCITT) стояли ведущие телефонные компании и министерствами связи наиболее развитых стран.

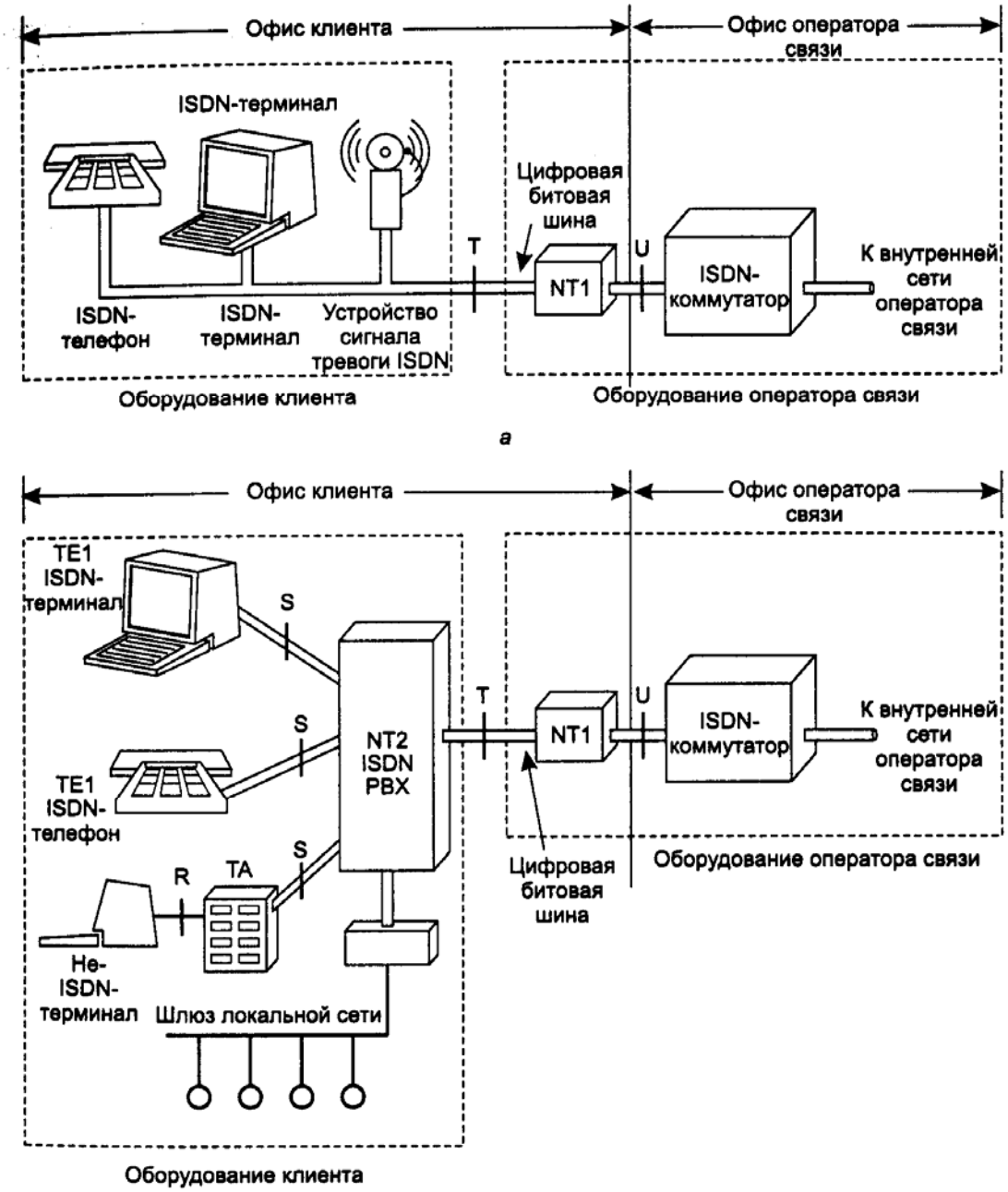
Первоначальная версия ISDN была рассчитана на скорость 64 кбит/с и получила название узкополосной N-ISDN (Narrowband). Эта технология не нашла широкого применения

из-за длительности разработки (к моменту окончательного утверждения всех протоколов скорости в 64 кбит/с было явно недостаточно) и больших финансовых затратах, поскольку потребовалось бы заменить не только станционное оборудование, но и все терминальные аппараты абонентов. Внимание к ISDN объясняется не самой технологией, а появившимися в связи с ней терминами и выделившимися из неё такими популярные технологиями, как ATM, xDSL, Frame Relay и пр.

Пользовательские интерфейсы ISDN.

На верхней части рисунка показана схема стандартного подключения частного абонента (малого офиса) к сети ISDN. Такой абонент с помощью витой пары может подключить к NT1 (Network Terminal 1) до 8 ISDN устройств. Согласно рекомендациям CCITT контрольные точки соединений обозначены буквами U, T, S и R.

На нижней части рисунка представлена схема подключения к сети ISDN через NT2 или PBX (Private Branch eXchange), играющий роль учрежденческой телефонной станции в обычных телефонных сетях.



Стандартизованные ISDN-интерфейсы:

A — аналоговый телефон с полосой 4 кГц

B — цифровой канал со скоростью 64 кбит/с (8 бит * 8 кГц) для передачи речи

C — цифровой канал со скоростью 8/16 кбит/с для передачи данных

D — цифровой дополнительный канал со скоростью 16 кбит/с для передачи данных

E — цифровой служебный канал со скоростью 64 кбит/с

H — каналы со скоростью 384 кбит/с (H0), 1536 кбит/с (H11) и 1920 кбит/с (H12).

Стандартное подключение к ISDN сети предусматривает скорость 144 кбит/с и состоит из двух каналов B и канала D (2B+1D).

ATM

Технология ATM (Asynchronous Transfer Mode — асинхронный режим передачи) позиционируется как универсальный сетевой «транспорт» для локальных и глобальных компьютерных сетей («полумагистральная»). Иногда для обозначение ATM используется термин «B-ISDN» (широкополосная (Broadband) ISDN), подчёркивающий то обстоятельство, что эта технология явилась результатом развития ISDN. К этапам создания ATM можно отнести технологию STM (Synchronous Transfer Mode – разработка Bell Labs 1968 г.) и технологию STDM (Statistical Time Division Mode – режим статистического временного уплотнения), адаптирующие ресурсы канала к потребностям абонентов. В 1993 г. усилиями IEEE, ITU-T, ANSI при участии IBM, AT&T и др. были приняты основные стандарты ATM в их нынешнем виде.

Основные идеи технологии ATM.

Основная идея технологии состоит в комбинировании принципов коммутации пакетов и коммутации каналов. На рисунке приведён пример установления соединения через фиксирующие виртуальный канал коммутаторы ATM (A, E, C, D). Данные по этому каналу передаются ячейками (пакетами) одинаковой длины в 53 байта. Обе идеи (виртуальные канал и постоянный размер пакета) направлены на ускорение передачи.

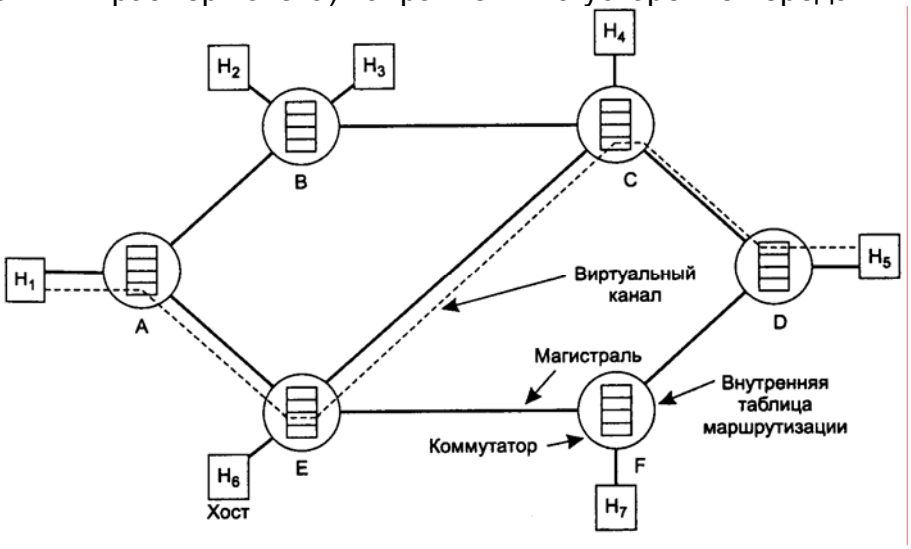
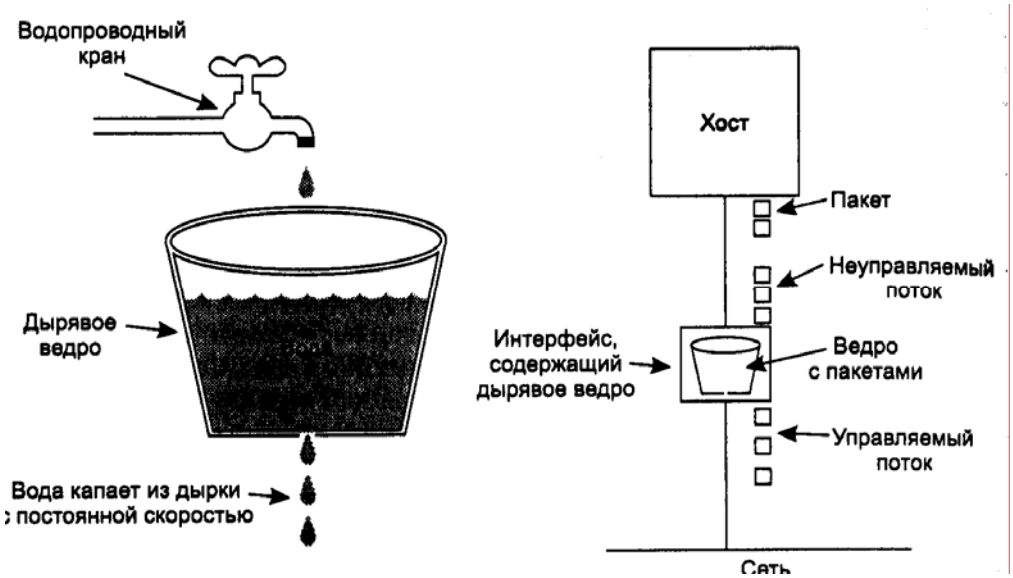


Рис. 2.2.1. Соединение ATM.

Регулирование (выравнивание) скорости с помощью коммутатора ATM. Одно из возможных решений называется принципом «дырявого ведра» проиллюстрировано рисунком 2.2.2. В ведре (коммутаторе) с ячейками не только накапливается необходимое их количество, но и производится сортировка, обеспечивая «правильный» (в соответствии с приоритетом) порядок выхода пакетов в сеть ATM.



Широкий диапазон скоростей и их согласованность со стандартными скоростями. В таблице 2.2.1 приведены скорости и примерные характеристики физической среды АТМ для локальных компьютерных сетей, в следующей таблице 2.2.2 – для глобальных сетей.

Характеристики физической среды АТМ для ЛВС.

Скорость Мбит/с	Физическая среда	Макс. расстояние между узлами м
25,6	UTP Cat. 3	100
51,84	UTP Cat. 3 Вол/опт. каб. Коаксиаль. каб.	100 2 000 400
100,0	Вол/опт. каб.	2 000
155,52	UTP Cat. 5, STP 1A Вол/опт. каб. Коаксиаль. каб.	100 2 000 200
622,08	Вол/опт. каб.	300

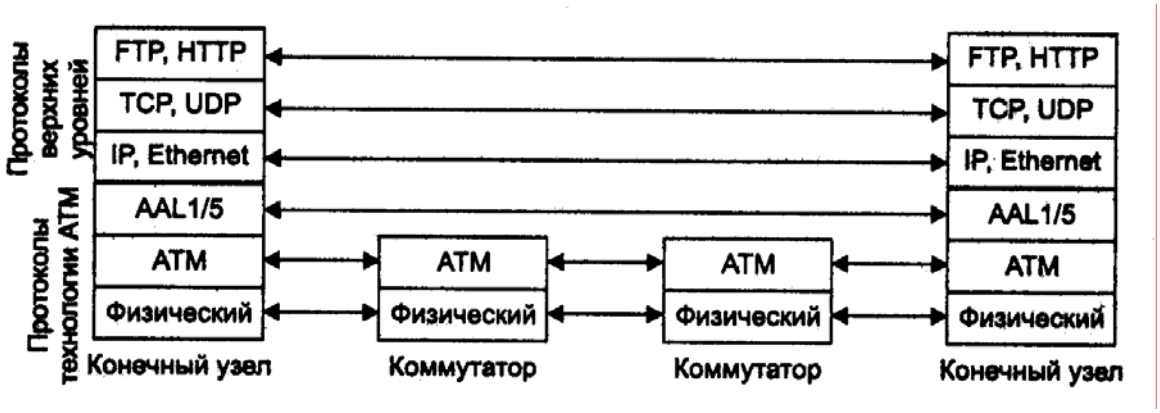
Характеристики физической среды АТМ для ГВС.

Скорость Мбит/с	Физическая среда	Макс. расстояние между узлами в км
1,544 (T1)/2,048(E1)	UTP Cat. 3	1,3
34,368(T3)/44,736(E3)	Твинаксиаль. каб.	0,4
51,84/155,52/622,08	Вол/опт. каб.	15 и более

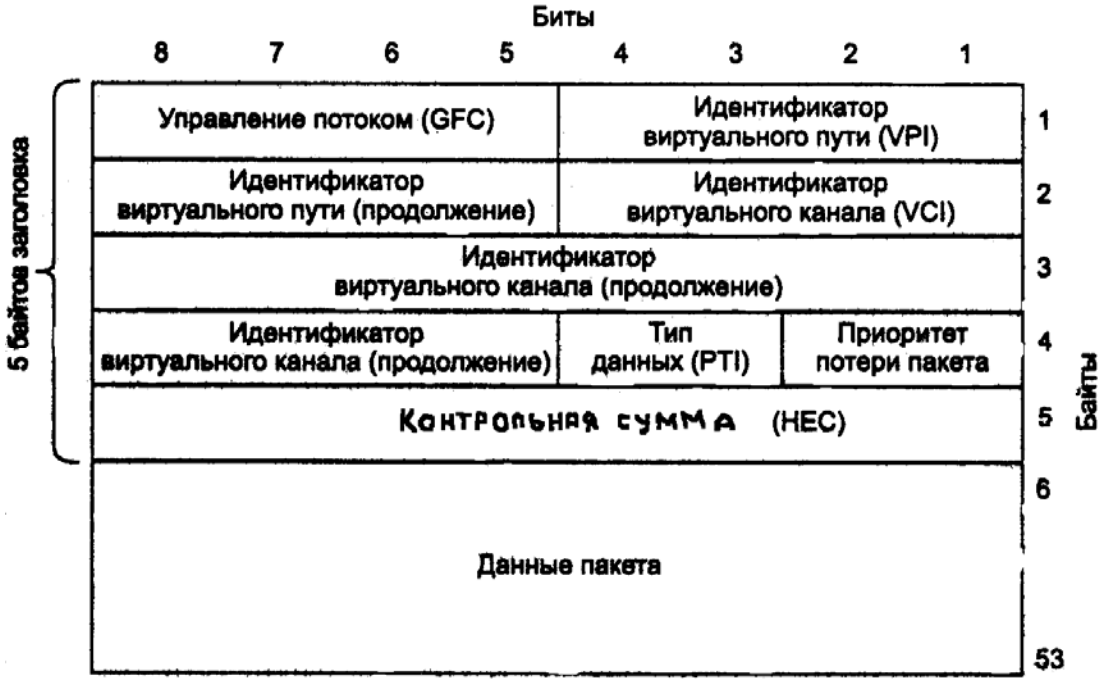
Характеристики классов трафика в АТМ

Класс трафика	Пост. бит. скорость	Треб. временная синхр	Установ. соединения	Примеры
A	+	+	+	Голос, TV
B	-	+	+	Сжат. голос, TV
C	-	-	+	TCP
D	-	-	-	IP, Ethernet
X	Устанавлив-ся пользоват-ем			

Многообразие уровней адаптации технологии к протоколам верхних уровней. уровень адаптации АТМ представляет собой набор протоколов AAL1 – AAL5 преобразования пакетов верхних уровней в ячейки АТМ, структура которых показана на рисунке 2.3.4.



Стек ATM



GFC (Generic Flow Control) – параметр взаимодействия конечного терминала и коммутатора.

VPI (Virtual Path Identifier) – идентификатор виртуального пути (общей части нескольких виртуальных каналов).

VCI (Virtual Channel Identifier) – идентификатор виртуального канала

PTI (Payload Type Identifier) – (3 бита) идентификатор типа ячейки – пользовательская или управляющая, имеет флаг перегрузки.

Приоритет потери ячейки CLP (Cell Loss Priority) – флаг кандидатов на удаление в случае необходимости.

HEC (Header Error Control) – контрольная сумма заголовка на базе расширенного кода Хэмминга.

В заключение следует отметить, что несмотря на несомненные преимущества ATM перед другими технологиями, её массовому применению в локальных сетях препятствует высокая стоимость оборудования, в особенности коммутаторов.

Ethernet

Ethernet/IEEE 802.3 (от лат. luminiferous ether — светоносный эфир) – самая популярная технология LAN с методом доступа CSMA/CD.

Технология была создана в 70-х гг. доктором Робертом Меткалфом (Robert Metcalfe) как часть проекта «офиса будущего» и обеспечивала скорость 3 Мбит/с. В 1980 г. фирмы DEC-Intel-Xerox довели скорость до 10 Мбит/с и в 1985 г. технология была официально утверждена 802-м комитетом IEEE. До сих пор можно встретить «фирменные» варианты Ethernet под

названиями Ethernet II/Ethernet DIX (DEC, Intel, Xerox) и Raw 802.3 (Novell), отличающиеся друг от друга небольшими изменениями формата кадра (пакета).

Иерархия протоколов Ethernet.

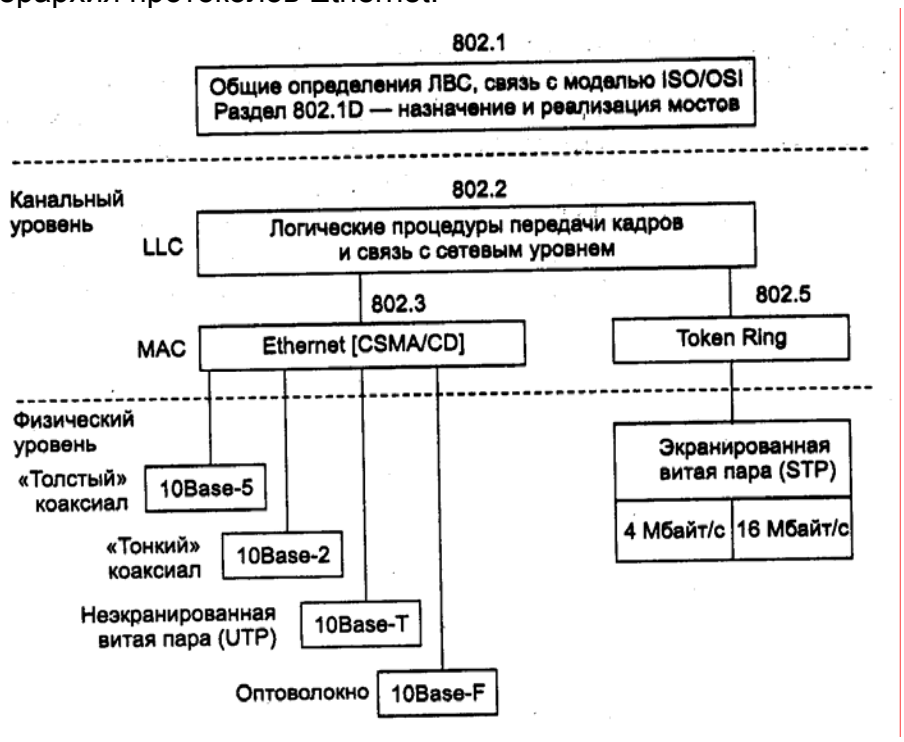
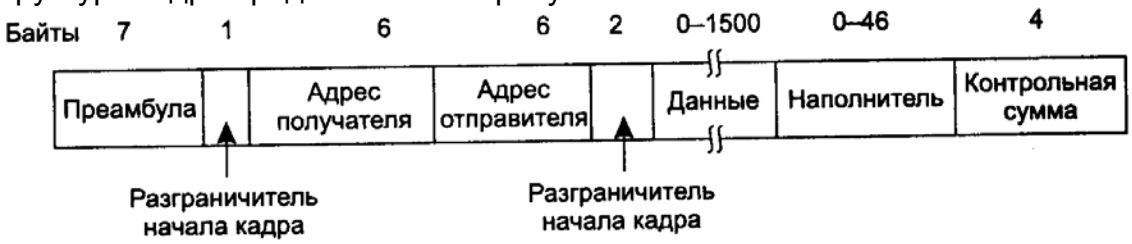


Рис. 2.3.1. Протоколы Ethernet

Согласно принятому IEEE стандарту канальный уровень технологии Ethernet делится на подуровень управления логическим каналом LLC (Logical Link Control), отвечающий за логику работы канального уровня, и подуровень доступа к среде MAC (Media Access Control), обеспечивающий формирование кадра.

Каждый узел сети снабжается **уникальным MAC адресом** из 6 байт, причём 3 байта (без двух старших бит) закрепляются в IEEE за производителем оборудования, а 3 оставшихся байта устанавливаются им самостоятельно.

Структура кадра представлена на рисунке 2.3.2.

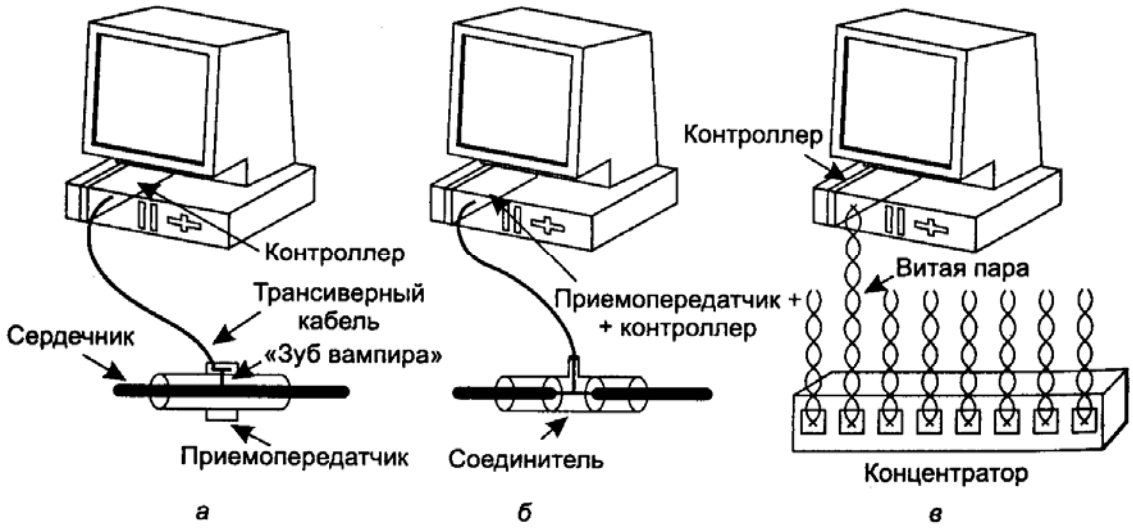


Принимая кадры, сетевые адаптеры устройств считывают MAC адрес получателя и при его совпадении с собственным адресом помещают кадр во входной буфер для последующей обработки, в противном случае – кадр отбрасывается.

Старшие два бита адреса получателя в зависимости от назначения кадра устанавливаются программно при его отправке. Например, у широковещательного кадра, обращённого ко всем узлам сети, старший бит устанавливается в 1, у кадра, адресованного группе узлов, в 1 устанавливается следующий бит адреса и, наконец, у кадра, предназначенного конкретному узлу, оба старших бита — нулевые.

Физическая среда Ethernet

Физическая среда играет важную роль как в формировании стоимости компьютерной сети, так и в потенциальных возможностях её развития. Как следует из рисунка базовые типы кабельных систем технологии Ethernet могут быть построены на двух вида коаксиального кабеля, оптического кабеля или витой пары.



Устаревшие коаксиальные кабельные системы обозначаются как 10Base5 и 10Base2. Первая цифра 10 означает «физическую» скорость передачи сигналов в 10 Мбит/с, слово «Base» – использование всего доступного частотного диапазона кабеля и, наконец, вторая цифра 5 или 2 — округлённый диаметр коаксиального кабеля в десятых долях дюйма. Кабели этих типов имеют волновое сопротивление 50 Ом, маркируются как RG 8/11 и RG58 и называются толстым (thick) и тонким (thin) Ethernet.

Оптические кабели обобщённо обозначаются как 10BaseF (Fiber). Различают стандарт 10BaseFL (доработка комитета IEEE 802.3 более ранней (80-е годы) технологии FOIRL (Fiber Optic Inter Repeater Link) для оптоволоконного соединения узлов сети) и 10BaseFB – для магистральных соединений оптических концентраторов и повторителей, отстоящих друг от друга на расстоянии до 2 км. По своим оптическим характеристикам кабели делят на одномодовые, рассчитанные на использование лазеров, и многомодовые, предназначенные для более дешёвых светодиодных излучателей. Из-за относительно высокой стоимости оптического кабеля и сложности его прокладки оптические кабельные системы редко используются в ЛВС.

Самым распространённым в ЛВС типом кабельной системы является витая пара 10BaseT (Twisted), представляющая собой заключенные в общую оболочку 8 разноцветных скрученных попарно проводов (IEEE 802.3i), из которых в классической технологии Ethernet используется только 2 пары для передачи и приёма сигналов. Альтернативным обозначением витой пары является UTP (Unshielded Twisted Pair) – неэкранированная витая пара.

Категории витой пары

Категория	**Верхняя частота (МГц)**	**Применение**
1	0	Телефон, сигнализация
2	1	Телефон, ArcNet
3	16	Телефон, 10BaseT
4	20	Token Ring
5	110(200)	100BaseT
6	350	1000BaseT
7	400(750)	1000BaseT

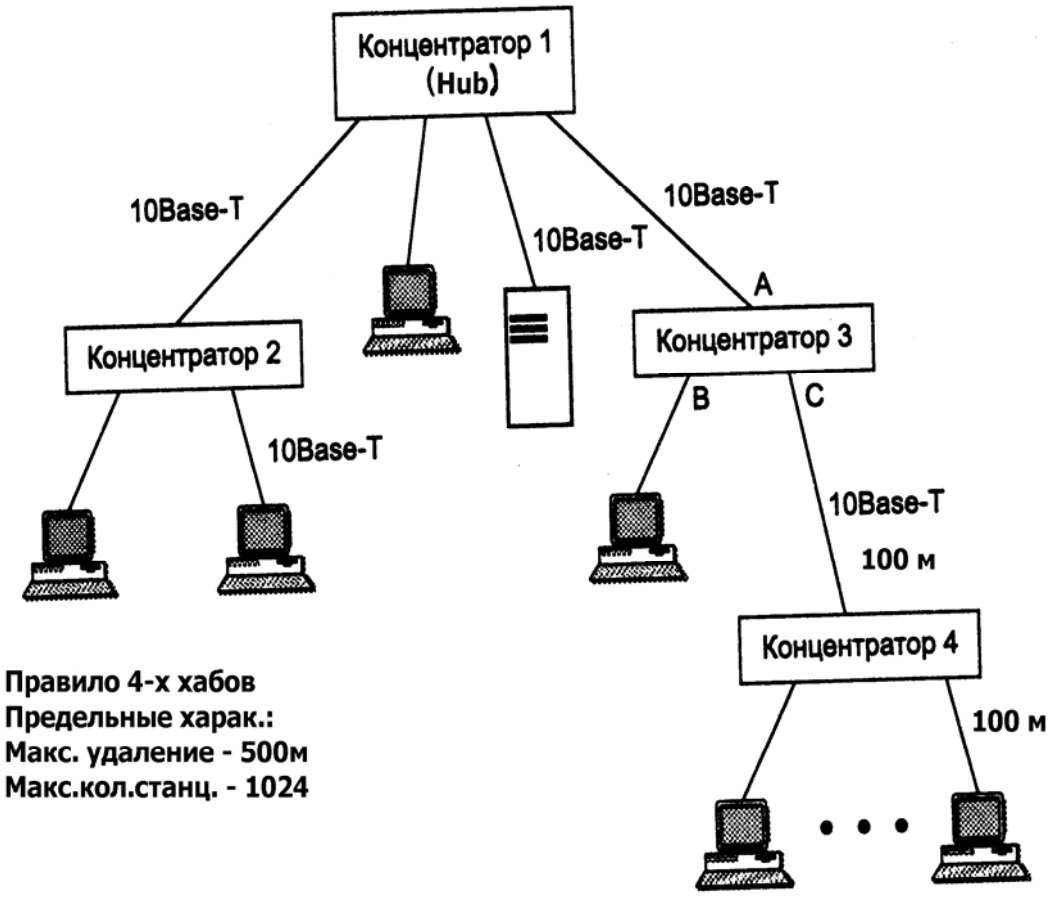
Современный подход к созданию кабельных систем предполагает использование UTP как для компьютерных, так и учрежденческих телефонных сетей. Использование физической топологии «звезда» и организация всех необходимых для работы сети коммутаций в едином центре получило название «структурированная кабельная системама» (СКС).

Стандарты Ethernet кроме UTP допускают применение более дорогой, используемой в технологии Token Ring, экранированной витой пары STP (Shielded Twisted Pair) Type 1A, отличающейся наличием общей экранирующей оболочки.

При построении ЛВС ограничение диаметра сети связано с явлениями затухания сигнала из-за неизбежных потерь, перекрёстными искажениями, отражениями и пр. Согласно принятым соглашениям для корректной работы сети длина соединительного кабеля не должна

превышать 100 м. Для увеличения диаметра сети возможно использование последовательного соединения концентраторов (hub), которые усиливают поступивший от любого узла (другого концентратора) сигнал и повторяют его на всех остальных своих портах (выходах).

Для предотвращения неустранимых коллизий рекомендуется придерживаться «правила 4-х хабов», т. е. в пределах коллизионного домена использовать не более 4 концентраторов.



Правило 4-х хабов не ограничивает размеры сети, т. к. коллизионный домен ограничивается коммутатором (Switch), посылающим пакеты в конкретный порт назначения и не дублирующий его в другие порты, или маршрутизатором (Router), реализующим функции коммутации пакетов на сетевом уровне. Различают также шлюзы (Gateway) – маршрутизаторы, связывающие разнородные сети.

Важным аспектом построения физической среды Ethernet является выбор сетевых адаптеров (NIC – Network Interface Card), устанавливаемых в компьютеры и осуществляющих физический доступ к сети.

Типы шин сетевых адапторов.

Тип шины	Разрадность (бит)	Частота (МГц)	Скорость обмена Мбит/с-Мбайт/с
ISA (Industry Standard Architecture)	16	8,33	66,64-8,33
EISA (Enhanced ISA)	32	8,33	266,56-33,32
MCA (Micro Channel Architecture)	32	10,0	320,0-40,0
VLB (VESA Local Bus)	32	33,33	1066,56-133,33
PCI (Peripheral Connection Interface)	32	33,33	1066,56-133,33

По возможности прямой работы с оперативной памятью компьютера (Bus mastering)

По размеру буферной памяти (стандартно входные и выходные буферы имеют размер 2 кбайта)

По «интеллектуальным» способностям – remote wake up (удалённая активизация).

По режиму обмена: симплекс (только передача или приём), дуплекс (одновременная передача и приём) и полудуплекс (часть времени передача, часть – приём).

По возможности обработки приоритета пакета IEEE 802.1p (QoS – Quality of Service).

Высокоскоростной Ethernet

Fast Ethernet (IEEE 802.3u) – самая распространённая сейчас высокоскоростная технология LAN. С 1992 г. по 1995 г. коалиция фирм 3Com, SynOptics и др. усовершенствовала технологию Ethernet, сохраняя метод доступа CSMA/CD. В 1995 г. IEEE принял дополнение к 802.3 – стандарт 802.3u для скорости 100 Мбит/с, по которому допускается использование в одной сети двух скоростей одновременно (10 и 100 Мбит/с).

Успех технологии во многом связан с возможностью использования (как показано в таблице 2.3.2.1) уже проложенных для обычного Ethernet соединительных кабелей.

Наименование	Кабель	Макс. расстояние до конц. (м)
100BaseT4	UTP Cat.3	100
100BaseTX	UTP Cat.5	100
100BaseFX	Многомод. опт. вол.	2000

Среда 100BaseT4 с использованием UTP Cat.3 применяются довольно редко из-за необходимости одновременной замены всего активного оборудования (концентраторов, коммутаторов, сетевых адаптеров и т. д.) в коллизионном домене. В этом типе физической среды используются все 4 пары кабеля UTP.

Среда 100BaseTX допускает использования в коллизионном домене двухскоростного активного оборудования. Естественно, скорость в 100 Мбит/с будет достигнута только, если оба узла поддерживают эту скорость. Как и в обычном Ethernet сигналы передаются только по 2-м из 4-х пар проводов.

Среда 100BaseFX использует 2 оптические нити.

Концентраторы технологии Fast Ethernet делятся на два касса:

класс I требует наличия портов всех видов (100BaseT4, 100BaseTX/FX)

класса II имеет порты либо типа 100BaseT4, либо типов 100BaseTX/FX

Поскольку концентраторы класса I преобразуют электрические сигналы (увеличение задержки) в пределах коллизионного домена рекомендуется иметь либо 1 концентратор класса I, либо 2 концентратора класса II, расстояние между которыми не должно превышать 5 м. Тем не менее, размеры сети по прежнему не ограничены, т. к. коллизионный домен ограничивается коммутатором, маршрутизатором или шлюзом.

Gigabit Ethernet (IEEE 802.3z/ав) – технология (1998-9 гг.) обеспечивает скорость 1000 Мбит/с и предназначена для локальных сетей с большим трафиком, возникающим, например, при широком использовании мультимедийных приложений, видеоконференций и т. д.

Физическая среда Gigabit Ethernet.

Наименование	Кабель	Макс. расстояние до конц. (м)
1000BaseSX/LX	Вол/опт. кабель	200-500
Twinax	Твинаксиальный кабель	25
1000BaseT	UTP Cat.5 и выше	100

Среда 1000BaseSX/LX согласно стандарту IEEE 802.3z (1998 г.) представляет собой коротковолновый (S –short) или длинноволновый (L –long) волоконно-оптический кабель.

Среда Twinax – двойной коаксиальный кабель применяется для соединения концентраторов/маршрутизаторов.

Среда 1000BaseT по стандарту IEEE 802.3ав (1999 г.) есть витая пара на ниже 5 категории. Для передачи сигналов в этой среде используется все 4 пары проводов. При

прокладке кабеля предъявляются особые требования по недопущению резких изгибов, близости силовых установок и т. д.

В пределах коллизионного домена рекомендуется иметь не более 1-го концентратора технологии Gigabit Ethernet.

В настоящее время комитетом 802 IEEE активно ведутся работы по стандартизации технологии 10 Gigabit Ethernet (IEEE 802.3ae).

Технологии удалённого доступа

Под удалённым доступом понимается предоставление ресурсов сети с использованием общедоступных, чаще всего телефонных каналов связи. Наиболее проблемным участком таких каналов является участок от абонента до телефонной станции. В городах это расстояние не превышает 1,5-2 км, т. е. около 1 мили, это и послужило причиной использования для обозначения участка термина «Последняя миля».

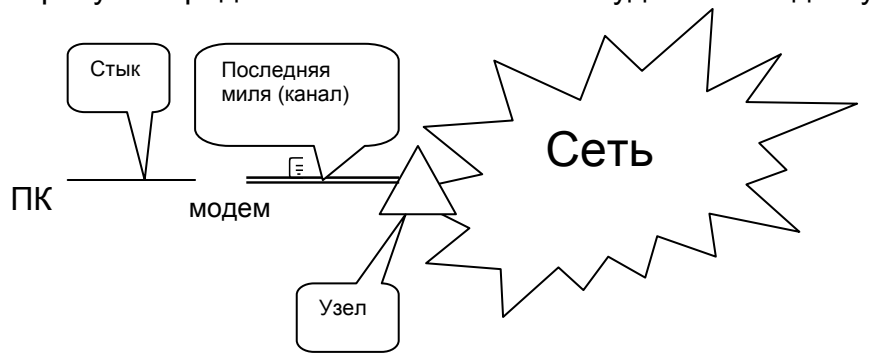
Проблема последней мили заключается в достижении возможно высокой скорости передачи информации при существующих ограничениях на полосу канала связи и величину отношения сигнал/шум, поскольку оба эти параметра по формуле Шеннона влияют на пропускную способность канала $C = F \log_2(1+ Pc/Pш)$ бит/с, где F — ширина полосы канала, Pc/Pш — отношение сигнал/шум.

К наиболее популярным и/или перспективным каналам относятся:

проводные каналы общественной телефонной сети

радиоканалы каналы сотовой связи

На рисунке представлена типовая схема удалённого доступа к сети.



Соединение персонального компьютера (ПК) с модемом (модулятором-демодулятором), осуществляющим обмен данными по каналу связи, называется стыком. Термин «стык» или «интерфейс» означает соединение двух отдельных устройств. В случае передачи данных для обозначения этих устройств используются аббревиатуры DTE (Data Terminal Equipment – цифровое терминальное устройство, т. е. ПК) и DCE (Data Circuit-Terminal Equipment – оконечное оборудование линии передачи данных, т. е. модем).

Наиболее популярными и/или перспективными стыками являются.

Стык по (последовательному) COM порту.

Название происходит от COMmunication Port и подразумевает обмен информацией последовательно бит за битом. Традиционные операционные системы персональных компьютеров поддерживают 4 COM порта, два из которых имеют 9 (DB-9) или 25 (DB-25) контактные разъёмы на задней стенке корпуса, а два других предназначены для работы со встраиваемыми устройствами. Стык рассчитан на скорости до 115,2 кбит/с и длину соединительного кабеля до 20 м (50 футов). Механические параметры разъёмов, а также назначения сигналов и их электрические характеристики описываются весьма близкими стандартами RS-232, V.24/V.28 и X.21.

Стандарт RS-232 принят EIA (Electronics Industries Association – Ассоциация электронной промышленности США). Наиболее распространенная версия обозначается как RS-232C.

Стандарты V.24/V.28 (электро-механические характеристики/назначение сигналов) приняты ITU-T (CCITT) в форме рекомендаций для устройств передачи данных, а стандарт X.21 принят ITU-T (CCITT) в рамках стека протоколов X.25 (физический уровень стека). Наиболее близка к перечисленным выше стандартам версия X.21bis.

Стык по порту USB (Universal Serial Bus) – универсальная последовательная шина, предусматривает обмен со скоростями 1,5 Мбит/с или 12 Мбит/с (USB версий 1.0 и 1.1 соответственно), а также 480 Мбит/с (USB версии 2.0). Стык допускает подключение до 127 различных устройств при длине соединительного кабеля 24 AWG до 14 м.

Стык Bluetooth (голубой зуб) получил своё название от прозвища датского короля X века н. э. Гарольда Блаатанда (Harald Blaatand), который принёс христианство в Скандинавию и объединил Данию и Норвегию. В качестве логотипа Bluetooth используется руническая запись инициалов короля.

Технология представлена компанией Ericsson в 1994 г. для соединения по радиоканалу гарнитуры и сотового телефона. Bluetooth предусматривает организацию пикосети (сверхмалой сети) из 7 узлов (1 узел главный и до 6 подчинённых узлов) с методом доступа опрос по логической топологии «звезда». Для соединения узлов пикосети может быть использовано до 79 радиоканалов в диапазоне 2,4 ГГц при скорости обмена до 720 кбит/с. Допустимые расстояния между узлами в основном зависят от мощности используемых передатчиков, которые делятся на 3 класса:

- класс 1 включает в себя передатчики с мощностью от 1 мВт до 100 мВт и обеспечивает соединение на расстоянии несколько сот метров
- класс 2 – передатчики с мощностями от 0,25 мВт до 2,4 мВт для соединения на десятки метров
- класс 3 – предусматривает мощность передатчика до 1 мВт для соединений до 10 метров

Стек протоколов TCP/IP

Несмотря на короткое с исторической точки зрения время существования компьютерных сетей и наличие разнообразны стеков, разработанных отдельными фирмами (например, стек IPX/SPX фирмы Novell) или международными организациями (например, X.25 ITU-T), к настоящему моменту определился доминирующий набор протоколов, используемых как в LAN, так и сети Internet и названных «стек TCP/IP». Это обстоятельство, а также особенности программы обучения заставляют остановиться на рассмотрении только этого стека.

Стек TCP/IP получил своё название от основных протоколов TCP (Transmission Control Protocol) и IP (Internet Protocol), разработанных в 70-е г. в рамках проекта сети ARPANET Министерства обороны США. Основные принципы TCP сформулированы Винтом Серфом (V. G. Cerf) и Бобом Каном (R. F. Kahn) в работе «A protocol for packet network interconnection» (IEEE Transaction on Communications, Vol. COM-22, № 5, 1974). Стек задумывался и разрабатывался как средство объединения компьютеров с различными характеристиками и операционными системами. Большое значение для популярности имела поддержка стека в операционной системе UNIX FreeBSD (Университет Беркли) .Модель стека была разработана до появления модели OSI и насчитывает меньшее количество уровней.

<table>
<tr><th>Уровни OSI</th><th>Протоколы стека TCP/IP</th><th>Уровни стека TCP/IP</th></tr>
<tr><td>Прикладной (Application)</td><td rowspan="3">HTTP, FTP, Telnet, …</td><td rowspan="3">Прикладной (Application)</td></tr>
<tr><td>Представительный (Presentation)</td></tr>
<tr><td>Сеансовый (Session)</td></tr>
<tr><td>Транспортный (Transport)</td><td>TCP, UDP</td><td>Транспортный (Transport)</td></tr>
<tr><td>Сетевой (Network)</td><td>IP, ARP, ICMP, RIP, OSPF, …</td><td>Сетевой (Network)</td></tr>
<tr><td>Канальный (Data Link)</td><td rowspan="2">Технологии (Сетевые интерфейсы) Ethernet, ATM, …</td><td rowspan="2">Физический (Physical)</td></tr>
<tr><td>Физический (Physical)</td></tr>
</table>

Приведём краткую характеристику основных протоколов стека.

HTTP (Hyper Text Transfer Protocol) – протокол передачи гипертекстовых документов используется для реализации приложений WWW (Word Wide Web) «всемирной паутины». Первый графический интерфейс для доступа к гипертекстовым документам появился в 1993 г. и носил название Mosaic (автор интерфейса Марк Андрессен (Mark Andressen) в 1995 г. основал Netscape Communications Corp.). В 1994 г. Европейский центр ядерных исследований (CERN — Conseil Europeen pour la Recherche Nucleaire) и Массачусетский технологический институт (M. I. T. — Massachusetts Institute of Technologies) основали некоммерческую организацию WWW Consortium для развития Web приложений.

FTP (File Transfer Protocol) – протокол передачи и приёма файлов.

Telnet – протокол эмуляции удалённого терминала.

TCP (Transmission Control Protocol) – протокол передачи данных с установлением соединения и обеспечением целостности доставки.

UDP (User Datagram Protocol) – протокол передачи данных без установления соединения и обеспечения целостности доставки.

IP (Internet Protocol) – базовый протокол доставки пакетов между узлами.ARP (Address Resolution Protocol) – протокол распознавания адреса, предназначенный для определения MAC-адреса узла с заданным IP адресом. Помимо определения MAC адреса для заданного IP адреса представляет интерес и обратная задача – по MAC адресу определить IP адрес. Для решения этой задачи существует протокол RARP (Reverse ARP). Более подробную информацию о протоколах ARP, Proxy ARP и связанных с этими протоколами вопросах можно найти в [4, с. 93-98].ICMP (Internet Control Message Protocol) – протокол пересылки диагностических сообщений о нарушениях работы сети.RIP (Routing Information Protocol) – «простой» протокол обмена информацией между маршрутизаторами. Применяется в небольших сетях, т. к. допускает не более 14 маршрутизаторов и использует широковещательные (групповые) запросы о состоянии маршрутизаторов каждые 30 с. Существенным недостатком протокола является возможность движения пакетов по замкнутому маршруту — петле.OSPF (Open Shortest Path First) – протокол обмена информацией между маршрутизаторами в больших сетях.

Пакет IP

Структура IP пакета.

32 бита (4 байта)

1 2 3 4 5 6 7 8		1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Версия	Длина заг.	Тип службы	Общая длина пакета	
Идентификатор пакета			D	M	Смещение фрагмента
Время жизни		Протокол	Контрольная сумма	
IP адрес источника				
IP адрес получателя				
Дополнительные параметры				
Данные				
…….				
Данные				

В связи с тем, что стек разрабатывался для операционной системы UNIX, пакет принято разбивать на 4 байтовые (32 битные) слова, содержимое которых приведено ниже.

Версия. Сейчас используется 4-я версия (IPv4) протокола. Наметившийся дефицит IP адресов разрешился принятием 6-й версии (IPv6) с 16 байтовыми (64-х битовыми) полями адресов, штатными мерами защиты и пр. В настоящее время поддержка (IPv6) опциональна.

Длина заголовка. Количество 4-х байтовых слов в заголовке пакета. Минимальное значение – 5 (заголовок минимальной длины – 20 байт). Более длинные заголовки используются, например, при фиксированных маршрутах и перечислении адресов узлов следования пакетов.

Тип службы. Это поле содержит информацию о приоритете пакета, желаемом режиме обработки пакета в маршрутизаторах и пр. На практике это поле чаще всего игнорируется маршрутизаторами.

Общая длина пакета (заголовок + данные) в байтах. Максимальное количество данных в пакете составляет 216-1 — 20=65 535 – 20 ≈ 64 кбайт. Минимальное значение – 21.

Идентификатор – 16-и битовая метка пакета, используемая для идентификации пакета в случае его фрагментации.

D (Do not fragment) – флаг запрета фрагментации (D=1 – флаг установлен и фрагментация запрещена).

M (More fragments) – флаг не последнего фрагмента пакета (M=1 – флаг установлен и пакет не является последним).

Смещение фрагмента задаёт в 8-и байтовых словах положение блока данных текущего пакета от начала не фрагментированного (исходного) пакета. Значение для всех фрагментированных пакетов (кроме последнего) должно быть кратно 8. Максимальное значение поля – 213=8 192 (первый фрагмент имеет смещение 0), что в 8-и байтовых словах обеспечивает максимальную длину пакета 8*8 192= 64 356 байт (на 1 байт больше, чем даёт поле Общая длина пакета).

Время жизни (TTL — Time To Live) – счётчик, ограничивающий время жизни пакета. При прохождении каждого маршрутизатора вычитается 1 + время ожидания в очереди в целых секундах. В современных маршрутизаторах время ожидания в очереди существенно меньше секунды. В маршрутизаторе, где значение поля становится равным 0, пакет уничтожается, а отправителю посылается сообщение об этом. Максимальное значение поля – 255. Поскольку при правильной работе реальных сетей (даже глобальных) количество маршрутизаторов редко превышает 30, в некоторых реализациях стека ограничиваются значением 128 (например, MS Windows).

Протокол определяет вышестоящий протокол, которому предназначены данные пакета.

Контрольная сумма вычисляется в 4-х байтовых словах и только для заголовка. При обнаружении ошибки пакет уничтожается. В каждом маршрутизаторе контрольная сумма пересчитывается.

IP адрес источника – 4-х байтовый адрес узла, из которого пакет был послан.

IP адрес получателя – 4-х байтовый адрес узла, к которому пакет был послан.

Дополнительные параметры – необязательное поле, содержащее дополнительные параметры, например, адреса узлов следования пакета при фиксированном маршруте. Поле дополняется нулями до целого числа 4-х байтовых слов.

Данные – переносимая пакетом информация, полученная от протокола вышележащего уровня. Поле дополняется нулями до целого числа 4-х байтовых слов.

Адресация в IP сети

Адреса в IP сетях состоят из [1, с. 495-507; 2, с. 440-442; 3, с. 326-337; 4, с.67-74]:

физического адреса узла – MAC адреса (физический уровень);

сетевого адреса – IP адрес (сетевой/транспортный уровень);

символьный адрес – DNS (Domain Name System) имя (прикладной уровень) или доменное имя используется для удобства запоминания. Связь между DNS именем и IP адресом устанавливается службой DNS.

Остановимся на полном сетевом IPv4 адресе, который представляет собой три 4-х байтовых числа:

адрес. Например, 192.168.3.11

маска. Например, 255.255.255.0

шлюз. Например, 192.168.3.1

Используется несколько форм записи байтов IP адреса:

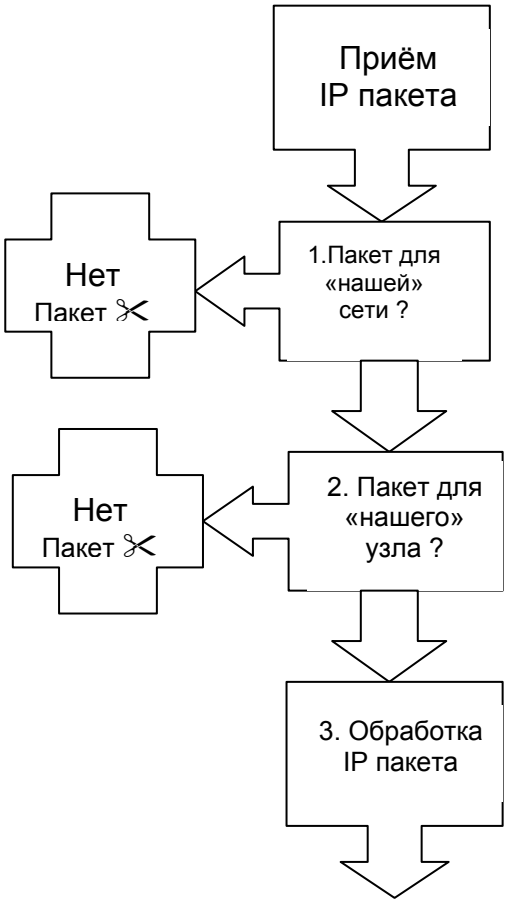
Десятичная нотация (наиболее употребительная) – значения чисел в каждом байте записываются как десятичные числа от 0 до 255=28-1 включительно.

Двоичная нотация — значения чисел в каждом байте записываются как двоичные числа от 0000 0000 до 1111 1111 включительно.

Шестнадцатиричная нотация — значения чисел в каждом байте записываются как шестнадцатиричные числа от 00 до FF включительно.

Маска служит для отделения в IP адресе номера сети от номера узла.

Смысл маски IP адреса можно понять, рассмотрев представленные на рисунке действия узла при приёме пакета.



На адрес назначения накладывается маска и определяется номер сети узла назначения. Термин «накладывается» означает побитовое логическое умножение (операция «И») 4-х байтового IP адреса на 4-е байта маски. Например,

IP адрес 192.168.3.187 (1100 0000.1010 1000.0000 0011.1011 1011)

маска 255.255.255.240 (1111 1111.1111 1111.1111 1111.1111 0000)

результат наложения (номер сети)

192.168.3.176 (1100 0000.1010 1000.0000 0011.1011 0000)

Если номер сети не «наш», пакет игнорируется. Если сеть «наша», то выполняется следующий шаг.

Проверяется:

совпадение своего номера узла и номера узла назначения или

наличие признака широковещательной рассылки. Адрес широковещательной рассылки имеет значения 1 в битах, относящихся к номеру узла (хоста). Для примера из предыдущей ссылки это 192.168.3.191 (1100 0000.1010 1000.0000 0011.1011 1111)

Если ни одно из условий не выполняется, то пакет игнорируется. Если хотя бы одно из условий выполняется, то выполняется следующий шаг.

Пакет обрабатывается согласно IP протоколу.

Шлюз – это адрес узла, которому посылается пакет при невозможности определения MAC адреса узла назначения.

Иногда используют более экономичную объединённую запись адреса и маски, указывая через знак «/» количество единичных старших разрядов маски. Для рассмотренного примера объединение адреса 192.168.3.11 и маски 255.255.255.0 это приводит к записи вида 192.168.3.11/24.

Иногда используют классовую систему деления адресов. По этой классификации сети делятся на 5 классов.

Класс А. Первый бит – 0. Маска 255.0.0.0. Диапазон от 1.0.0.0 до 126.255.255.254. Диапазон от 0.0.0.0 до 0.255.255.255 зарезервирован для специальных целей. Например, адрес 0.0.0.0 – внутренний адрес любого узла. Диапазон от 127.0.0.0 до 127.255.255.255 – для интерфейсов обратной связи. Например, адрес 127.0.0.1 – традиционная «заглушка» для тестирования стека. Всего различных номеров сетей – 125, в каждой сети может быть до (28*28*28-2)=16 777 214 узлов Номер x.0.0.0 используется для обозначения всей сети, а номер

x.255.255.255 – для широковещательной рассылки. Для локальных сетей отведён диапазон от 10.0.0.0 до 10.255.255.255.

Класс B. Первые биты – 10. Маска 255.255.0.0. Диапазон от 128.0.0.0 до 191.255.255.254. Общее количество номеров сетей – 26*28=16 384, в каждой сети может быть (28*28-2) = 65 534 узла. Для локальных сетей отведён диапазон от 172.16.0.0 до 172.31.255.255 (172.16.0.0/12).

Класс C. Первые биты – 110. Маска 255.255.255.0. Диапазон от 192.0.0.0 до 223.255.255.254. Номеров сетей – 25*28*28= 2 097 152, в каждой сети может быть (28-2) = 254 узла. Для локальных сетей отведён диапазон от 192.168.0.0 до 192.168.255.255.

Класс D. Первые биты – 1110. Групповые/широковещательные адреса. Диапазон от 224.0.0.0 до 239.255.255.255. Для локальных сетей отведён диапазон от 239.0.0.0 до 239.255.255.255.

Класс E. Первые биты – 11110. Зарезервированные адреса. Диапазон от 240.0.0.0 до 247.255.255.255.

В сетях с большим (свыше 100 компьютеров) количеством узлов целесообразным является использование протокола DHCP (Dynamic Host Configuration Protocol) автоматической раздачи IP адресов и одноимённой службы.

Протокол UDP

Протоколы UDP и TCP относятся к транспортному уровню модели стека TCP/IP.

Протокол UDP (User Datagram Protocol) не требует подтверждения получения, не обеспечивает гарантированности доставки и, следовательно, целостности переданных данных (сборки данных из разных пакетов). Протокол используется для передачи команд и сетевой информации (например, при разрешении имен в DNS), а также для передачи вышележащим протоколам, обеспечивающим гарантированность доставки и целостность данных своими средствами.

←——— Слово 32 бита (4-е байта) ———→	
Порт источника	Порт получателя
Длина	Контрольная сумма
Данные	
….	
Данные	

Порты источника и получателя – 16-и битовые (2-х байтовые) идентификаторы прикладных протоколов источника и получателя соответственно. Эти идентификаторы необходимы для разделения данных при одновременной работе различных прикладных процессов. Например, при одновременном приёме файлов (протокол FTP) и просмотре web-страницы (протокол HTTP) на одном и том же узле. За известными протоколами (по умолчанию) закреплены первые 1024 порта (например, FTP – 21 порт, HTTP – 80 и т. д.), но номера портов могут быть и переназначены произвольным образом. Совокупность прикладного протокола, IP адресов и номеров портов узлов назначения и источника называется сокетом (socket – гнездо). В сокете номер порта указывается за IP адресом после двоеточия (например, 212.46.206.2:80).

Длина – длина всего (с заголовком) UDP пакета. Максимальная длина UDP пакета есть максимальный размер данных в IP пакете минус минимальная длина заголовка UDP пакета, т. е. (65 535 – 20) – 8 = 65 507 байт.Контрольная сумма – дополнение до нуля всех двухбайтовых слов пакета и псевдозаголовка. Перед заголовком для повышения надёжности вставляется псевдозаголовок из важнейших полей заголовка IP пакета

IP адрес источника		
IP адрес получателя		
0	Протокол	Длина

Протокол – идентификатор протокола (например, 17 – UDP, 6 – TCP).

Длина – длина UDP/TCP пакета.

Протокол TCP

TCP (Transmission Control Protocol) протокол обеспечивает сквозную доставку данных прикладным процессам на взаимодействующих по сети узлах. TCP — надёжный потоковый протокол с установлением соединения и последующим двунаправленным обменом данными. Смысл приведённых характеристик поясняет представленная в таблице 3.4.1 структура TCP пакета.

Source Port, Destination Port, Checksum, Data имеют тот же смысл, что и поля порт источника, порт получателя, контрольная сумма и данные в структуре UDP пакета.

SN – порядковый номер первого байта в поле данных пакета среди байтов передаваемого файла в текущем соединении. Например, если в TCP пакете в поле данных содержатся байты с 2001 по 3000, то SN=2001. После достижения максимально возможного значения (232-1) нумерация байтов начинается с 0. При использовании пакета для подтверждения (данные не передаются) в поле SN записывается увеличенный на 1 номер последнего переданного байта.Таблица 3.4.1. Структура TCP пакета.

←Слово 32 бита (4-е байта)→																															
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Source Port																Destination Port															
Sequence Number (SN)																															
Acknowledgment Sequence Number (ACK SN)																															
Data Offset				0						U	A	P	R	S	F	Window															
Checksum																Urgent Pointer															
Options (Padding)																															
Data																															
….																															
Data																															

ACK SN – порядковый номер ожидаемого байта, т. е. предыдущие байты до ACK SN – 1 включительно приняты успешно. Поле имеет смысл при установленном флаге A.

Data Offset – длина заголовка TCP пакета в 32-битных словах. Минимальное значение поля равно 5 (поле options отсутствует), максимальное – 15 (60 байт).

Флаги:

U – активизировано (имеет смысл) поле Urgent Pointer.

A – активизировано (имеет смысл) поле ACK SN.

P – немедленное выталкивание данных из буфера процессу-получателю.

R – аварийный разрыв соединения и очистка всех буферов.

S – запрос на установление соединения.

F – последний пакет с данными.

Window – размер окна в байтах. Для ускорения процесса передачи в протоколе TCP используется метод скользящего окна. Этот метод позволяет источнику передавать пакеты, не дожидаясь прихода подтверждения приёма предыдущих данных. Объём в байтах передаваемых таким образом данных и определяет значение поля. Значение поля задает получатель в пакете-подтверждении. Источник последовательно отправляет данные в TCP пакетах в пределах окна до получения подтверждения со значениями ACK SN и Window. После получения подтверждения байты до ACK SN – 1 считаются переданными и удаляются из буфера. Тем временем, байты данных продолжают передаваться в пределах указанного в поле Window количества. Если объём переданных и неподтверждённых данных достиг

значения окна (Window), то передача прекращается до получения подтверждения. Если источник получает пакет-подтверждение со значением ACK SN меньшим, чем он принял раньше (заблудившийся пакет), то этот пакет игнорируется.

Urgent Pointer – указатель (pointer) длины в байтах строчных (urgent) данных перед отправляемыми данными. Эти строчные данные могут быть использованы для задания режима работы прикладного процесса-получателя. Значение поля имеет смысл при установленном флаге U.

Options – необязательное поле опций дополнительных услуг протокола. Максимальный размер поля – 40 байт. При использовании поля оно всегда дополняется (padding — набивка) нулевыми байтами до целого числа 4-байтовых слов.

Протокол FTP

Протокол FTP (File Transfer Protocol) является одним из старейших протоколов стека TCP\IP.

Этот протокол для передачи файлов использует два TCP соединения, одно — для передачи команд (порт 21 на стороне клиента) и второе — для передачи данных (порт 20 на стороне сервера). Соответствующие порты приёма данных на стороне клиента и приёма команд на стороне сервера устанавливаются в процессе инициации FTP сеанса.

Возможны два режима работы – активный и пассивный. В первом — клиент ждёт передачи данных (сервер инициирует TCP соединение для передачи данных, он активен), во втором – активен клиент. Так, в активном режиме при открытии FTP сеанса клиент открывает пассивное TCP соединение, находящееся в ожидании активности сервера (состояние LISTEN), и задаёт порт для приёма данных. В свою очередь, сервер, получив номер этого порта, начинает передавать на него пакеты с данными. В пассивном режиме, наоборот, сервер сообщает клиенту номер порта передачи данных и ждёт соединения.

Комбинируя пассивный и активный режимы клиент может организовать прямую передачу файлов между серверами как показано на рисунке 3.5.1.1.

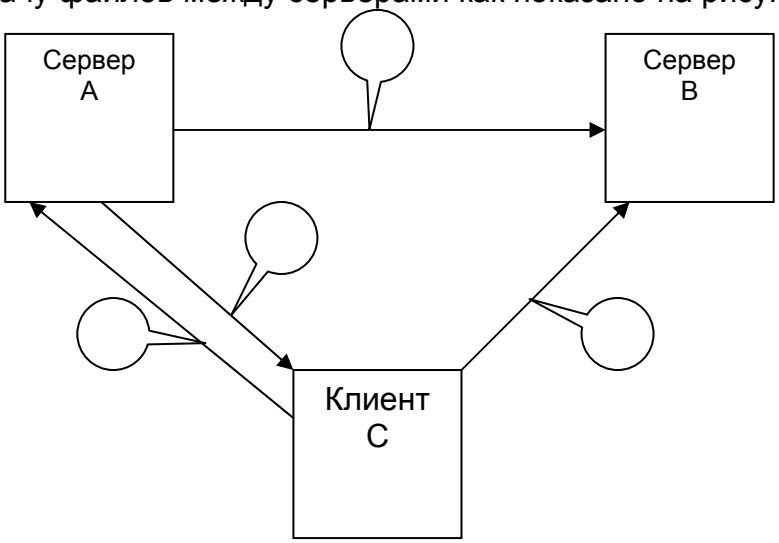


Рис. 3.5.1.1. Пряма передача файлов между серверами с помощью FTP.

Организация прямой передачи файлов между серверами реализуется в 4-е шага:

Клиент C задаёт пассивный режим серверу A.

В ответ получает от него IP адрес и порт для передачи данных.

Клиент C задаёт серверу B активный режим и указывает IP адрес и порт сервера A для передачи данных.

Сервер B инициирует TCP соединение для передачи данных с сервера A и после установления этого соединения сервер A передаёт данные серверу B.

Возможность управления работой сервера клиентом таит реальную угрозу безопасности не только самого сервера, но и других серверов в сети. По этой причине, чаще всего, активный режим запрещён для использования.

К сожалению, при установке сеанса FTP, имя пользователя и его пароль передаются открытым образом. Для повышения безопасности в FTP предусматривается сеанс с

анонимным пользователем (anonymous), имеющим ограниченные администратором сервера права.

Протокол HTTP

Протокол HTTP (Hyper Text Transfer Protocol) является базовым для службы WWW (World Wide Web) доступа к документам с гипертекстовым ссылками. Согласно этому протоколу для каждой новой ссылки открывается новое TCP соединение, использующее по умолчанию 80 порт.

Протокол предполагает задание URL (Uniform Resource Locator – метки) ресурса программе браузера (например, MS Internet Explorer) в качестве параметра. По URL браузером формируется запрос в форме URI (Uniform Resource Identifier) – идентификатора запрашиваемого ресурса, полный формат которого можно встретить в таких протоколах прикладного уровня, как FTP или протоколы для электронной почты.

Формат URL предусматривает следующий набор параметров, разделённых знаками «//», «:», «@», «/», «#» и «?» -

http://user: password@www. server: port/path#fragment? query

Эти параметры (аргументы) имеют следующий смысл:

user: password – имя пользователя и его пароль. Как правило, не указываются, даже если для доступа к ресурсу требуется аудентификация. В случае ограничения прав пользователей на ресурс, запрос без параметров user: password вызовет ответ сервера WWW ресурса с кодом ошибки 401, по которому браузер сгенерирует запрос пользователю о его имени и пароле и сформирует новый запрос на ресурс уже с указанием этих параметров. Причина использования такого механизма авторизованного запроса кроется в том, чтобы не передавать параметры user: password в явном виде. Предусмотрено два способа аудентификации – без криптографической защиты (схема Basic) и с защитой (схема Digest – дневник, краткое изложение, слепок – термин, широко употребляемый в криптографии).Схема Basic предполагает преобразование строки user: password по алгоритму Base64. Этот алгоритм применяется в электронной почте для записи присоединённых файлов с произвольными двоичными данными в виде набора латинский букв, знаков и цифр, т. е. в виде хотя и неосмысленного, но текста. По этому алгоритму преобразуемые данные разбиваются на блоки по 24 бита (3 байта), каждый блок делится на 4 группы по 6 битов в каждой. Каждая группа отождествляется с символом (байтом) буквы латинского алфавита, цифры или специального знака. Легко заметить, что алгоритм Base64 представляет собой алгоритм канального кодирования с избыточностью 25 % (скоростью 0,75), что приводит к увеличению передаваемых данных на ¼.Схема Digest предусматривает шифрование параметров user: password по алгоритму MD5 (Message Digest версии 5). Этот алгоритм представляет собой процедуру вычисления хэш-функции, по которой данные произвольной длины преобразуются в 128 бит (16 байт). Краткое описание MD5 можно найти, например, в www. server: port — доменное имя и порт (80 по умолчанию) WWW-сервера.path – путь к файлу-ресурсу (index. html по умолчанию).fragment – метка внутри документа (начало по умолчанию).query – аргумент запроса.

Протокол Telnet

Telnet – базовый протокол ОС UNIX, обеспечивающий терминальный доступ пользователей к удалённому компьютеру [4, с. 423-433].

Первоначально терминалом являлось устройство типа пишущей машинки, на котором оператор (пользователь) печатал команды и наблюдал результаты. Позднее терминал разделили на монитор и клавиатуру.

По умолчанию в Telnet используется 23 порт. На удалённом компьютере должна быть запущена серверная часть, а на компьютере пользователя – клиентская. Клиентская программа носит то же название – telnet и допускает ввод параметров из командной строки. К этим параметрам относятся:

Имя (IP адрес) сервера и номер порта

Тип текстового терминала

Имя пользователя

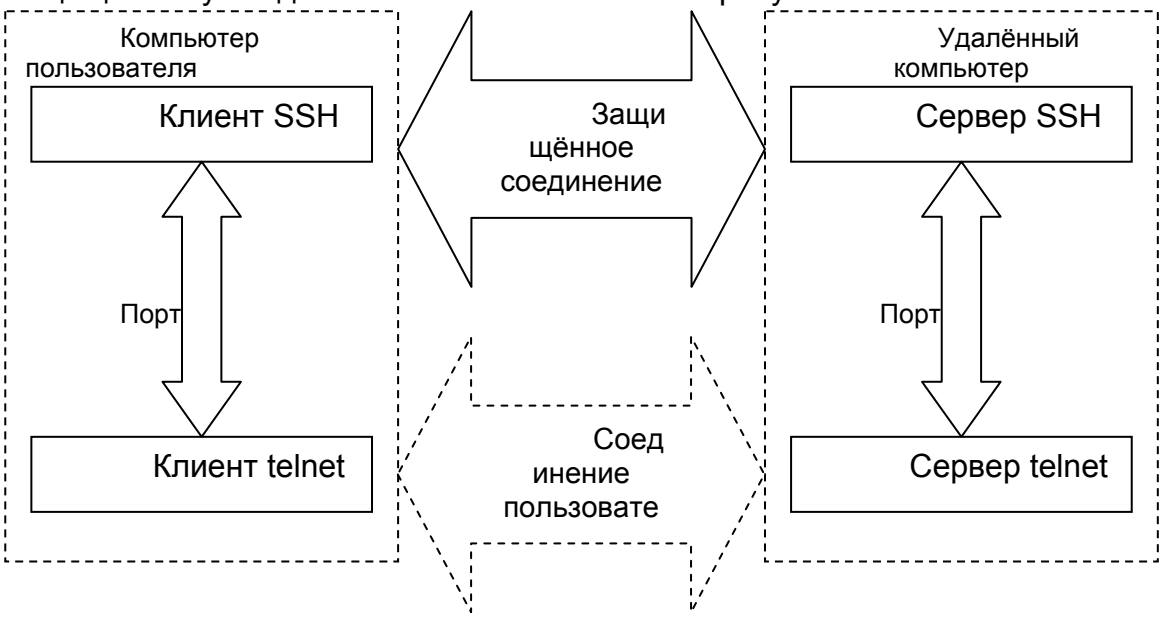
Имя журнала соединения

Определение действий некоторых функциональных клавиш клавиатуры и др.

Синтаксис командной строки зависит от программной реализации telnet и с этой точки зрения telnet можно рассматривать как службу или сервис.

Работа протокола telnet предусматривает передачу серверу (удалённому компьютеру) по протоколу TCP каждого набранного пользователем знака в отдельном пакете. В случае включённого эха сервер возвращает знак на монитор пользователя. Результаты выполнения запущенных на сервере программ передаются уже блоками. В пределах прав пользователя и возможностей терминала telnet обеспечивает полный доступ к программам и файлам сервера. При установлении соединения в процессе аудентификации символы имени пользователя и пароля передаются в открытом виде, что делает использование telnet крайне опасным.

Наиболее популярный метод повышения безопасности прикладных терминальных протоколов (например, telnet) является протокол SSH (Secure SHell), использующий 22 порт по умолчанию. Так же, как и в telnet, на удалённом компьютере запускается серверная часть SSH, а на пользовательском компьютере – клиентская. После установления соединения все данные передаются в зашифрованном виде и все данные прикладных протоколов туннелируются по этому защищённому соединению как это показано на рисунке 3.5.3.1.



Перед использованием telnet удалённый компьютер и компьютер пользователя устанавливают защищённое соединение по 22 порту (подразумевается, что до использования SSH в клиентской и серверной части уже определены пароли криптографической защиты). При вызове telnet открывается 23 порт, но передаваемые пакеты перехватываются клиентом SSH, шифруются и отправляются по защищённому каналу. Сервер SSH расшифровывает данные и по 23 порту передаёт серверу telnet. Реакция сервера передаётся в обратном порядке. Пользователь не ощущает работы протокола SSH и работает как с обычным клиентом telnet по 23 порту.

Протоколы электронной почты

Электронная почта (E-mail) – один из старейших и наиболее распространённых сетевых сервисов, популярных как в локальных, так и глобальных сетях [2, с. 673-701; 4, с.461-486].

Система электронной почты появилась в 1982 г. как сервис предка Internet сети ARPANET. Эта система значительно отличалась от принятых CCITT рекомендаций серии X.400. Сложность рекомендаций X.400 и их непродуманность привели к редкому для сетевых технологий случаю, когда инициативная разработка победила международный стандарт. Службы электронной почты, отвечающие X.400, не нашли широкого применения и представляют скорее научный интерес.

Электронное почтовое сообщение, как и в обычной почте, содержит конверт с необходимой для доставки информацией, заголовка с полезными для автоматизированной обработки адресатом данными и собственно сообщения.

Конверт и заголовок имеют формализованные поля. Наиболее важными из них являются (обязательные для заполнения отправителем поля выделены жирным шрифтом):

To: — адрес (а) получателя (лей) в формате имя_ящика@имя_почтового_сервера

Cc: — (carbon copy) адрес (а) дополнительного (ных) получателя (лей)

Bcc: — (blind carbon copy) слепой (ые) адрес (а) получателя (лей), о которых другим не сообщается

From: — адрес автора письма (кому можно отвечать)

Sender: — адрес отправителя письма

Received: — поле, куда при прохождении каждого узла добавляется имя узла, дата и время приёма

Return-Path: — имена узлов на пути письма

Date: — дата и время отправки письма

Reply-to: — адрес, куда надо ответить

Message-id: — уникальный идентификатор письма (для ссылок)

In-Reply-id: — идентификатор письма, на которое даётся ответ

Subject: — тема письма

Предусматривается возможность введения автором письма собственного поля, которое должно начинаться с X

Тело сообщения представляет собой набор строк из не более, чем 1000 (рекомендуется до 78) ASCII (American Standard Code for Information Interchange) знаков, т. е. 7-и битных чисел, представляющих буквы латинского алфавита, знаки препинания и цифры (популярным для такого представления является термин «кодировка»). Символы национальных кодировок (например, знаков кириллицы), двоичные файлы (например, с аудио, или видео информацией) и др. отображаются в соответствии с соглашением MIME (Multipurpose Internet Mail Extension – многоцелевые расширения электронной почты в Интернете), которое предусматривают поле с указанием способа кодировки (например, Base64 – см. параграф 3.5.2).

Базовым методом обеспечения конфиденциальности электронной почты является её криптографическая защита. Наиболее популярная система именуется PGP (Pretty Good Privacy — достаточно хорошая конфиденциальность). Эта система предложена Филом Циммерманом (Phil Zimmerman) и предусматривает использование нескольких алгоритмов шифрования (RSA, IDEA, MD5).

Другая система носит название PEM (Privacy Enhanced Mail – почта повышенной секретности) и отличается от PGP необходимостью связи с центрами сертификации ключей, меньшей степенью защиты (для кодирования данных в системе PGP используется ключи длинной 128 бит, а в системе PEM – только 56 бит), но полным соответствием рекомендациям ITU-T (X.400 и X.509).

Протоколы электронной почты характеризуются значительным разнообразием от фирменных, пригодных в программных продуктах конкретных фирм-производителей, до общепризнанных. Речь идёт о протоколах именно систем электронной почты, а не о распространённых системах эмуляции почтовых служб на базе протокола HTTP (см., например, www. mail. ru).

Среди почтовых протоколов можно выделить:

SMTP (Simple Mail Transfer Protocol – простой протокол электронной почты) – протокол, используемый для обмена почтой между узлами и отправки писем от клиента к почтовому серверу. По умолчанию протокол использует 25 порт.

POP3 (Post Office Protocol v.3 –протокол электронной почты версии 3) – протокол для получения почты клиентом. По умолчанию протокол использует 110 порт.

IMAP v4 (Internet Message Access Protocol v.4 –протокол интерактивного доступа к электронной почте версии 4) – протокол, аналогичный POP3, но позволяющий клиенту хранить и обрабатывать почту на самом почтовом сервере. По умолчанию протокол использует 585 порт

Протокол SMNP

Протокол SNMP (Simple Network Management Protocol – простой протокол сетевого управления) первоначально разрабатывался для управления маршрутизаторов, но затем был расширен на любые сетевые устройства (по умолчанию порты 161/162). В настоящее время актуальна версия 2 протокола (1999 г.) [1, с. 791-805; 2, с.660-672].

Протокол построен по принципу клиент — сервер (на управляемом сетевом устройстве должна быть запущена программа клиента) и включает в себя протокол управления (взаимодействие управляемого и управляющего узлов), язык ASN.1 (Abstract Syntax Notation v.1 — абстрактная синтаксическая нотация версии 1) описания модели управления и собственно модель управления MIB (Management Information Base — база управляющей информации). Распространению протокола мешает его низкая защищённость и ориентация на использование протокола UDP, приводящего к возможной потере сообщенийDNS

Задача разрешения имен подразумевает определение IP адреса узла по его символьному имени и определение символьного имени по заданному IP адресу.

Исторически первый, но до сих пор действующий механизм разрешения имен связан с прямым заданием таблицы соответствия символьных имён и IP адресов в файле hosts/lmhosts (первый файл используют UNIX/Linux и некоторые др. операционные системы (ОС), а второй – ОС фирмы Microsoft). Оба файла текстовые и их форматы и ключи можно найти в MS Windows в одноимённых файлах с расширением. sam (sample – образец). Очевидно, для сколько-нибудь крупной сети решить задачу таким образом полностью не представляется возможным, хотя запись в эти файлы сведений об основных серверах, маршрутизаторах, шлюзах и пр. весьма эффективна для ускорения старта компьютера в сетевом окружении.

Другой, достаточно популярный способ разрешения имён связан с использованием NetBIOS (Network Basic Input/Output System) поверх TCP/IP [3, с. 415-444, 634-637]. Эта система была разработана совместными усилиями Microsoft и IBM в 80-е годы как сетевой сервис ввода/вывода для операционной системы Windows. Позже, для реализации доступа пользователей к ресурсам сети был разработан протокол NetBEUI (NetBIOS Extended User Interface – расширенный пользовательский интерфейс NetBIOS) как основной сетевой протокол в ОС Windows for Workgroups и NT. Наконец, с повсеместным распространением стека TCP/IP компания Microsoft была вынуждена выпустить реализацию NetBIOS, использующую протокол IP для передачи необходимых данных (NetBIOS поверх TCP/IP). До сих пор продолжается поддержка NetBIOS в ОС Windows 2000/NT/XP, правда уже не как основного механизма доступа к ресурсам сети. NetBIOS целесообразно использовать в небольших, одноранговых сетях.

Изначально, каждый узел в сети с NetBIOS имеет символьное имя (до 15 знаков) с идентификатором ресурса (16-ый знак), который указывает на роль узла (файловый сервер, принт-сервер, рабочая станция и пр.). «Чистый» NetBIOS применим только для небольших сетей и считается «немаршрутизируемым», т. к. –

система имён не позволяет идентифицировать сеть

широко используются широковещательные запросы для получения и обновления сведений об узлах сети (большинство маршрутизаторов широковещательные запросы не пропускают)

Для устранения указанных недостатков компания Microsoft предложила службу WINS (Windows Internet Name Service – служба Windows имен Internet) на базе серверов имен NetBIOS. Следует отметить, что несмотря на упоминание сети Internet, WINS не применяется в этой глобальной сети.

Первый недостаток NetBIOS устраняется в WINS тем, что вводится групповое имя для сети, а второй – тем, что запросы при разрешении имён обращены к конкретным серверам WINS. Неустойчивость в работе службы, трудности администрирования и затруднительность использования в глобальной сети Internet, к настоящему моменту заставили компанию Microsoft перейти к полноценной поддержке DNS.

DNS (Domain Name System – доменная система имён) реализуется с помощью одноименного прикладного протокола, использующего по умолчанию 53 порт [4, с. 305-422; 3, с. 669-717; 2, с. 651-660; 1, с.511-517]. Система DNS была разработана в рамках ОС UNIX и соответствующая служба, использующая DNS, имеет ту же аббревиатуру, но расшифровывается как Domain Name Service.

Имена в DNS строятся по иерархическому принципу в виде перевёрнутого дерева. Домены верхнего уровня (корневые) делятся по профессиональному принципу (. com — коммерческие,. gov — государственные,. net — сетевые и пр. узлы) или по национальному (. ru — русские,. fi — финские,. fr — французские и т. д.). ОС UNIX разрабатывалась в США и, само собой считалось, что все узлы находятся там же. Сейчас можно встретить двойные имена доменов, например,. com. tw – коммерческие тайваньские.

В свою очередь, каждый домен содержит поддомен, имя которого добавляется слева и отделяется точкой, и т. д. Заканчивается запись добавлением слева имени узла. Имя каждого домена, поддомена или узла не должно превышать 63 символа, а полное имя – 255 символов. Для обозначения имён традиционно используется латинский алфавит, цифры и тире (знак _ недопустим), но, в принципе, можно зарегистрировать домен с именем на кириллице, но смысл этого проблематичен.

Данные об именах зарегистрированных в любом домене поддоменов/узлов и их IP адресах хранятся в двух таблицах на DNS-серверах, где также имеется имя и адрес вышележащего домена. По первой таблице для заданного символьного имени определяется цифровой адрес (прямое преобразование и, соответственно, т. н. «прямая зона»), а по второй — по заданному адресу находится символьное имя (обратное преобразование и «обратная зона»).

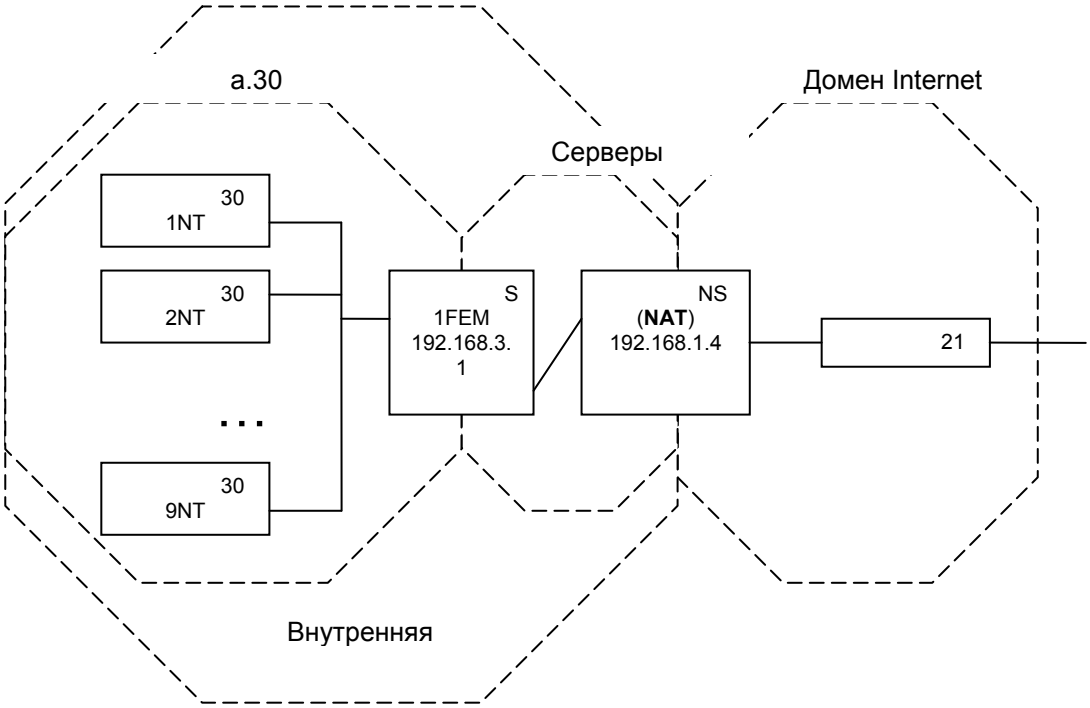
Для повышения надёжности в каждом домене должно быть не менее 2-х серверов (primary — первичного и secondary — резервного), причём физически эти серверы должны находиться в разных сетях и могут располагаться не в тех доменах, имена узлов которых они содержат.

Корневой домен поддерживают свыше 10 DNS серверов, IP адреса и имена которых «зашиты» в сетевые ОС. Регистрацию новых имён и выделение соответствующих IP адресов производит владелец домена. Например, регистрацию в домене. ru производит РосНИИРОС, где регистрация имени и получение IP адреса обойдётся приблизительно в 50$, а годовая поддержка адреса – в 10$.Все изменения в таблице имен производятся на первичном DNS сервере, резервные серверы только обновляют свои записи по записям первичного сервера. Репликация (обновление) зоны производится с помощью надёжного протокола TCP, в то время, как для DNS запросов клиентов, применяется протокол UDP. Для ускорения процесса разрешения имени и уменьшения трафика в сети иногда устанавливают так называемые кэш-серверы DNS, которые записывают часто используемые имена и адреса.Режим работы DNS сервера может быть рекурсивным и не рекурсивным. В случае рекурсивного режима при невозможности разрешить DNS запрос этот запрос транслируется специально заданному другому DNS серверу (форвардеру – forfarders), который затем возвращает полученный ответ. При не рекурсивном режиме — в отсутствии информации о запрашиваемом узле производится обращение к корневым DNS серверам, а от них вниз по цепочке до получения ответа.

NAT

NAT (Network Address Translation — трансляция сетевых адресов) реализует преобразование (подмену) IP адресов локальных сетей во внешние IP адреса глобальной сети Internet [1, с. 601-607; 3, с.898-900; 8, 473]. Необходимость такого преобразования следует из соглашения об использовании части IP адресов только в локальных сетях (см. п. 3.2), по которому маршрутизаторы глобальной сети уничтожают пакеты с этими адресами.

NAT действует на сетевом и частично на транспортном уровнях, обеспечивая преобразование в IP пакетах адресов узлов локальной сети во внешний адрес. Преобразование производится путём замены адреса внутреннего узла на внешним адрес. Заменяемые адреса запоминаются в таблице, с помощью которой производится обратная замена при получении ответного пакета. Следует отметить, что для устранения возможной неразличимости преобразуется не только IP адрес, но и с помощью PAT (Port Address Translation) номер порта.



Кроме преобразования адресов NAT позволяет уменьшить потребность в IP адресах для глобальных сетей, т. к. все пользователи локальной сети могут получать доступ к ресурсам глобальной сети через один внешний адрес.

NAT — не единственный способ отправки пакетов из локальной сети в глобальную, альтернативой трансляции адресов является использование сервера-посредника.

Proxy сервер

Proxy сервер (сервер посредник) выступает как посредник запросов протоколов прикладного уровня. [3, с. 905-907].

Узлы внутренней локальной сети направляют свои запросы к Proxy серверу, а он, в свою очередь, или отвечает содержимым из своей кэш памяти, либо запрашивает требуемый ресурс и ответ переправляет внутреннему узлу. Решение принимается после определения наличия в кэш памяти Proxy сервера актуальной версии запрашиваемого ресурса (проверяется совпадение времени последнего изменения ресурса на сайте и в кэш памяти). Такой механизм позволяет решать несколько задач:

Уменьшается количество требуемых внешних IP адресов

Предоставляется возможность закрытия нежелательных ресурсов Internet

Уменьшается трафик

Каждый прикладной протокол требуется в Proxy сервере самостоятельной поддержки, причём некоторые прикладные протоколы (например, мультимедийные) не поддерживаются такими Proxy.

Схема работы Proxy сервера представлена на рисунке 4.3.1.

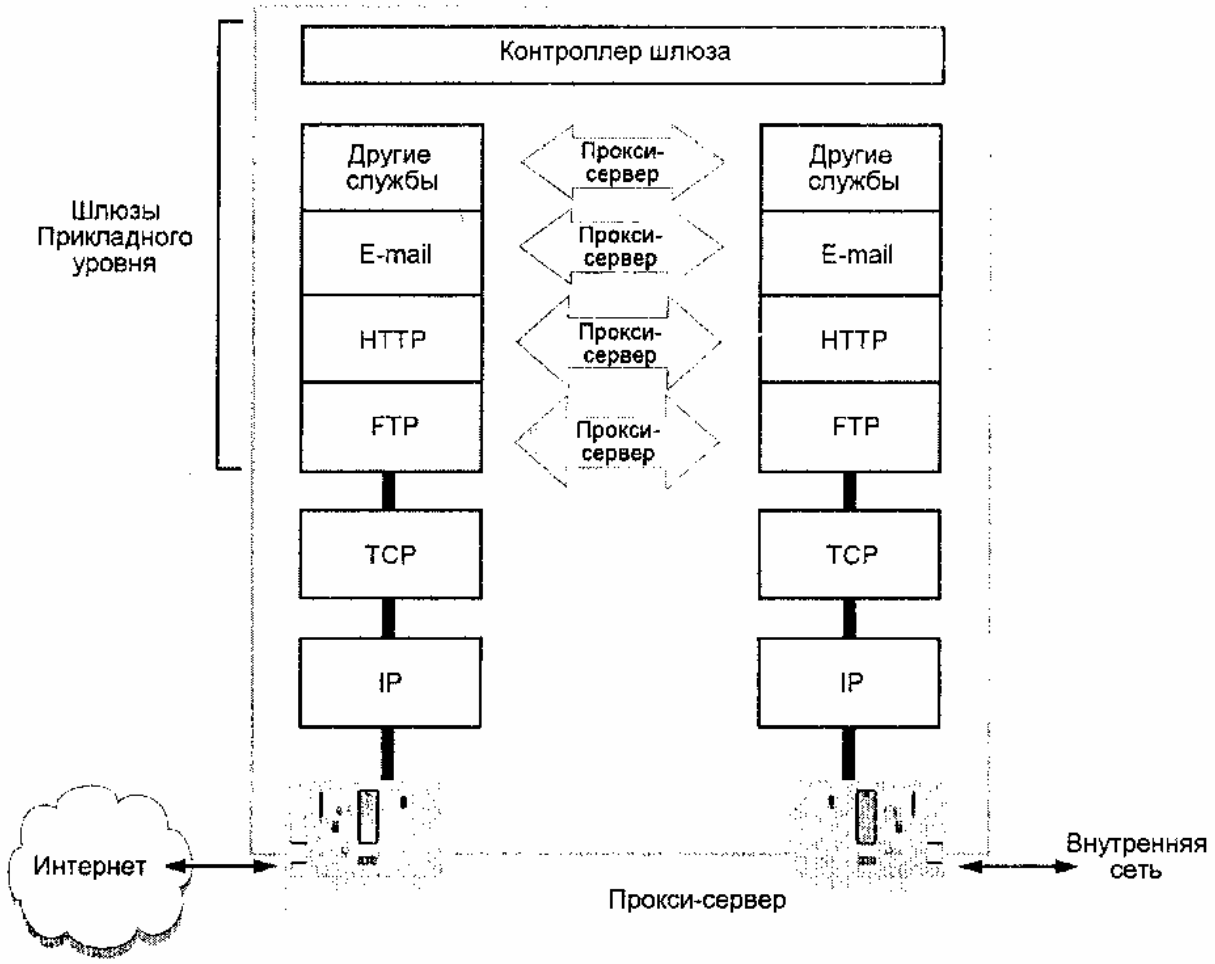


Рис. 4.3.1. Схема работы Proxy сервера

В последнее время стали популярными не требующие настроек в браузере «транслирующие» Proxy серверы, использующие NAT и создающие у пользователя иллюзию «прямой» работы в сети Internet. Для клиента отказ такого сервера практически не отличим от недоступности ресурса (ICMP пакеты, например, от утилиты ping, благополучно достигают узла назначения, а http/ftp/… запросы — «утыкается» в неработающий Proxy).

WEB публикации

В настоящее время существует достаточное количество серверных программных продуктов для представления информационный ресурсов по протоколу http, или Web (WWW) публикаций. Остановился на трёх наиболее популярных в России.

Apache – один из старейших свободно распространяемых Web серверов для Unix/Linux систем (существуют и коммерческие версии Apach, например, для Windows систем (IBM) и др.)

Название сервера связывают с многочисленными «заплатками» (patch) первых версий программы, что и привело к обозначению сервера как «сервера из патчей».

Основные функции Web сервера:

Аутентификация клиентов (если это необходимо)

Обработка запросов клиентов (количество одновременно обрабатываемых запросов задаётся специальным параметром и определяется мощностью сервера)

Автоматическая очистка устаревших соединений

IIS (Internet Information Services) –Web сервер для Windows NT/2K/03 систем фирмы Microsoft. Актуальная, 6-я версия IIS входит в состав MS Windows 2003 Server.

Особенности IIS v.6.0 –

Поддержка http версии 1.1 (поддержка передачи со сжатием данных — http compression и аутентификация с использованием MD5)

Реализация механизма Web DAV (Distributed And Versioning) – редактирование содержимого сайта по http

Поддержка SMTP для совместного развёртывания почтового сервера

Поддержка NNTP (Network News Transfer Protocol) для совместного развёртывания сервера новостей

Поддержка FTP для развёртывания личного ftp сервера клиента в пределах его каталога

Установка PICS (Parental Internet Content Selection) рейтинга – самоценки содержимого сайта на подобие принятой в США классификации кинофильмов.

Поддержка SSL v.3.0 и SGC (Server-Gated Cryptography) для 128 битного шифрования шлюзовых функций и выбора алгоритмов шифрования.

Защита ASP (Active Server Pages) – фирменного механизма Microsoft для динамического формирования ответа на запрос клиента. В ранних версиях этот механизм снижал защиту сервера, т. к. ряд операций выполнялся с правами администратора. Версия с улучшенной защитой получила название ASP. Net ограничивает права при выполнении потенциально опасных операций.

Поддержка до 64 Гбайт дискового пространства

Совершенствование мер защиты

Ограничение очередей запросов

Контроль «зависших» соединений

Ограничение полосы (скорости) обмена

Остановка гиперактивных процессов

NetWare Enterprise Web Server –Web сервер для NetWare систем фирмы Novell. Актуальная версия поставляется с Novell NetWare 6.0/6.5 и может быть развёрнута совместно с предлагаемым Apache Web Server (для любителей Apache).

Особенности Enterprise Web Server –

Редактирование содержимого страниц через Web браузер

Поддержка различных сред разработки приложений – Perl, JavaScript, NetBasic Scripting

Интеграция с NDS и работа через SSL для усиления защиты

Мультимедийные службы

IP-телефония, Internet-вещание (-радио), конференции – далеко неполный перечень популярных мультимедийных сетевых служб и приложений [7, с. 45-66].

Первые опыты передачи голоса по сети Internet относятся к 1983 г. (Кембридж, Массачусетский университет, США), а выпуск коммерческого оборудования фирмой Vocal Tec (Израиль)– к 1995 г.

Мультимедийные службы предъявляют ряд дополнительных требований при организации соединения. Важнейшими из этих требований являются — Непрерывность, так, например, при передаче речи задержка в 150 мс считается допустимой, а в 400 мс — делает переговоры затруднительными.

Допустимость потерь, поскольку человеческие органы чувств (зрение и слух) обладают заметной инерцией и способностью восполнять потери за счет деятельности мозга.

IP multicasting — многоадресность соединения, например, при организации конференций.

Современный взгляд на полный сетевой сервис наиболее ярко отражён в идее мультисервисных NGN сетей (New Generation Network), предоставляющих весь комплекс информационного сервиса от простой электронной почты, до услуг типа «видео по заказу» и видеоконференций.

Один из наиболее масштабных проектов этого направления является TIPHON (Telecommunication & Internet Protocol Harmonization over Networks), который предусматривает предоставление пользователям телефонной связи, в том числе с мобильных терминалов стандарта GSM, обмена факсимильными сообщениями и всех служб сети Internet. Проект разрабатывался ETSI (European Telecommunication Standards Institute) с 1997 по 1999 г. К достижениям проекта можно отнести утверждение представленных в таблице 4.6.1 классов обслуживания.

Характеристика	Класс обслуживания			
	Высший (4)	Высокий (3)	Средний (2)	Низкий (1)
Качество речи (по 5 бальной шкале)	> 4,3 (G.711)	≈ 4,3 (G.726 32 Кбит/с)	≈ GSM	Нет
Среднее время задержки (мс)	< 150	< 250	< 350	< 450
Среднее время уст. соединения ©	< 3	< 8	< 15	< 20

Схема соединений по проекту TIPHON представлена на рисунке 4.6.1.

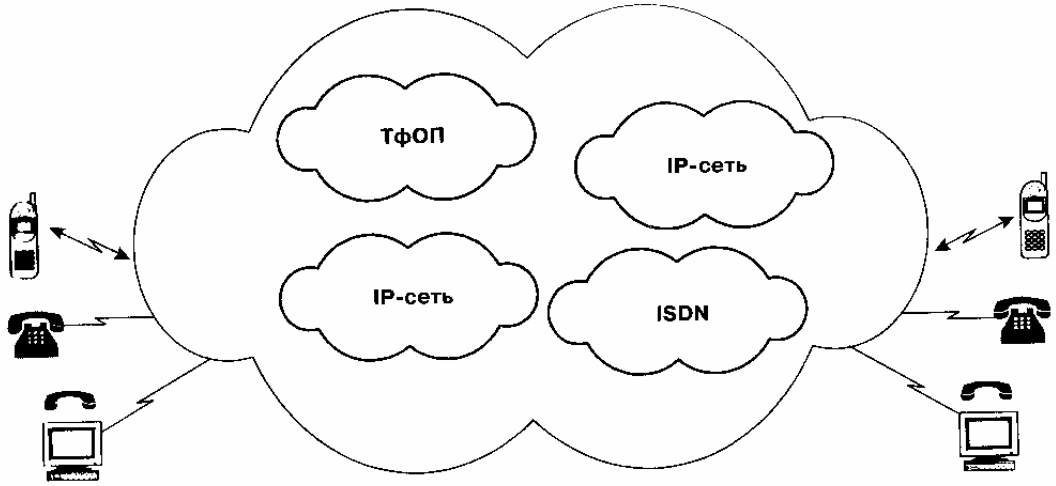


Рис. 4.6.1. Схема соединений по проекту TIPHON.

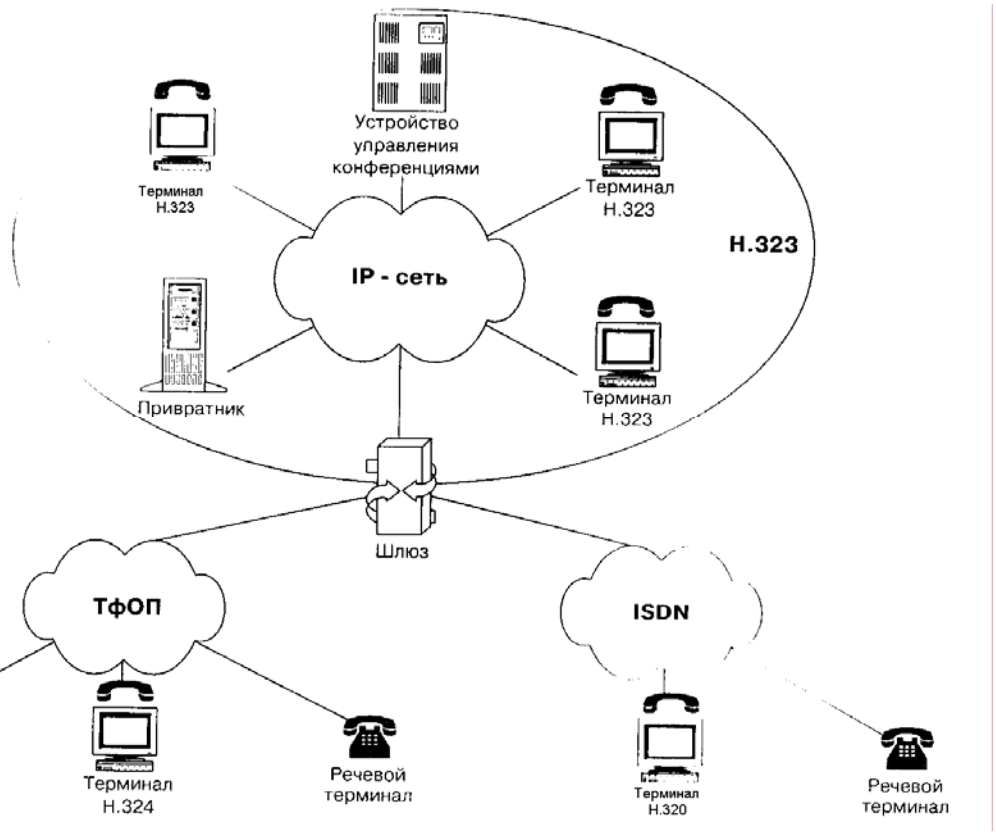
К действующим стандартам в области мультимедийных приложений в IP сетях относят протокол H.323, а также протоколы IP телефонии — SIP и MEGACO/H.248.

H.323

H.323 –один из наиболее популярных протоколов для реализации мультимедийных приложений в IP сетях [7, с. 23-30, с. 131-192].

Протокол относится к т. н. «зонтичный» протоколам, которые охватывают целое направление и оставляют детализацию конкретных решений за уточняющими протоколами. Актуальная, 3-я версия протокола (1999 г.) включает протоколы/алгоритмы кодирования/сжатия видео (H.261, H.263) и аудиоинформации (G.711, G.722, G.723, G.728, G.729), мультиплексирования (H.225.0), управления каналом (H.245) и передачи данных (T.120). Помимо протоколов H.323 в 1996-1999 гг. ITU-T был разработан ряд связанных протоколов для мультимедийных приложений: H.320 – для телефонных и N-ISDN сетей; H.321 – для телефонных, широкополосных ISDN сетей, сетей технологии ATM, локальных вычислительных сетей; H.322 – для ЛВС с гарантированным качеством обслуживания и H.324 – для аналоговых каналов телефонной сети общего пользования.

Согласно протоколу H.323 обслуживание абонентов производится при их подключении к оборудованию зоны. Состав устройств зоны представлен на рисунке 4.6.1.1.



Важнейшим устройством зоны является привратник (Gatekeeper), играющего роль контроллера зоны. Привратник выполняет следующие функции по обслуживанию зоны:

регистрация терминалов при их активизации

контроль доступа абонентов через терминалы

преобразование телефонного номера вызываемого абонента в IP адрес его привратника для установления соединения по IP сети

контроль состояния канала

ретрансляция сигналов управления между терминалами

Шлюз (Gateway) – устройство преобразования формата данных в телефонной или ISDN сети в формат IP сети.

Терминал (Terminal) – оконечное устройство пользователя

Устройство управления конференциями MCU (Multipoint Control Unit) – обеспечивает обмен мультимедийными данными между тремя и более участниками. Организация конференций возможна только посредством относительно дорогих MCU, причём количество участников ограничено их техническими характеристиками. Предусматривается три способа проведения конференций, проиллюстрированных рисунком 4.6.1.2.

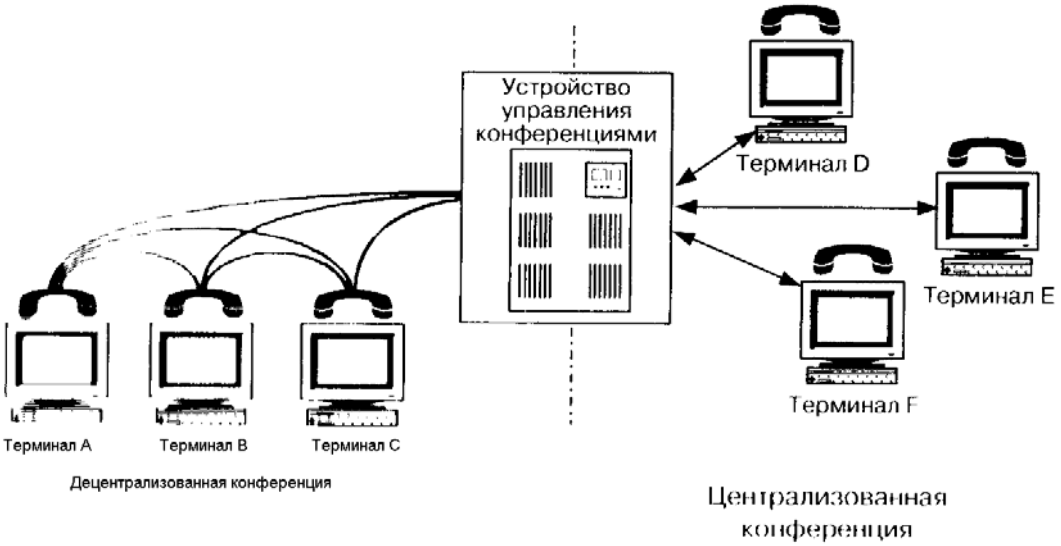


Рис. 4.6.1.2. Способы проведения конференций.

При централизованной организации конференций относительно высокие технические требования предъявляются к устройству управления конференциями, что определяет высокую стоимость этого устройства.

При децентрализованной организации требуются дорогие терминалы с высокой стоимостью.

Наконец, при смешенной организации возможен компромисс между характеристиками и стоимостью терминального оборудования и MCU, однако во всех случаях высокая стоимость как самой аппаратуры, так и высокоскоростного доступа к IP ссети препятствует массовому использованию конференций в практике использования сети Internet.

Прокси-сервер протокола H.323 должен обеспечивать:

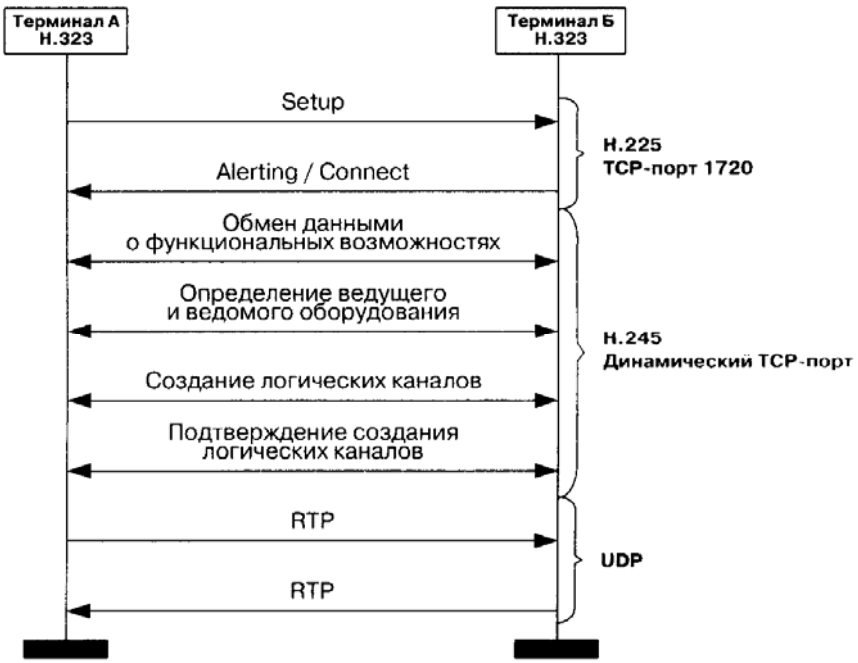
подключение терминалов через каналы без обеспечения качества обслуживания (без поддержки протокола RSVP – Resource ReserVation Protocol) путём туннелирования

маршрутизацию трафика H.323 отдельно от обычного трафика IP сети

функции NAT для терминалов из LAN

защиту доступа к трафику H.323

Полезным для понимания особенностей протокола H.323 может служить представленный на рисунке сценарий установления соединения, по которому создание соединения производится с помощью надёжного протокола TCP, а сами данные передаются на транспортном уровне по протоколу UDP.



На рисунке использованы следующие обозначения:

Setup – запрос на соединение;

Alerting – терминал Б свободен;

Connect – номер порта для H.245.

RTP (Real-time Transport Protocol) – прикладной протокол IETF (Internet Engineering Task Force) для передачи мультимедийных данных реального времени по IP сети. Для контроля доставки RTP пакетов используется протокол RTCP (Real Time Control Protocol) [7, с. 125-128].

Помимо влияния абсолютной величины задержки при передаче мультимедийной информации важную роль в субъективном восприятии играет непостоянство величины задержки (джиттер). Для борьбы с джиттером по протоколу RTP в мультимедийный поток данных вводятся временные метки, позволяющие вычислить величину задержки и компенсировать их путём определения средней величины и буферизации.

← Слово 32 бита (4-е байта) →																															
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
V=2		P	X	CC				M	PT							SN															
Timestamp																															
SSRC																															
CSRC …																															

В таблице использованы следующие обозначения:

V – версия протокола (2 – текущая версия);

P – индикатор/маркер использования заполнения (например, для кратности 32 битам поля передаваемых данных);

X – индикатор использования поля расширения заголовка в экспериментальных версиях RTP;

CC – счётчик отправителей (идентификаторы отправителей находятся за заголовком);

M – индикатор границ потока, например, для видео – конец кадра, для аудио – начало звука после паузы;

PT – тип и формат данных (например, сами данные, или команда управления RTCP);

SN – порядковый номер пакета (начинается с произвольного числа);

Timestamp – временная метка создания потока по часам отправителя;

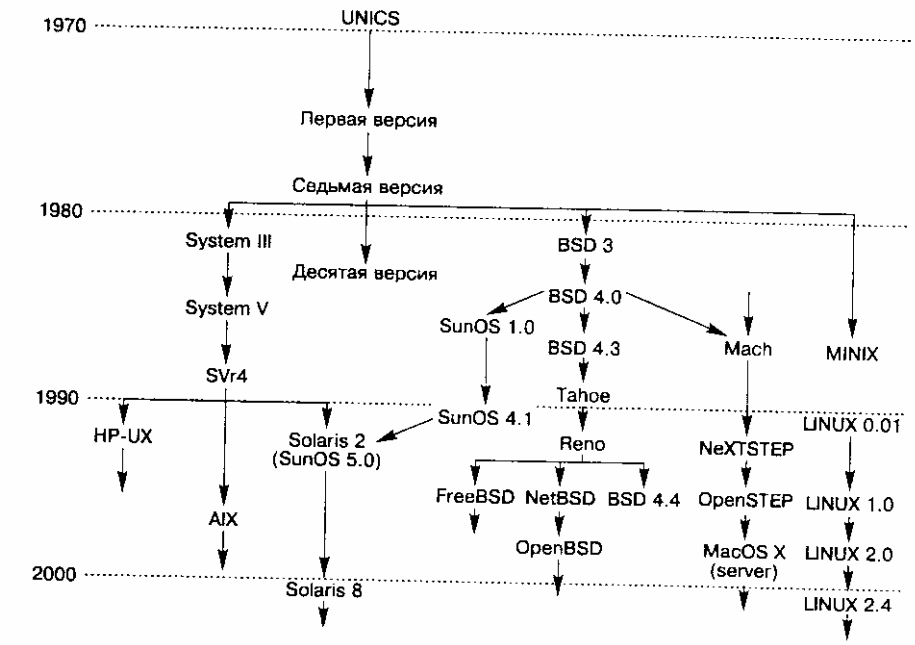
SSRC – псевдослучайное число, идентифицирующее источник на время сеанса;

CSRC — список идентификаторов источников от 0 до 15.

UNIX/Linux.

UNIX — одна из первых сетевых операционных систем [6, с. 647-652; 3, с.545-565] 1).

Основные этапные версии развития системы представлены на рис. ↓.



Причинами популярности UNIX являются:

Кросплатформенность2)

Открытость 3)

Логичность 4)

Запрет на разработку компьютерных программ для учредителя Bell Labs — корпорации AT&T заставил передать UNIX для некоммерческого использования в университетские круги, где она непрерывно модернизировалась.

К «этапным» версиям относят:

Базовые версии – System III, V и SVr4 (System V Relies 4)

«Берклеевская» линия BSD (Berkley Software Distribution) с популярной версией Tahoe (BSD 4.3) и общественной группой Reno (Nevada USA), развивающей FreeBSD (версия BSD 4.4), NetBSD (поддержка IPv6, Firewall и др. сетевые функции) и OpenBSD (криптографическая защита)

Линия для компьютеров Macintosh (Mach, NeXTSTEP, OpenSTEP, MacOS X)

Линия коммерческих5) фирменных продуктов – SunOS, Solaris (Sun Solaris Microsystems Inc.), HP-UX (Hewlett Packard), AIX (IBM)

Linux — развитие Линусом Торвальдсоном (Linus Torvaldson) MINIX — упрощённой версии UNIX. В последние годы широкое распространение получили такие «некоммерческие»6) фирменные продукты, как Red Hat, Debian, Slackware, Coldera и др.

Архитектура UNIX систем содержит 4-е довольно чётко разделённых уровня:

Аппаратный уровень (драйверы устройств, обеспечивающие интерфейс со следующим уровнем)

Уровень ядра, в котором используется всего около 100 системных вызовов и выполняется управление процессами (демонами)

Оболочка, облегчающая терминальный доступ к ядру. Наиболее популярные оболочки – csh (C shell), ksh (Korn Shell) и bash

Уровень программ

Удобство графического представления привело к созданию клиент-серверного графического интерфейса, получившего название X Windows. 7) В последние годы популярность приобрела созданная на базе X Windows графическая среда GNOME 8) содержащая такие X клиенты, как менеджер дисплея (Display Manager) и менеджер окон (Windows Manager). Менеджер дисплея запускается при загрузке X Windows и отвечает за регистрацию в системе (имена, пароли), загружает пользовательский сценарий и окружение. Менеджер окон служит для работы с окнами. 9)

Безопасность компьютерных сетей.

Безопасность компьютерных сетей (информационных систем) – комплексная проблема, решаемая системными методами.

Основополагающие документы:

Оранжевая книга (DoD 5200.28-STD – Trusted Computer Systems Evaluation Criteria) 1).

Красная книга (NCSC-TG-005 – Trusted Network Interpretation of the Trusted Computer Systems Evaluation Criteria) 2).

CCITSE (Common Criteria for Information Technology Security Evaluation) – Общие критерии оценки безопасности информационных систем

ISO 17799 – Международный стандарт по безопасности 3).

ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.

ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

Документы технической комиссии при президенте РФ 4).

Критерии безопасности информации:

Доступность — 6 уровней от Д0 (без неё остановится работа) до Д5 (может понадобиться когда-нибудь)

Целостность – 5 уровней от Ц0 (последствия нарушения необратимы) до Ц4 (не сказывается на работе)

Конфиденциальность – 6 уровней от К0 (несанкционированный доступ приводит к краху) до К5 (не влияет на работу)

Классификации предметов защиты:

Объекты (устройства, файлы, терминальное оборудование и пр.), средства (программы, службы, сервисы и пр.) и субъекты (персонал)

Физические (компьютеры, коммутационное оборудование, терминальное оборудование и пр.), информация (файлы, базы, структуры и пр.) и сервисы (удалённый доступ, управление, администрирование и пр.)

Оптимизационная задача: модель информационной системы (объекты защиты) + критерии + стоимость достижения требуемого уровня => минимизация затрат защиты работоспособной системы.

Методы защиты: физические, организационные, криптографические (программные) 5).

Терминология: хакер (без материальной выгоды), кракер (для денег) и фрикер (телефонные сети).

Наиболее уязвимые сервисы (протоколы) по данным CERT 6).

Рейтинг	Сервис	% уязвимых инсталляций
1	RPC (Remote procedure calls)	93,4
2	SMTP	61,1
3	Finger (информационная служба по 79 порту)	59,6
4	Trivial FTP (без аутентификации)	57,4
5	HTTP	42,4
6	DNS	35,0
7	FTP	33,0

Рейтинг наиболее уязвимых программ/утилит по данным SANS 7) [8, с. 200-201].

BIND (Berkeley Internet Name Domain) – реализация службы DNS для UNIX/Linux версии 8.2.2 и ниже предоставляют полный доступ (уровень root) к компьютеру

Приложения Web-серверов

Сервисы на базе RPC (rpc. cmsd, rpc. statd и др.) позволяют получить полный доступ (уровень root) к компьютеру

Сервисы удалённого доступа к данным (RDS – Remote Data Service) Microsoft Internet Information Server позволяет выполнять команды с привилегиями администратора

Sendmail – почтовый сервис UNIX/Linux версии 8.10 и ниже «прозрачен» для компьютерных червей 8)

Сервисы sadmind (Solaris) и mountd (Unix) доступа и управления сетевой файловой системой (NFS – Network File System) при переполнении буфера позволяют получить полный доступ (уровень root) к компьютеру

Совместный доступ к файлам по NetBIOS из-за слабости контроля (пользователь сам предоставляет доступ) приводит к уязвимости компьютеров

Наиболее популярные типы атак [8, с.153-185; 4, с. 264-311] 9):

D|DoS (Distributed | Deny-of-Service) – распределённый | отказ от обслуживания – разрушение механизмов доступа к информации и/или организация запредельной нагрузки на атакуемый сервер

Ping-of-death (декабрь 96) – подача утилитой ping пакета недопустимо большого размера 10)

SYN flood (сентябрь 96) – подача потока ложных запросов на TCP соединение

Smurf – организация потока запросов ICMP hello с обратным адресом жертвы

Fraggle – запуск отладочного UDP сервиса chargen (character generation – создание потока символов) с обратным адресом жертвы

Организация ложных DHCP клиентов

Teardrop – подача IP пакетов с неправильными значениями смещения фрагмента и длины пакета. В буфере сборки возможно появление отрицательного значения, воспринимаемого как максимальное (64 кбайт), и затирание используемых областей памяти

Land – адрес отправителя = адресу жертвы (зацикливание ответов)

Nuke – подача через 139 порт TCP пакетов со строчными параметрами в прикладные процессы Windows, где эти параметры не предусмотрены.

Атаки на поток данных

Прослушивание (sniffing) сети на предмет определения IP адресов и открытых портов путём сканирования или установки сетевой карты в режим перехвата

Перехват путём ложных ARP ответов

Tiny Fragment Attack – атака крошечными фрагментами. Маршрутизатор уничтожает только первый из фрагментированных пакетов, а остальные пропускает и они могут быть собраны жертвой

Ложные дубликаты TCP подтверждений, приводящие к необоснованному увеличению окна отправителя.

Преждевременные TCP подтверждения могут привести к потере целостности (потерянные пакеты будут подтверждены)

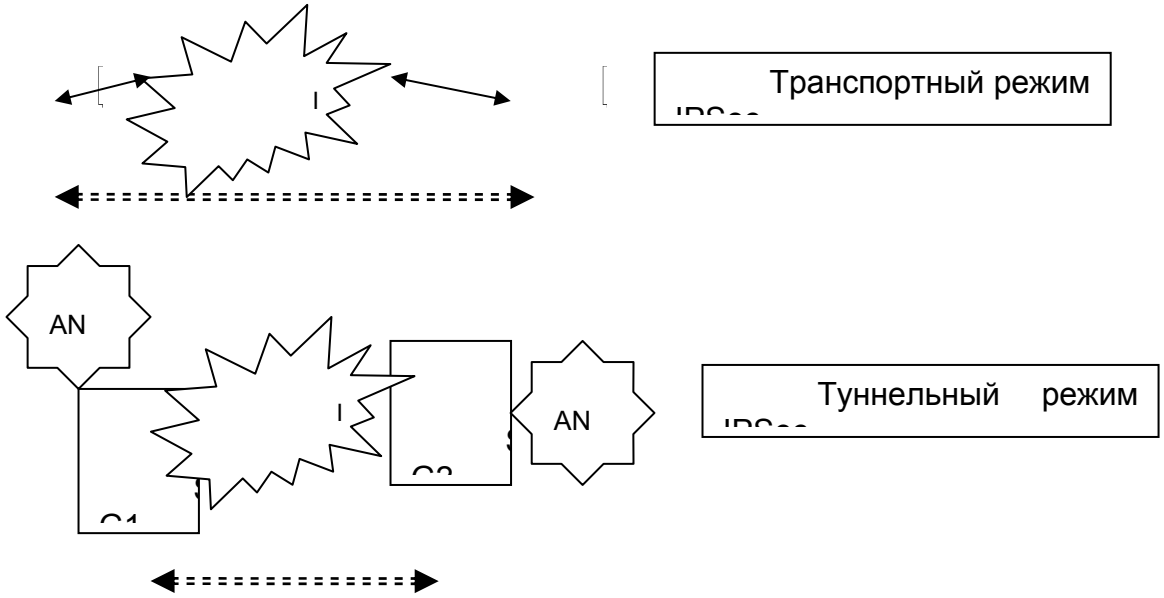
Атаки на маршрутизаторы

Атаки на клиентов Java Virtual Machine и ActiveX

IPSec

IP-Security (IPSec) – набор протоколов сетевого уровня для защищённого обмена данными в TCP/IP сетях [8, с. 427-436] 1).

Два режима – транспортный и туннельный (см. рис. ↓) 2).



Протокол защиты заголовка пакета формирует Authentication Header (AH) и обеспечивает:

Целостность данных

Подлинность происхождения данных

Защиту от повторений

Формат AH показан на рис. ↓

32 бита (4 байта)

1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8 1 2 3 4 5 6 7 8
Следующий заголовок	Длина значимых данных	Зарезервировано
Индекс параметра безопасности		
Последовательный номер		
Данные аутентификации		

Следующий заголовок (Next header) указывает тип данных за AH (установлен IANA – Internet Assigned Numbers Authority)

Длина значимых данных (Payload length) – длина AH в 32битовых словах – 2

Зарезервированное поле заполнено нулями

Индекс параметра безопасности (Security parameters index) – идентификатор способа защиты (0 – защиты нет)

Последовательный номер (Sequence number) – порядковый (с 0) номер пакета

Данные аутентификации (Authentication data) – например, хэш-функция неизменяемых или предсказуемых полей заголовка пакета.

Размещение AH в IP пакете для транспортного и туннельного режима показывает рис. ↓

Исх. IP заголов.	TCP заголовок и Данные

← Оригинальный IP пакет

Исх. IP заголов.	AH	TCP заголовок и Данные

← Транспортный режим

←−−Аутентификация (кроме изменяемых полей)−−−−−−−−−−−→

Нов. IP заголов.	AH	Исх. IP заголов.	TCP заголовок и Данные

← Тунн. р.

←−−−−−−−−−−−−−−−−−−Аутентификация (кроме изменяемых полей)−−−−−−−−−−−→

В туннельном режиме новый IP заголовок содержит адрес шлюза.

Протокол инкапсуляции содержимого пакета Encapsulated Security Payload (ESP) предусматривает шифрование содержимого пакета и обеспечивает:

- Конфиденциальность и целостность данных
- Подлинность происхождения данных
- Защиту от повторений

Размещение ESP в IP пакете для транспортного и туннельного режима показывает рис. ↓

Исх. IP заголов.	TCP заголовок и Данные

← Оригинальный IP пакет

Исх. IP заголов.	Загол. ESP	TCP заголовок и Данные	Хв.	Аут

← Трансп. режим

←−−−−−Шифрование−−−−−−−−−−→

←−−−−−−−−−Аутентификация −−−−−−−−−−−−→

Туннельный режим

Нов. IP заголов.	Загол. ESP	Исх. IP заголов.	TCP заголовок и Данные	Хв.	Аут

←−−−−−−−−−−−−−−−−−−−Шифрование−−−−−−−−−−→

←−−−−−−−−−−−−−−−−−−−−−−−Аутентификация −−−−−−−−−−−−→

Загол (овок) ESP содержит 2 32-битных слова: индекс параметра безопасности (Security parameters index) и последовательный номер (Sequence number) (см. заголовок AH).

Хв (ост) ESP состоит из заполнителя (Padding), дополняющего блок шифруемых данных до требуемого размера и скрывающего истинный размер этих данных; 8-битового поля длины заполнителя (Pad length) и 8-битового поля следующего заголовка (Next header).

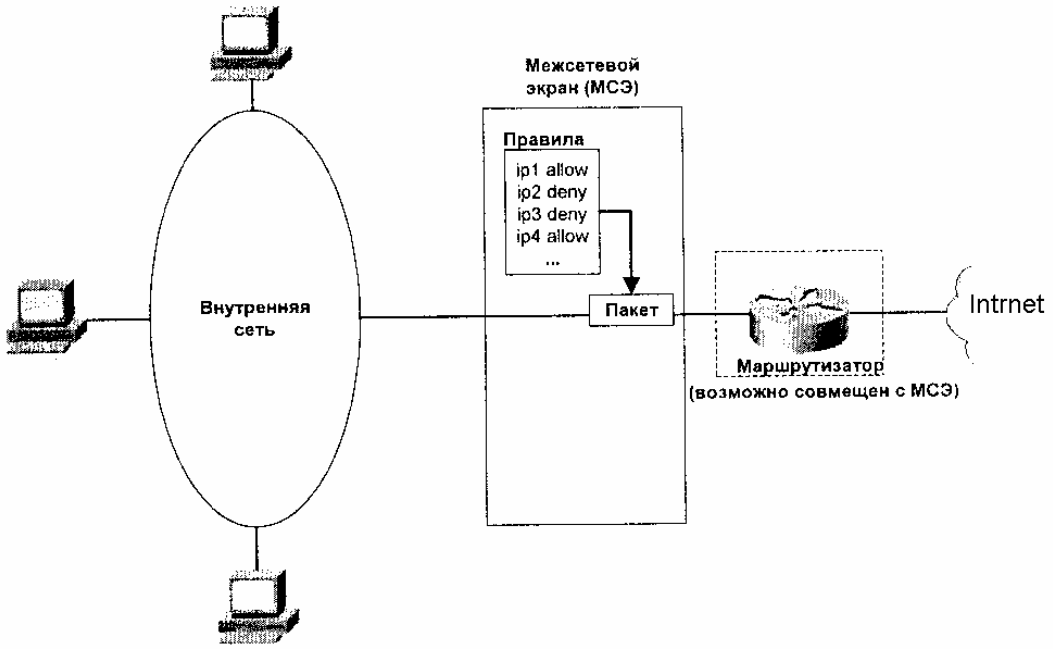
Аут (ентификационные) данные (Authentication data) – «цифровая подпись» содержимого пакета.

Для защиты как IP заголовков, так и содержимого пакета используют оба протокола.

Межсетевой экран

Межсетевой экран (МСЭ) или firewall – фильтр пакетов для защиты внутренней информационной среды (Intranet) от несанкционированных действий со стороны внешней среды (Extranet/Internet) [8, с. 466-472] 1).

Расположение firewall иллюстрирует рис. ↓.

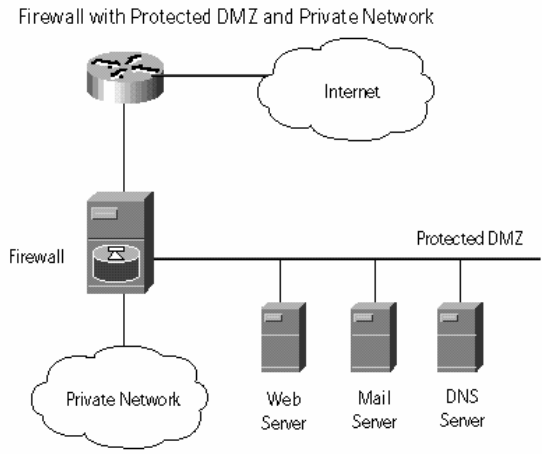


Простой пакетный фильтр (packet filter) обычно размещается на шлюзе (маршрутизаторе) и работает совместно с NAT разрешая, запрещая или отвечая на пакеты согласно устанавливаемым правилам (цепочкам) в зависимости от направления следования пакетов (OUT/IN), IP адресов, портов и протоколов. Каждый пакет рассматривается независимо от предыдущих. Может защитить от некоторых атак типа DoS (ping-of-death, SYN-flood и др.).

МСЭ с контролем соединения (virtual circuit control) чаще всего выполнен в виде отдельного устройства и устанавливает правила пропуска или уничтожения пакетов в зависимости от «виртуального» соединения, т. е. учитываются предыдущие пакеты 2).

МСЭ с контролем приложения (application layer gateway) практически не отличается от сервиса proxy и в продвинутых моделях проксирует не только традиционные приложения с HTTP, FTP, но и другие протоколы.

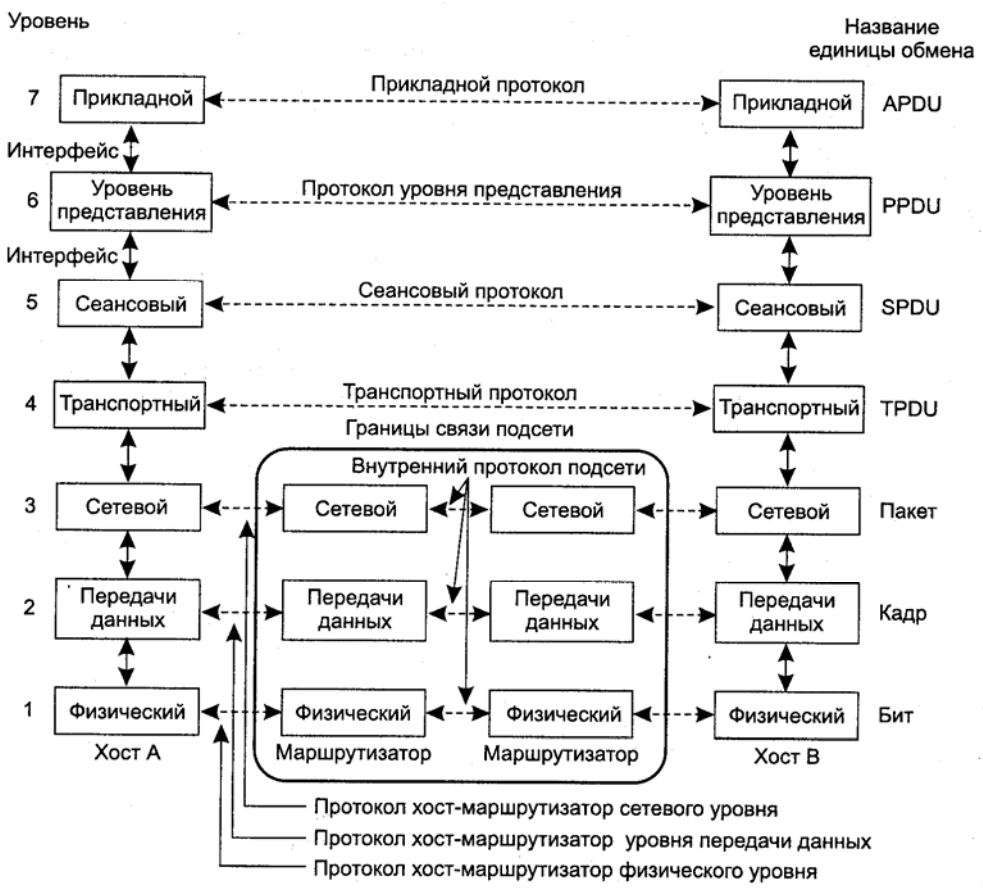
Наиболее защищённой считается структура с выделением ресурсов для публичного доступа в т. н. демилитаризованную зону (DeMilitarized Zone — DMZ) с двумя МСЭ, устраняющими проникновение из вне во внутреннюю сеть (см. рис. ↓).



29. VLAN, VPN.

VLAN (Virtual Local Area Network) и VPN (Virtual Private Network) – два популярных способа решения задачи построения независимых сетей, использующих общие физические линии связи в локальных и глобальных сетях соответственно. VLAN решает эту задачу на уровне технологии (Ethernet), а VPN – на уровнях стека протоколов (TCP/IP).

Наиболее «продвинутое» построение VLAN для технологии Ethernet основано на стандарте 802.11Q, 1) согласно которому в заголовке кадра Ethernet устанавливается номер подсети, обрабатываемый коммутаторами и/или сетевыми картами [1, с. 458-464]. Один и тот же порт коммутатора (сетевую карту) можно ассоциировать с несколькими номерами виртуальных подсетей для организации доступа к общему сетевому ресурсу (серверу). Следует отметить, что для содержимого кадра при организации VLAN не предполагается использование какой-либо защиты и «независимость» виртуальных подсетей построена на «правильной» отправке кадра коммутатором или пропуске «чужих» кадров сетевой картой. Очевидно, что такой подход оправдан только, когда кадр физически не выходит за пределы организации и можно гарантировать защиту от несанкционированного перехвата.



Для обозначения семиуровневой модели иногда используется прилагательное «эталонная», подчёркивающее теоретический характер этой модели. Действительно, за редким исключением, ни один из практически используемых стеков протоколов не соответствует этой модели в точности.

Среди причин этого явления можно выделить следующие. Во-первых, все основные практически используемые стеки (TCP/IP, IPX/SPX, ATM, X.25 и др.) разрабатывались до появления семиуровневой модели.

Во-вторых, форма описания семиуровневой модели в момент появления была весьма далека от совершенства и многие разработчики просто не смогли своевременно понять её важность.

В-третьих, кажущаяся громоздкость модели делала разработанные на её основе стеки коммерчески невыгодными и пригодными только для научных исследований.

Тем не менее, семиуровневая модель позволяет сопоставить между собой различные стеки, даёт «точку отсчёта» для разработки новых сетевых решений и с этих позиций роль модели остаётся весьма значимой.

Оглавление