Тема 1. Виды и принципы построения информационных сетей

1.1. Классификация информационных сетей

Информационные сети классифицируются по многочисленным признакам: по масштабности, по особенностям архитектуры, по целевому назначению, по способам коммутации и т.д.

По масштабности в настоящее время информационные сети принято делить на глобальные (широкомасштабные), городские и локальные сети. Использовавшееся ранее понятие региональные сети в настоящее время потеряло актуальность.

Глобальные сети (**WAN,** Wide Area Network). Скорости передачи данных в WAN лежат в диапазоне от десятков Кбит/с до сотен Гбит/с. WAN сеть содержит сложные маршрутизаторы пакетов, которые вводят значительные паузы при маршрутизации трафика. Глобальная сеть не имеет единого хозяина: ее участки принадлежат разным хозяевам.

Городские сети (**MAN,** Metropolitan Area Network) являются сравнительно новым видом сетей. Технологии MAN позволяют взаимодействовать в географических областях средних размеров (размер большого города) и работают на скоростях от десятков Кбит/с до десятков Гбит/с. MAN работают с меньшими паузами, чем WAN, но не могут обеспечить взаимодействие на таких же больших расстояниях. Типичные MAN работают со скоростями от 56 Кбит/с до 1000 Мбит/с. В технологиях MAN сеть содержит активные коммутирующие элементы, которые приводят к появлению коротких задержек.

Локальные сети (**LAN,** Local Area Network). Локальные сети обычно занимают пространство комнаты, здания, университетского городка. Работают со скоростями от 4 Мбит/с до единиц Гбит/с. В LAN каждый компьютер обычно содержит сетевое интерфейсное устройство, соединяющее компьютер с сетевой средой.

Иногда также используют следующие понятия**.**

CAN (Campus Area Network) — кампусная сеть, объединяющая локальные сети близко расположенных зданий.

Объединенная сеть (интерсеть) — сеть, состоящая из двух или более соединенных друг с другом независимых сетей.

GAN (Global Area Network) — глобальная сеть (не общепризнанный термин, в Интернет эта аббревиатура может обозначать и нечто иное).

По особенностям архитектуры сети делятся на коммуникационные и компьютерные.

Коммуникационные (транспортные) сети предназначены для обеспечения связи и информационного обмена между территориально

разнесенными пользователями, компьютерные сети являются предметом изучения нашего курса.

По целевому назначению информационные сети подразделяются на: информационные сети общего назначения и информационные сети специального назначения.

Информационные сети общего назначения**.** Эти сети предназначены для широкого круга пользователей. Примеры: сеть коммутации пакетов общего назначения X25, телефонная сеть общего пользования (ТСОП), Интернет.

Информационные сети специального назначения. Такие сети ориентированы либо на определенную предметную область (сети САПР, АСНИ и т.д.), либо на определенную группу пользователей (корпоративные сети, виртуальные частные сети).

Корпоративные сети. Корпоративная сеть это сеть корпорации, т.е. сеть объединения предприятий, работающих под централизованным управлением и решающих общие задачи. Как правило, корпорация представляет собой сложную структуру, имеет распределенную иерархическую систему управления.

Предприятия, отделения и административные офисы корпорации могут находиться на достаточно большом удалении друг от друга, что приводит к необходимости использования технологии не только локальных, но и глобальных и городских сетей. Современные корпоративные сети базируются на технологии интранет.

Виртуальные частные сети (Virtual Private Network – **VPN)**. Термин впервые применен в 1970-х годах и ассоциировался с дешевыми телефонными переговорами по Internet. VPN позволяет частным пользователям, работающим дома или находящимся в дороге, подключаться к VPN-серверу частной сети используя общедоступные сети, например, Интернет. VPN обеспечивает необходимую безопасность; для пользователей, не имеющих разрешение на VPN-подключение к интрасети, эта сеть недоступна и не видна в сетевом окружении.

1.2. Коммуникационные сети

Коммуникационные сети подразделяются на первичные и вторичные сети.

Первичная сеть может быть аналоговой или цифровой и представляет собой совокупность типовых каналов, групповых трактов, сетевых узлов, сетевых станций.

Вторичные сети организуются на базе первичной сети и подразделяются на телефонные, телеграфные, телевизионные, звукового вещания, передачи данных.

По используемой среде линии связи подразделяются на:

проводные (сигналы распространяются вдоль непрерывной направляющей среды): воздушные, кабельные, волноводы, оптоволоконные, сверхпроводящие кабельные линии;

радиолинии (сигнал распространяется посредством радиоволн в открытом воздушном пространстве): наземные, радиорелейные, космические.

По масштабности (по территориальному признаку) транспортные сети подразделяют на три категории:

1. Сетевое ядро (соединяет города, страны и континенты). Требование по пропускной способности от единиц до сотен Гбит/с. Верхняя граница для США, Западной Европы и Японии; нижняя – для развивающихся стран.

2. Городская транспортная сеть (от сотен Мбит/с до десятков Гбит/с).

3. Сеть доступа (от единиц до сотен Мбит/с). Конечные пользователи могут подключаться к сети доступа со скоростью от десятка Кбит/с до единиц Мбит/.

Основным типовым каналом аналоговой транспортной сети является канал тональной частоты (ТЧ). Это типовой канал с полосой частот от 300 до 3400 Гц. Для увеличения пропускной способности каналы тональной частоты согласно рекомендациям CCITT (МКТТ) объединяют в группы:

первая группа – 12 каналов ТЧ,

вторая группа – 60 каналов ТЧ,

третья группа – 300 каналов ТЧ.

Допускается создание других групп, например, четвертичных – три 300-канальные группы.

В цифровых сетях цифровой канал представляет собой битовый тракт с цифровым (импульсным) сигналом на входе и выходе канала. Оконечное оборудование таких каналов работает только с цифровыми сигналами.

Базовым цифровым каналом является канал DS0 (Digital Signal, Level 0: цифрой сигнал нулевой уровень) со скоростью передачи информации 64 Кбит/с (стандарт для канала голосовой телефонии).

Цифровые каналы строятся на принципах либо плезиохронной цифровой иерархии (PDH — Plesiochronous Digital Hierarchy; 1960 гг.; разработана в лаборатории Bell Labs; устаревшая технология), либо синхронной цифровой иерархии (SDH —Synchronous Digital Hierarchy; 1988 г., ITU).

На основе DS0 строятся следующие каналы PDH.

DS1 (Digital Signal, Level 1). Объединение (уплотнение) 24-х каналов DS0, скорость -- 1.544 Мбит/с.

На такой скорости работает североамериканская линия (технология) T1. Технологическим аналогом T1 в Европе являются E1. Объединение 30-ти DS0, 2.048 Мбит/с.

Линии T1 разработаны в 60-х годах прошлого века американской компанией Bell Telephone System и использовались для голосовой связи и передачи факсов. При передаче используется временное разделение (уплотнение) каналов; частота дискретизации сигнала — 8000 1/с. Дискретные отсчеты (длительностью 5,2 миллисекунды) передаются последовательно с использование всех 24 каналов. В T1 возможно дробление каналов: каждый из 24 каналов может быть передан в индивидуальное распоряжение отдельного пользователя.

DS2. Объединение 4-х DS1 (96 DS0), скорость -- 6.312 Мбит/с. Линия T2. В Европе E2. Объединение 4-х E1, скорость —- 8.448 Мбит/с.

DS3. Объединение 7-ми DS2 (672 DS0), скорость —- 44.736 Мбит/с. Линия T3. В Европе E3 Объединение 4-х E2, скорость —- 34.368 Мбит/с.

DS4. Объединение 6 DS3 (4032 DS0), скорость — 274,176 Мбит/с. Линия T4. В Европе E4. Объединение 4-х E3, скорость — 139.264 Мбит/с.

В Европе имеется так же E5. Объединение 4-х E4, скорость — 564.992 Мбит/с.

SDH-технология в сравнении с PDH-технологией обладает рядом значительных преимуществ. SDH-технология позволяет избежать использования большого числа дорогостоящих мультиплексоров и демультиплексоров и создать гибкую, надежную и хорошо управляемую структуру сети, позволяющую (в отличие от PDH) напрямую выделять требуемые цифровые каналы из высшей иерархии SDH. В PDH для выделения необходимого канала мультиплексор должен демультиплексировать весь информационный поток. Преимущества SDH таковы, что SDH стала технологией N 1 для создания транспортных сетей.

Следует отметить, что созданию SDH-технологии предшествовала североамериканская технология SONET (Synchronous Optical NETwork, ANSI, 1995г.), которую с известным упрощением можно рассматривать как часть стандарта SDH. В табл. 1.1 показано соответствие между иерархиями SDH и SONET.

Таблица 1.1. Уровни иерархии SDH и SONET

Скорость передачи Мбит/с	Уровень SDH	Уровень иерархии SONET
51,84	STM-0 или STM-1/3	OS-1/STS-1
155,52	STM-1	OC-3/STS-3
466,56	STM-3	OC-9/STS-9

622,08	STM-4	OC-12/STS-12
933,12	STM-6	OC-18/STS-18
1244,16	STM-8	OC-24/STS-24
1866,24	STM-12	OC-36/STS-36
2488,32	STM-16	OC-48/STS-48
9953,28	STM-64	OC-192/STS-192
39813,12	STM-256	OC-768/ STS-768

В стандарте SDH уровни иерархии именуют Synchronous Transport Module level N (STM-N).

В технологии SONET используются два обозначения:

Optical Carrier level N (OC-N) для волоконно-оптического кабеля;

Synchronous Transport Signal level N (STS-N) для электрического сигнала.

Несмотря на свое название SONET не ограничивается только оптическими каналами. Спецификация SONET определяет требования для оптического одно- и многомодового волокна, а также для 75-омного коаксиального кабеля.

1.3. Технология ISDN

ISDN (Integrated Services Digital Network) -- цифровая сеть с интеграцией услуг (концепция разработана в 1974 году). Технология обеспечивает передачу любого вида информации в цифровой форме (речь, видеоинформация, компьютерные данные, графические изображения, факс и т.д.). Технология ISDN использует те же абонентские линий, что и аналоговая телефония (длина линии до 6 км, посредством репитеров длина может быть увеличена).

Первая ISDN станция введена в эксплуатацию в 1976г. Технология стандартизована в 1984 году (CCITT I.122, I.430, I.43). Стандарт в Европе: **Euro ISDN** (ETSI —- European Telecommunications Standards Institute). Становление технологии ISDN характеризуется вялотекущим развитием в 80-е годы прошлого столетия, обусловленным проблемой совместимости и дороговизной оборудования и актуализацией в начале 90-х гг.

Стандартное подключение линий ISDN осуществляется по интерфейсам **BRI** (Basic Rate Interface) или **PRI** (Primary Rate Interface).

Интерфейс BRI (базовый доступ, служба 2B+D или ISDN2) обеспечивает два дуплексных B-канала по 64 Кбит/с каждый и один служебный канала D-канал с пропускной способностью 16 Кбит/с для обеспечения взаимодействия (синхронизации сигнализации) городской АТС и ISDN - оборудования. В качестве линии ISDN BRI использует обычную

линию телефонной сети общего пользования (ТСОП). Каждому B-каналу присваивается номер, аналогичный телефонному. B-каналы используются индивидуально и коммутируются по вызову. Абонентская линия ISDN заканчивается блоком сетевого окончания NTBA, к которому можно подключить до 8 цифровых оконечных устройств (однотипных или разнотипных: цифровой телефон, компьютер, факс, видеотелефон и т.д.). Однако одновременная работа возможна только для двух устройств.

Интерфейс **PRI** (первичный доступ **ISDN**, служба 30B+D или **ISDN30**) обеспечивает в Европе 30 дуплексных B-каналов по 64 Кбит и один специальный D-канал с пропускной способностью 64 Кбит/с (пропускная способность PRI составляет 2,048 Мбит/с). PRI может применяться для соединения удаленных филиалов с центральным офисом, а так же для подключения учрежденческих АТС к цифровой телефонной сети. Операторы могут предоставлять PRI и с требуемым числом B-каналов (например, с четырьмя или шестью).

1.4. Технологии xDSL

Термин Digital Subscriber Line (**DSL)** —- цифровая абонентская линия появился в начале 80-х годов прошлого столетия и употреблялся для обозначения ISDN-линии. В настоящее время понятие DSL охватывает множество цифровых технологий, которые отличаются от ISDN более высокими скоростями передачи данных, разнообразием принципов физической транспортировки, а так же тем, что используют некоммутируемые, постоянно включенные линии.

Понятие DSL объединяет следующие основные технологии:

ADSL (Asymmetric Digital Subscriber Line) —- асимметричная цифровая абонентская линия.

R-ADSL (Rate-Adaptive Digital Subscriber Line) —- цифровая абонентская линия с адаптацией скорости соединения.

ADSL Lite (G.lite), низкоскоростной вариант ADSL.

HDSL (High Bit-Rate Digital Subscriber Line) —- высокоскоростная цифровая абонентская линия (работает по двум медным парам).

HDSL 2 —- более современная разработка HDSL (работает по одной медной паре).

IDSL, (ISDN Digital Subscriber Line) —- цифровая абонентская линия ISDN.

SDSL (Single Digital Subscriber Line) —- однолинейная цифровая абонентская линия.

VDSL (Very High Bit-Rate Digital Subscriber Line) —- сверхвысокоскоростная цифровая абонентская линия.

Асимметричные ADSL, R-ADSL, ADSL Lite технологии используются для интерактивных приложений (просмотр Web-страниц), а симметричные DSL технологии: для корпоративных приложений (почта, обмен файлами, видеоконференции).

Технология ADSL (разработана в начале 90-х гг.) является асимметричной: скорость передачи данных от сети к пользователю («нисходящего» потока) значительно выше скорости передачи данных в сеть от пользователя («восходящего» потока). ADSL обеспечивает по одной витой паре проводов скорость «нисходящего» потока данных от 1,5 Мбит/с до 8 Мбит/с и скорость «восходящего» потока данных от 640 Кбит/с до 1,5 Мбит/с. (нижние значения скоростей указаны для расстояния 5,5 км, верхние – для 3,5 км).

Технология R-ADSL обеспечивает те же скорости передачи данных, что и технология ADSL, но позволяет адаптировать скорость передачи к состоянию передающей среды.

ADSL Lite (G.lite) является дешёвым и простым в установке вариантом ADSL. Обеспечивает скорость «нисходящего» потока данных до 1,5 Мбит/с, «восходящего» потока до 512 Кбит/с или по 256 Кбит/с в обоих направлениях.

HDSL является симметричной технологией. Она обеспечивает скорость передачи 1,544 Мбит/с по двум парам и 2,048 Мбит/с по трем парам проводов на расстоянии 3,5 — 4,5 км. Телекоммуникационные компании используют технологию HDSL в качестве альтернативы линиям T1/E1. Для увеличения длины линии HDSL могут использоваться специальные повторители. Технология HDSL 2 является развитием технологии HDSL. Она обеспечивает HDSL характеристики, но использует одну пару проводов.

Технология IDSL обеспечивает дуплексную передачу данных на скорости 144 Кбит/с. Использует ту же, что и IDSL модуляцию 2B1Q, но, в отличие от ISDN, линия IDSL является некоммутируемой постоянно включенной линией.

SDSL как же как и технология HDSL обеспечивает симметричную передачу данных со скоростями, соответствующими скоростям линии T1/E1, но при этом SDSL использует только одну витую пару, а ее максимальное расстояние передачи ограничено 3 км. Технология SDSL в известном смысле является предшественницей технологии HDSL 2.

VDSL является самой высокоскоростной xDSL технологией. Обеспечивает (по одной витой паре) 13 - 52 Мбит/с для нисходящего потока и 1,5 - 2,3 Мбит/с для восходящего потока данных (в симметричном режиме поддерживаются скорости до 26 Мбит/с). Однако, максимальное расстояние передачи данных для этой технологии составляет 300 - 1300 метров. Новый стандарт VDSL2 (G.993.2) ориентирован на передачу данных по телефонному кабелю со скоростью до 100 Мбит/с в обоих направлениях на расстояниях до 350 метров.

1.5. Технология оптического спектрального уплотнения

Технология оптического спектрального мультиплексирования (уплотнения) позволяет в едином световом потоке, пересылаемом по оптическому волокну объединить от 4 до 200 и более информационных каналов с разной длиной волны (экспериментально достигнута пропускная способность в 1 Тбит/с для одной волоконно-оптической нити). На приемной стороне выполняется обратная операция: демультиплексирование каналов и выделение информационных сигналов.

Различают следующие технологии оптического спектрального мультиплексирования:

DWDM (Dense Wavelength Division Multiplexing) —- плотное спектральное уплотнение.

CWDM (Coarse Wavelength Division Multiplexing) —- грубое спектральное уплотнение.

SWDM (Selective Wavelength Division Multiplexing) —- селективное спектральное уплотнение.

Технология DWDM является самой совершенной и дорогостоящей. Применяются для построения высокоскоростных международных и региональных транспортных сетей. Цена передатчика DWDM в четыре-пять раз выше стоимости аналогичного устройства CWDM и, кроме того, DWDM требует дополнительных расходов, поскольку устройства DWDM потребляют больше энергии и рассеивают больше тепла. При этом лазеры DWDM обеспечивают скорость передачи до 10 Гбит/с, в то время, как лазеры CWDM только около 2,5 Гбит/с. Технология DWDM позволяет передавать в одном волокне более 200 каналов.

Технология CWDM рассчитана на применение в относительно коротких линиях (до 50 км) с небольшим количеством каналов (до 16). Системы CWDM, обеспечивая столь же высокую степень безопасности и качества обслуживания, как и DWDM, позволяют добиться максимального отношения пропускной способности к стоимости линии. CWDM применяются для связи между узлами корпоративной сети клиента и коммутационными центрами регионального провайдера.

Технология SWDM позволяет использовать узлы системы SDH/SONET для **“**включения” в существующее волоконно-оптическое кольцо еще одной длины волны путем подключения дополнительного модуля в существующие устройства; при этом не происходит усложнения топологии сети и не ухудшается ее управляемость.

1.6. Общие сведения о стандартах на информационные сети. Основные организации по стандартизации

1.6.1. Общие сведения о стандартах на информационные сети

Стандарт (по определению ISO). Технический стандарт или другой документ, доступный и опубликованный, коллективно разработанный или

согласованный и общепринятый в интересах тех, кто им пользуется, основанный на интеграции результатов науки, технологии, опыта, способствующий повышению общественного блага и принятый организациями, полномочными на национальном, региональном и международном уровнях.

Различают 5 уровней стандартов:

1. Стандарты международных организаций, например, ISO, IEC, ITU.

2. Стандарты международно-групповых объединений, например, CEN, CENELEC, ETSI;

3. Национальные стандарты, например, ANSI, BSI, DIN, ГОСТ, ГОСТ Р, СТБ;

4. Стандарты профессиональных организаций, например, IEEE, ISA, ISOC, IAB, IETF, IRTF, IESG, ECMA;

5. Стандарты отдельных фирм, например, Intel, Xerox, IBM.

Различают также юридические, фактические и промышленные стандарты.

Стандарт де-юре (de jure; юридически принятый) – это стандарт, который создан официально признанной организацией (ISO, IEC, ITU). Их иногда называют базовыми или формальными стандартами. Такие стандарты являются открытыми. Они доступны любому пользователю (платно или как RFC — бесплатно), а продукция, изготовленная на их основе, не требует лицензии. Стандарт де-юре может продаваться или, как RFC, распространяться свободно.

Стандарт де-факто (de facto; фактический) – стандарт на продукцию поставщика, который захватил большую часть рынка, и который другие поставщики стремятся эмулировать, копировать или использовать.

Промышленный стандарт – это стандарт, который широко применяется в промышленности. Это может быть как стандарт де-юре, так и де-факто. Неудачные стандарты де-юре часто не становятся промышленными.

1.6.2. Основные организации по стандартизации

ISO (International Organization for Standardization; ИСО) — Международная организация по стандартам. Основана в 1946 году. Осуществляет разработку международных стандартов в различных областях человеческой деятельности путем координации деятельности национальных организаций. ISO работает под эгидой ООН и включает представителей более 100 стран**.**

IEC (International Electrotechnical Commission: Международная Электро-техническая Комиссия; **МЭК**). Работает под эгидой ООН.

JTC1 (Joint Technical Committee 1 — Объединенный технический комитет 1). Обеспечивает формирование системы базовых стандартов в области информационных технологий (ИТ) и их расширений для конкретных сфер деятельности. Образован в 1987 г. на основе ISO и IEC (ISO /IEC).

Работа в JTC1 над стандартами ИТ, относящимися к окружению открытых систем (Open Systems Environment - OSE), распределена по следующим подкомитетам (Subcommittees - SC):

- C2 - Символьные наборы и кодирование информации.
- SC6 - Телекоммуникация и информационный обмен между системами.
- SC7 - Разработка программного обеспечения и системная документация.
- SC18 - Текстовые и офисные системы.
- SC21 - Открытая распределенная обработка (Open Distributed Processing - ODP), управление данными (Data Management - DM) и взаимосвязь открытых систем (Open System Interconnection - OSI).
- SC22 - Языки программирования, их окружения и интерфейсы системного программного обеспечения.
- SC24 - Компьютерная графика.
- SC27 - Общие методы безопасности для ИТ-приложений.

Дополнительно к названным подкомитетам была создана группа по функциональным стандартам **(**Special Group on Functional Standards **- SGFS)** для обработки предложений по Международным стандартизованным профилям (International Standardized Profiles - ISPs), представляющим определения профилей ИТ.

CCITT (International Consultative Committee for Telegraphy and Telephony) — международный комитет по телефонии и телеграфии (МККТТ), организован в 1957 году. Имел французское название. Документы CCITT носят название "Recommendations" (Рекомендации, с большой буквы). С 1993 г. стандартизацией в области телекоммуникаций (с сохранением преемственности) занимается сектор ITU-T, стандарты которого также называются Рекомендациями (так что, например, Рекомендации V.42 CCITT и V.42 ITU-T означают одно и то же).

ITU (International Telecommunication Union) **—** международный телекоммуникационный союз, структурное подразделение ООН. Этот комитет называют также Международным союзом электросвязи (**МСЭ**).

ITU-T (International Telecommunications Union-Telecommunications Standardi-zation Sector; ITU-TSS, сокращенно: ITU-T**)** – один из трех секторов ITU. Другие сектора:

Сектор радиосвязи **(ITU-R).**

Сектор стандартизации телекоммуникаций и развития телекоммуникаций **(ITU-B),** специализируется по вопросами стратегии и политики в области связи.

В задачи ITU-T входит установление стандартов в области связи. Членами этого сектора являются министерства связи различных стран и крупные коммуникационные компании. Этот сектор вырабатывает стандарты (рекомендации) четырех серий:

E (E – серия) – общая эксплуатация в телефонной службе;

T - телематическое оконечное оборудование (включает все, кроме телефонии и телеграфии);

V - передача аналоговых сигналов;

X - передача цифровых данных.

К стандартам международного уровня относятся и стандарты семейства (стека) протоколов TCP/IP.

Координирует разработку этих стандартов техническая группа **IAB** (Internet Activities Board), которая включает подразделения **IRTF** и **IETF**.

IRTF **(**Internet Research Task Force**;** IRTF отвечает за исследования и разработку набора протоколов Internet) и IETF.

Подразделение IETF (Internet Engineering Task Force) включает более 80 рабочих групп. IETF выпускает стандарты TCP/IP в виде серии документов, названных RFC (Request for Comment). Стандарты TCP/IP всегда публикуются в виде документов RFC, но не все RFC являются стандартами. На май 2003 года количество RFC превышало 3500. Более детально вопросы, связанные с RFC будут рассмотрены в разделе курса «Стек протоколов TCP/IP.

ECMA (European Computer Manufacturers Association) – европейская ассоциация изготовителей вычислительных машин или позже: европейская ассоциация производителей компьютеров, ЕАПК. ECMA организована в 1961 г. по инициативе ведущих западноевропейский компаний в области средств обработки данных.

ANSI (American National Standards Institute) - Американский институт стандартов организация, ответственная за стандарты в США. ANSI является членом ISO.

BSI, DIN – национальные организации по стандартизации Англии и Германии соответственно.

В Республике Беларусь государственные стандарты бывшего СССР (ГОСТ) имеют статус государственных стандартов Республики Беларусь (Постановление Госстандарта РБ №3 от 17.12.1992г.).

ГОСТ Р – стандарты России,

СТБ — стандарты РБ. Различаются также отраслевые стандарты (ОСТ), стандарты предприятий (СТП) и руководящие документы отрасли (РД).

IEEE (Institute of Electrical and Electronic Engineers) — институт инженеров по электротехнике и радиоэлектронике. Профессиональная организация США, основанная в 1963 году для координации разработки компьютерных и коммуникационных стандартов. Подкомитет этой организации IEEE 802 (создан в 1980 г.) подготовил группу стандартов для локальных сетей.

ISA – Приборостроительное общество Америки, разрабатывает стандарты локальных сетей реального времени.

1.7. Эталонная модель OSI

1.7.1. Концепция OSI

RM OSI (Reference Model Open Systems Interconnection) — эталонная модель взаимодействия открытых систем (ЭМ ВОС) разработана международной организацией по стандартам ISO.

Модель OSI определяет общий подход к построению архитектуры систем распределенной обработки информации. Она описывает и регламентирует структуру взаимодействия открытых систем. Термин «открытая система» подчеркивает тот факт, что если какая-либо система отвечает стандартам, принятым в данной концепции, то эта система будет открыта для взаимодействия с любой другой системой, отвечающей этим стандартам. Работы по созданию OSI начались в ISO и в CCITT в середине 70-х годов прошлого столетия. В мае 1983 г. подкомитет ПК16 «Взаимосвязь открытых систем ISO» принял стандарт ISO 7498 «Базовая эталонная модель взаимодействия открытых систем» и практически одновременно CCITT принимает одноименную рекомендацию X.200. Оба документа опубликованы в конце 1984 г.

Из существующих сетевых концепций и архитектур комитет ПК16 выбрал сетевую концепцию OSI, близкую к концепции SNA фирмы IBA.

В основу эталонной модели положена идея декомпозиции процесса функционирования открытых систем на отдельные компоненты (подсистемы), называемые уровнями. Взаимодействие между уровнями по горизонтали осуществляется согласно стандартным протоколам. При этом по вертикали каждый нижестоящий уровень обеспечивает вышестоящему уровню определенный набор услуг (межуровневый стандартный интерфейс).

Протоколы регламентируют правила взаимодействия одинаковых уровней у различных пользователей, а межуровневый интерфейс — правила

взаимодействия смежных уровней одного пользователя. Набор услуг N-го уровня модели OSI (совокупность функциональных возможностей данного и всех нижележащих уровней, включая средства, реализующие эти возможности) составляет N-ую службу модели OSI (сервис N-го уровня или N-сервис). N-ая служба (N-сервис) предоставляет услуги N+1 уровню, так что в модели OSI можно выделить шесть уровней службы: физическая служба, канальная служба, сетевая служба, транспортная служба, сеансовая служба и представительная служба.

Основные понятия по описанию стандартов на службы различных уровней модели OSI определены в документах ISO TB8509 и CCITT X.210.

1.7.2. Основные понятия модели OSI

К основным понятиям модели OSI относятся:

1. Протокол — совокупность семантических и синтаксических правил, определяющих работу функциональных устройств в процессе связи.

2. Интерфейс — граница между двумя функциональными устройствами, определенная своими функциональными характеристиками, общими механи-ческими характеристиками соединения, характеристиками сигналов обмена и другими полезными характеристиками.

3. Пользователь службы — объект в некоторой открытой системе, который использует службу через точку доступа к службе (ТДС).

4. Точка доступа к службе —- точка, в которой логический объект уровня предоставляет сервис логическому объекту смежного верхнего уровня.

5. Услуга уровня — функциональная возможность, которую данный уровень вместе с нижерасположенными уровнями обеспечивает смежному верхнему уровню.

6. Служба уровня — совокупность услуг уровня и правил их использования.

7. Поставщик службы — некоторое множество объектов, обеспечивающих службу для ее пользователей.

8. Примитив службы – абстрактное, не зависящее от конкретной реализации, представление взаимодействия между пользователем и поставщиком службы.

9. Примитив запроса — примитив, инициируемый пользователем службы для вызова некоторой процедуры

10. Примитив индикации — примитив, инициируемый поставщиком службы для вызова некоторой процедуры либо для указания о ее вызове одним из взаимодействующих пользователей сервиса в ТДС данного уровня.

11. Примитив ответа — примитив, инициируемый пользователем службы для завершения в определенной ТДС некоторой процедуры, ранее вызванной посредством примитива индикации в этой ТДС.

12. Примитив подтверждения — примитив, инициируемый поставщиком службы для завершения в определенной ТДС некоторой процедуры, ранее вызванной посредством примитива запроса в этой ТДС.

1.7.3. Уровни OSI. Основные задачи и выполняемые функции

В модели OSI взаимодействие делится на семь уровней или слоев, см. рис.1.1. Каждый уровень имеет дело с одним определенным аспектом взаимодействия, так что проблема взаимодействия декомпозирована на 7 частных проблем, каждая из которых может быть решена независимо от других. Каждый уровень поддерживает интерфейсы с выше- и нижележащими уровнями.

Физический уровень выполняет передачу битов по физическим каналам, таким, как коаксиальный кабель, витая пара или оптоволоконный кабель. На этом уровне определяются характеристики физических сред передачи данных и параметров электрических сигналов (такие параметры, как: напряжение в сети, сила тока, число контактов на разъемах и т.п.). Типичными стандартами этого уровня являются, например RS232C, V35, IEEE 802.3 и т.п.

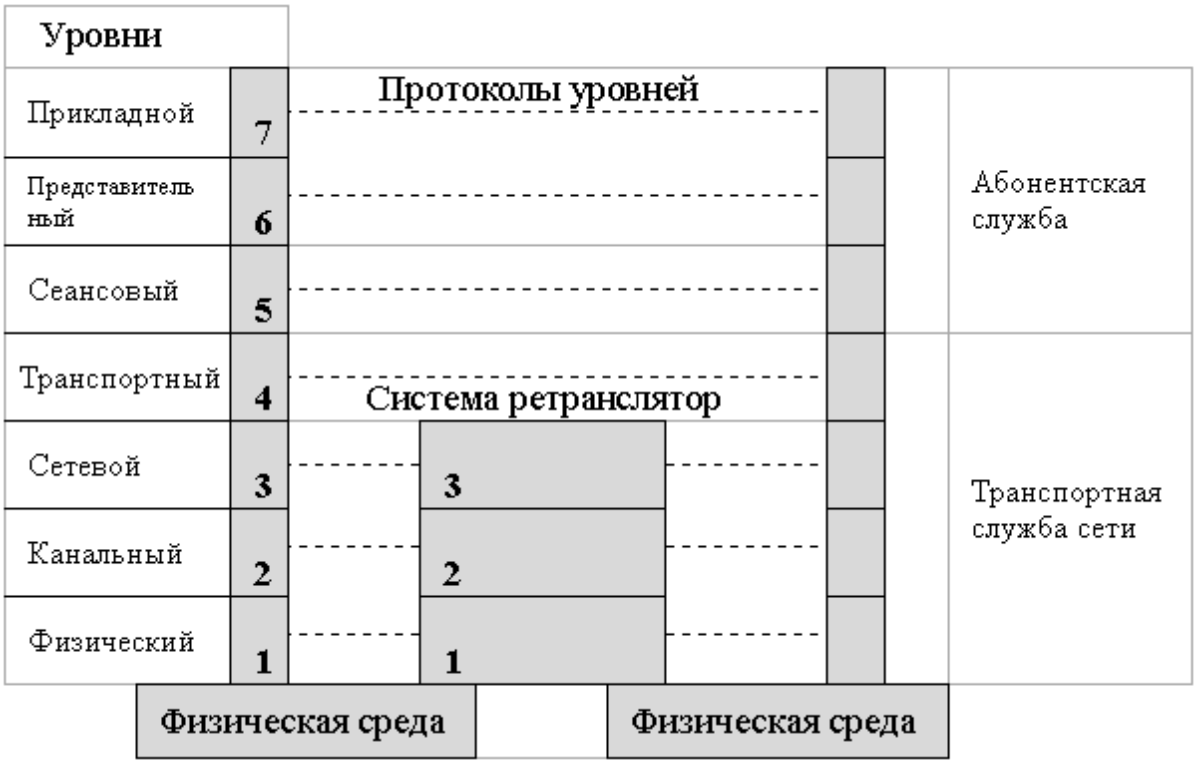

Рис. 1.1. Уровни RM OSI.

Канальный уровень обеспечивает передачу кадра данных между любыми узлами в сетях с типовой топологией, либо между двумя соседними узлами в сетях с произвольной топологией. В протоколах канального уровня заложена определенная структура связей между компьютерами и способы их адресации. Адреса, используемые на канальном уровне в локальных сетях, часто называют MAC - адресами. К канальному уровню относятся протоколы, определяющие соединение, например, SLIP (Serial Line Internet Protocol), PPP (Point to Point Protocol), NDIS, пакетный протокол, ODI и т.п.

Сетевой уровень обеспечивает доставку данных между любыми двумя узлами в сети с произвольной топологией, при этом он не отвечает за надежность передачи данных. К сетевому (межсетевому) уровню относятся протоколы, отвечающие за отправку и получение данных.

Транспортный уровень обеспечивает передачу данных между любыми узлами сети с требуемым уровнем надежности. Для этого на транспортном уровне имеются средства установления соединения, нумерации, буферизации и упорядочивания пакетов.

Сеансовый уровень предоставляет средства управления диалогом, позволяющие фиксировать, какая из взаимодействующих сторон является активной в настоящий момент, а также предоставляет средства синхронизации в рамках процедуры обмена сообщениями. Условно к этому уровню можно отнеси механизм портов протоколов TCP и UDP Berkeley Sockets. Однако обычно, в рамках архитектуры TCP/IP такого подразделения не делают.

Уровень представления. Уровень представления имеет дело с внешним представлением данных. На этом уровне могут выполняться различные виды преобразования данных, такие как компрессия и декомпрессия, шифровка и дешифровка данных (этот уровень необходим для преобразования данных из промежуточного формата сессии в формат данных приложения). В Internet это преобразование возложено на прикладные программы

Прикладной уровень представляет собой набор разнообразных сетевых сервисов, предоставляемых конечным пользователям и приложениям. Примерами таких сервисов являются, например, электронная почта, передача файлов, сетевое подключение удаленных терминалов. Этот уровень определяет протоколы обмена данными прикладных программ. В Internet к этому уровню могут быть отнесены такие протоколы, как: TELNET, FTP, SMTP, HTTP и др.

При построении транспортной подсистемы (транспортная служба сети) наибольший интерес представляют функции физического, канального и сетевого уровней, тесно связанные с используемым в данной сети оборудованием (сетевыми адаптерами, концентраторами, мостами, коммутаторами, маршрутизаторами). Функции прикладного, сеансового уровней и уровня представления (составляющие абонентскую службу) реализуются операционными системами и системными приложениями конечных узлов; при этом транспортный уровень выступает посредником между этими двумя группами протоколов.

В компьютерных сетях широко используется понятие стека протоколов, под которым понимается иерархически организованная совокупность протоколов, решающих задачу взаимодействия узлов сети.

Стек OSI (не путать **с** моделью OSI, которая является концептуальной схемой) представляет собой набор протоколов полностью соответствующих модели OSI. Он (стек OSI**)** включает независимые от производителей спецификации протоколов для всех семи уровней модели OSI. Протоколы OSI сложны и требуют более мощных компьютеров.

Стек OSI — международный, независимый от производителей, стандарт. Согласно программе GOSIP (США) все компьютерные сети, устанавливаемые в правительственных учреждениях США после 1990 года, должны или непосредственно поддерживать стек OSI, или обеспечивать средства для перехода на этот стек в будущем. Стек OSI более популярен в Европе, где меньше старых сетей, использующих свои собственные протоколы. Одним из крупнейших производителей, поддерживающих OSI, является компания AT&T.

На базе стека протоколов формируются транспортные профили. Например, профиль TC 54, который ориентирован на передачу данных в локальной сети FDDI.

1.8. Стеки протоколов. Стек протоколов TCP/IP

1.8.1. Понятие стека протоколов

Понятие стека протоколов как иерархически организованной совокупности протоколов, решающих задачу взаимодействия узлов сети рассмотрено в п. 1.7 ; там же обсужден стек OSI, который, в отличие от других стеков протоколов, полностью соответствует модели OSI.

Особенности сети и ее характеристики во многом определяются используемым стеком протоколов. Если в небольших сетях возможно использование одного стека, то в крупных корпоративных сетях используется, как правило, несколько стеков. В настоящее время в компьютерных сетях применяются следующие стандартные стеки протоколов:

TCP/IP,
Novell NetWare,
IBM SNA,
DECnet,
Apple Talk**,**

Протоколы стеков реализуются на различных уровнях модели OSI. Их можно разбить на три типа:

протоколы приложений, обеспечивающие взаимодействие и обмен данными для прикладных программ;

транспортные протоколы, устанавливающие сеансы коммуникаций между компьютерами;

сетевые протоколы, обеспечивающие формирование информации адресации и маршрутизации, контроль ошибок и выработку запросов на повторную передачу.

1.8.2. Стек протоколов TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) является промышленным стандартом протоколов для глобальных сетей. Основное назначение стека протоколов TCP/IP – обеспечение межсетевого взаимодействия. Под термином "TCP/IP" обычно понимают все, что связано с протоколами TCP/IP (это не только названные проколы, но и протоколы, построенные на использовании TCP и IP, а также соответствующие прикладные программы).

В настоящее время стек TCP/IP является лидером сетевых технологий, что объясняется следующими его свойствами:

- TCP/IP наиболее завершенный стандартный и популярный стек сетевых протоколов, имеющий многолетнюю историю.
- Практически все большие сети передают основную часть своего трафика посредством протокола TCP/IP.
- На этом стеке протоколов работает сеть Internet.
- Этот стек служит основой для создания Intranet (интрасетей) – современной технологии корпоративных сетей (транспортные услуги Internet, гипертекстовая технология WWW).
- Все современные операционные системы поддерживают стек TCP/IP.
- TCP/IP это гибкая технология для соединения разнородных систем (как на транспортном подсистем, так и на прикладном уровне).
- Это устойчивая масштабируемая межплатформенная технология для приложений клиент-сервер.

Важность стека протоколов TCP/IP такова, что обычно под **internet** (internet с маленькой буквы) понимают технологию обмена данными, основанную на использовании семейства протоколов TCP/IP. Другими словами, Интернет с маленькой буквы – это то же, что и **Internet-технологии.** В то время как под **Internet (**Интернет с большой буквы) понимают глобальное сообщество мировых сетей, использующее internet для обмена данными**.** Поэтому изучение принципов построения сети Internet необходимо начинать с семейства протоколов межсетевого обмена TCP/IP.

Координирует разработку стандартов стека протоколов **TCP/IP** техническая группа **IAB** (Internet Activities Board), которая **о**бразованна в 1983 году (после реорганизации ICCB – Internet Configuration Control Board, 1981 г.) как исследовательская группа DARPA (Агентство перспективных исследований министерства обороны США). С июня 1992 г. **IAB** работает под эгидой **IS** (Internet Society; создана в январе 1992 г.).

Техническая группа **IAB** включает подразделения **IRTF** и **IETF.** IRTF (Internet Research Task Force) отвечает за исследования и разработку набора протоколов Internet. Подразделение **IETF** (Internet Engineering Task Force**)** включает более 40 рабочих групп и выпускает стандарты TCP/IP в виде

серии документов, называемых **RFC (**Request for Comment). Стандарты TCP/IP всегда публикуются в виде документов RFC, но не все RFC определяют стандарты.

Стек протоколов TCP/IP описан **в RFC 1112, RFC 1123, RFC 1823.**

Любой RFC должен строго соответствовать требованиям, изложенным в RFC 1543 (Инструкция авторам RFC).

При чтении RFC (для уяснения требований к реализации протокола) необходимо придерживаться следующей интерпретации ключевых слов (RFC 1123):

MUST (необходимо, должен)

Применяется для указания, что данное требование спецификации необходимо обеспечить в любом случае.

SHOULD (рекомендуется, следует)

Используется для указания, что данное требование спецификации должно быть обеспечено, если этому не препятствуют серьезные причины.

MAY (возможно, может)

Используется для указания, что данное требование спецификации является опциональным и может быть либо реализовано, либо нет - по необходимости.

Реализация считается несовместимой, если нарушено хотя бы одно из **необходимых** требований спецификации протокола. Реализация, удовлетворяющая всем **необходимым** и **рекомендуемым** требованиям, называется **полностью совместимой**, а удовлетворяющая всем **необходимым**, но не всем **рекомендуемым** требованиям называется условно совместимой.

Протокол RFC может находиться в следующих состояниях:

Предлагаемый протокол (**Proposed Standard**).

Протокол был предложен в качестве стандарта и находится в стадии начального рассмотрения

Предварительный стандарт (**Draft Standard**).

Протокол прошел начальное рассмотрение и находится в почти законченном виде. Имеются, по крайней мере, две его независимых реализации.

Стандартный протокол (**Internet Standard**).

Протокол пересмотрен и принят как полный стандарт. Он является составной частью TCP/IP.

Экспериментальный протокол (**Experimental**).

Протокол пока не предлагался для стандартизации; с ним проводятся эксперименты.

Ознакомительный протокол (Informational).

Протокол разработан сторонней организацией, находится вне компетенции IAB и опубликован в виде RFC для ознакомления. Состояние и статус протоколам семейства TCP/IP присваивает IAB.

Устаревший протокол (**Historic**).

Протокол устарел и в настоящее время не используется.

Протокол может иметь следующий статус:

Обязательный. Все узлы, использующие TCP/IP, должны реализовывать этот протокол.

Рекомендуемый. Поощряется использование данного протокола во всех узлах

Используемый по выбору. Узлы могут реализовывать этот протокол по выбору.

Ограниченного пользования. Протокол не предназначен для широкого использования, например, он может быть экспериментальным.

Нерекомендуемый. Данным протоколом пользоваться не рекомендуется. Например, не рекомендуются устаревшие протоколы.

1.8.3. Общая характеристика стека протоколов TCP/IP

Приведенная на рис. 1.2 схема стека протоколов TCP/IP является упрощенным представлением этого стека протоколов. Она иллюстрирует лишь общее представление о месте наиболее известных протоколов. Современные IP-сети гораздо сложнее, так например, прикладной уровень этого стека содержит буквально тысячи протоколов.

Краткая характеристика приведенных на рис 1.2 протоколов.

IP – межсетевой протокол, обеспечивает сервис доставки пакетов между узлами.

ARP – протокол разрешения адресов, отображает межсетевые адреса в физические.

RARP – обратный протокол разрешения адресов, отображает физические адреса в интерсетевые.

ICMP – межсетевой протокол, обеспечивает передачу управляющих сообщений и сообщений об ошибках между хостами (рабочими машинами) и шлюзами.

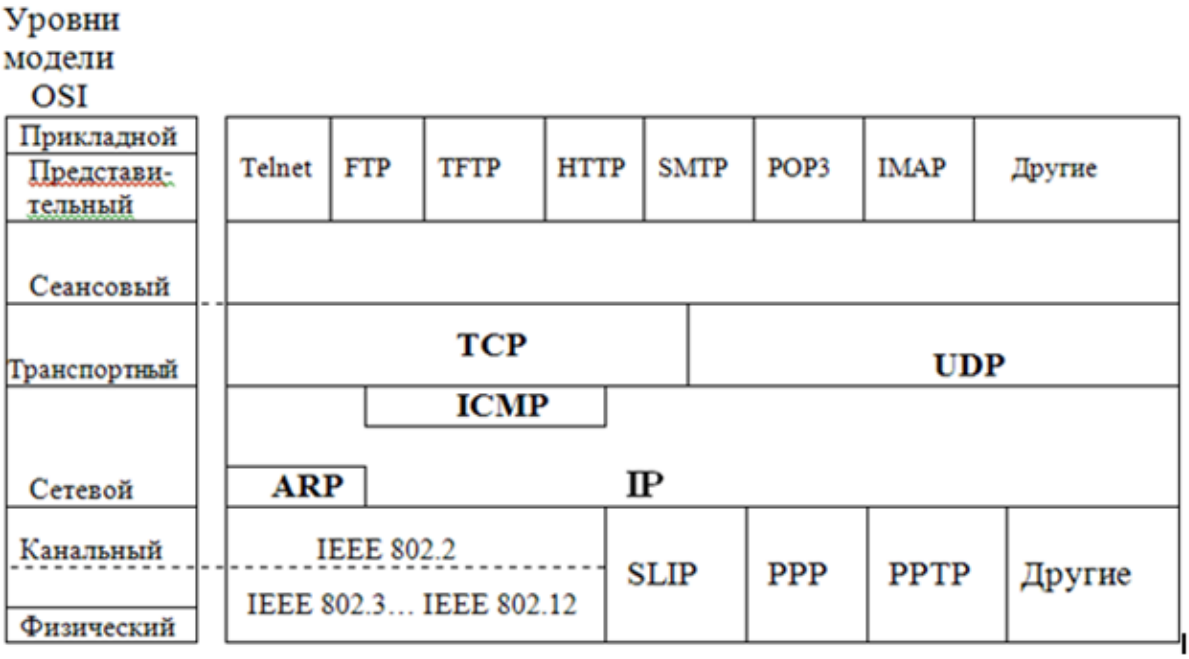

Рис. 1.2. Соотношение стека протоколов TCP/IP и модели OSI.

TCP –- протокол управления передачей, обеспечивающий сервис надежной доставки потока данных между клиентами.

UDP – пользовательский дейтаграммный протокол, обеспечивает ненадежный сервис доставки пакета без установления соединения между клиентами.

Telnet – протокол эмуляции терминала.

FTP – протокол транспорта файлов.

TFTP – упрощенный FTP.

SMTP – протокол простой почтовой службы (передачи почты).

POP3 –- протокол почтового отделения (получения почты из почтового ящика)

IMAP – протокол расширяющий возможности **POP3** (позволяет управлять почтой непосредственно на почтовом ящике сервера).

HTTP – протокол передачи гипертекстовой информации, обеспечивает доступ к WWW.

Стек TCP/IP отличается от стека OSI. Он содержит четыре уровня.

Рассмотрим специфику этих уровней.

Уровень 4 (уровень доступа к сети) соответствует физическому и канальному уровням модели OSI. Этот уровень является **сетевым интерфейсом стека TCP/IP**. В стандартах стека TCP/IP он специфицируется лишь частично, но поддерживает все популярные стандарты физического и канального уровня. Для локальных сетей это **Ethernet**, **Token Ring**, **FDDI**, **100VG-AnyLAN и др.,** для глобальных сетей — протоколы соединений "точка-точка" **SLIP** и **PPP**, протоколы территориальных сетей с коммутацией пакетов **X.25**, Frame Relay. Разработана также специальная

спецификация, определяющая использование технологии **ATM** в качестве транспорта канального уровня.

Обычно при появлении новой технологии локальных или глобальных сетей она быстро включается в стек TCP/IP посредством разработки соответствующего стандарта (RFC), определяющего метод инкапсуляции IP-пакетов в кадры протоколов новой технологии.

К 3-му уровню *(*уровню Internet или уровню межсетевого взаимодействия) относятся не только протоколы **IP, ARP, RARP, ICMP,** но и все протоколы, связанные с составлением и модификацией таблиц маршрутизации. К ним, например, относятся: протоколы сбора маршрутной информации **RIP** (Routing Internet Protocol) и **OSPF** (Open Shortest Path First).

На 2-ом уровне (транспортном уровне) функционируют протокол управления передачей **TCP** (Transmission Control Protocol) и протокол дейтаграмм пользователя **UDP** (User Datagram Protocol). Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования виртуальных соединений. Протокол UDP (также как и протокол IP) обеспечивает ненадежную передачу прикладных пакетов дейтаграммным способом.

Уровень 1 (прикладной уровень) характеризуется большим количеством протоколов и сервисов. Основные протоколы этого уровня указаны на рис 1.2.

Тема 2. Общая характеристика локальных сетей

2.1. Отличительные особенности локальных сетей

Локальные сети (LAN), обеспечивая совместное использование информационных ресурсов сети и периферийных устройств, характеризуются следующими особенностями:

1. Локальная сеть, как правило, является собственностью организации (фирмы) и обслуживает сотрудников, которые подчинены руководству этой организации (фирмы). Другие сети MAN и WAN ориентированы на обслуживание клиентов (не сотрудников), которые используют сеть для своих нужд в рамках договора об обслуживании.

2. Обеспечивают возможность совместного использования общей коммуникационной среды при высокой достоверности передачи данных (10^{-8}-10^{-14}) и достаточно высокой скорости передачи данных (от 4 Мбит/с до единиц Гбит/с.). В настоящее время на отдельных магистральных участках глобальных сетей скорость передачи может быть и значительно выше (до сотен Гбит/с), но в WAN имеют место существенные задержки при маршрутизации трафика;

3. Размещаются на сравнительно небольшой территории;

4. Обеспечивают высокий уровень взаимодействия устройств сети;

5. Содержат относительно дешевые средства передачи и интерфейсные устройства;

6. Обеспечивают простое и недорогое наращивание сети и соединение с другими сетями.

К основным характеристикам ЛС относятся:

топология сети,
скорость передачи данных,
размер сети,
физическая среда, используемая для передачи данных,
используемые протоколы и методы доступа**.**

2.2. Топология локальных сетей

Различаются следующие основные виды топологии локальных сетей: звездообразная, шинная, кольцевая. Под топологией понимают обобщенную геометрическую модель физической структуры сети.

Звездообразная топология (рис.2.1) характеризуется наличием центрального узла, к которому подключаются компьютеры (рабочие станции или сервера). В качестве такого узла может использоваться концентратор (Hub), коммутатор (Switch) или специальный компьютер (сетевой сервер с функциями коммутации и управления локальной сетью).

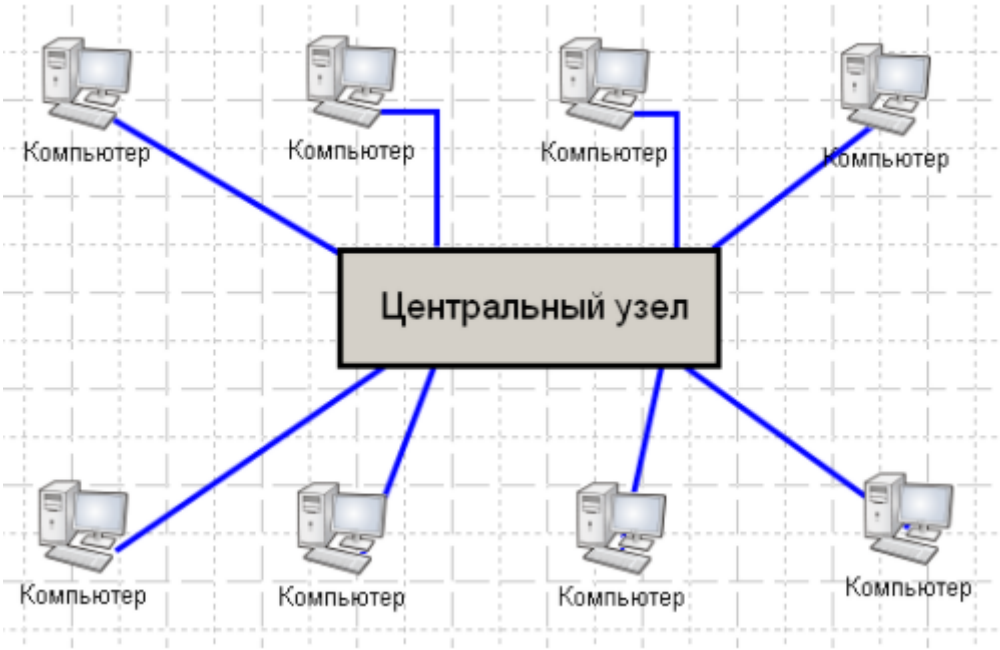

Рис. 2.1 Звездообразная топология сети**.**

В локальной сети с шинной топологией (рис.2.2) компьютеры с помощью сетевых адаптеров подключаются к шине (общей магистрали), в качестве которой чаще всего используется (использовался) коаксиальный кабель с заглушками (терминаторами) на концах кабеля.

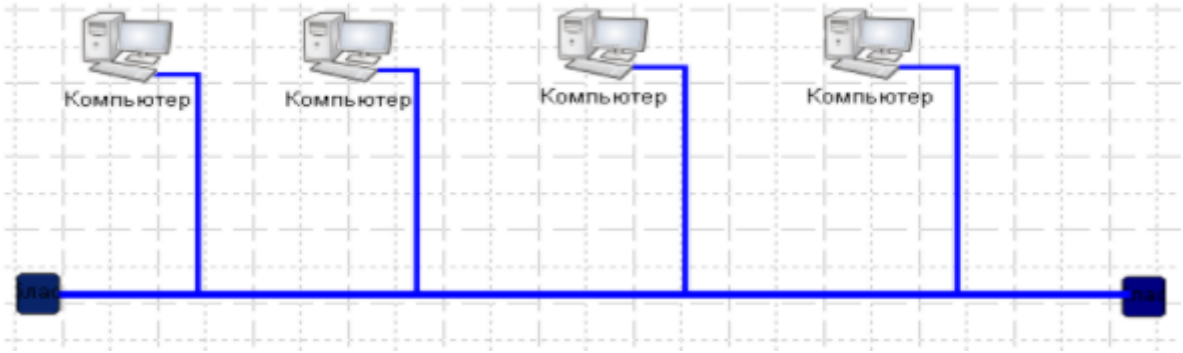

Рис. 2.2. Шинная топология сети.

Следует иметь в виду, что физическая топология сети (как мы увидим в последующих разделах курса) может не совпадать с ее (сети) логической организацией. Так, например, локальная сеть, имеющая звездообразную топологию, логически может иметь шинную организацию и, наоборот.

В локальной сети с кольцевой топологией (рис.2.3) компьютеры подключаются к кольцу, при этом применяется так называемый эстафетный метод передачи данных (данные до адресата передаются от компьютера к компьютеру).

Рис. 2.3. Кольцевая топология сети.

Современные локальные сети, как правило, имеют более сложную топологическую структуру. Они состоят из объединения локальных подсетей с однотипной топологией либо содержат определенную совокупность подсетей с разными топологиями. В этом плане различают: древовидную топологию (комбинация локальных сетей с шинной топологией), топологию типа распределенная «звезда» (комбинация сетей со звездообразной топологией), смешанную топологию (некоторая комбинация из двух или трех рассмотренных выше видов топологии).

2.3. Классификация аппаратно-программных средств локальных сетей

К аппаратным средствам ЛС относятся:

1. Компьютеры (IBM PC, Sun, Next, Macintosh и др.)

2. Сетевые адаптеры, адаптеры локальных радиосетей (специализированные радиомодемы).

3. Соединительные средства:

3.1. Сетевые соединительные средства: коннекторы , трансиверы, репитеры , концентраторы , коммутаторы, мосты.

3.2. Межсетевые соединительные средства: репитеры, мосты, маршрути-заторы, бранмауэры, шлюзы, модемы.

4.Передающая среда:

4.1. Проводная передающая среда (коаксиальный кабель, витая пара, волоконно-оптический кабель).

4.2. Беспроводная передающая среда (широкополосные радиосигналы, маломощное СВЧ-излучение, инфракрасное излучение).

5. Периферийное оборудование (принтеры, плоттеры, сканеры и т.д.).

К программным средствам ЛС относятся:

1. Сетевые операционные системы.

2. Сетевые драйверы.

3. Сетевые СУБД, серверы баз данных.

4. Сетевые утилиты:
4.1. Операционные сетевые утилиты.
4.2. Сетевые утилиты администрирования.
4.3. Смешанные утилиты.

2.4. Одноранговые и двухранговые локальной сети

Компьютер в локальной сети как участник сетевого взаимодействия теряет часть своей автономии. При этом сетевые программные средства компьютера составляет часть сетевой операционной системы в широком смысле слова. Так что под сетевой операционной системой в широком смысле понимают совокупность операционных систем отдельных компьютеров, обеспечивающих обмен сообщениями и разделение ресурсов по единым правилам (протоколам). В узком же смысле сетевая ОС — это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

Локальные сети (и сетевые операционные системы) делятся на одноранговые (децентрализованные или пиринговые) и двухранговые (или серверные, или клиент-сервеные, или сети с централизованным управлением). Существуют также гибридные или частично децентрализованные сети,

В одноранговой сети каждый компьютер (узел) является как клиентом, так и сервером. Компьютер с установленной одноранговой ОС, имеет потенциально равные возможности (peer; peer-to-peer); ресурс любого такого компьютера, объявленный разделяемым, становится доступным всем компьютерам сети. Одноранговые сети появились в 1985 г. (Apple Macintosh). Примеры одноранговых ОС: ОС LANtastic, Personal Ware, Windows for Workgroup, Windows NT Workstation, Windows 95, Windows 98, Windows 2000 Professional, Windows XP.

Одноранговые сети просты в организации и эксплуатации. Применяются для объединения небольших групп пользователей, не предъявляющих высоких требований к надежности работы сети, к защищенности информации от несанкционированного доступа и к скорости доступа.

В локальных сетях предприятий и корпораций используются клиент-серверные сетевые ОС. Примеры клиент-серверных сетевые ОС: Banyan Vines, Novell NetWare, IBM LAN Server, Sun NFS, Windows NT Server, Windows 2000 Server (семейство), Windows 2003 Server (семейство), Windows 2008 Server (семейство).

2.5. Роли компьютеров в локальной сети

В локальных сетях компьютеры могут использоваться в качестве:

1. Клиентов, которые используют сетевые ресурсы, но не предоставляют свои ресурсы другим компьютерам.

2. Одноранговых узлов, работающих с сетевыми ресурсами и разрешающих доступ других машин к своим ресурсам.

3. Серверов, предоставляющих сервисные услуги другим компьютерам (файловый сервер, сервер печати, сервер приложений, сервер баз данных, FTP- сервер, SMTP-сервер, POP-сервер, WWW-сервер и т.д.). Компьютеры могут выполнять несколько серверных функций одновременно, например, совмещать работу с файлами, службу печати, работу с базами данных.

Файловые серверы обеспечивают: передачу, хранение, синхронизацию и архивирование файлов. Синхронизация гарантирует хронологическое изменение файлов и правильное их обновление.

Сетевая печать сокращает расходы за счет совместного доступа к принтерам, в особенности, если применяются дорогие модели устройств печати (высококачественные цветные принтеры, высокоскоростные и крупноформатные принтеры, графопостроители). Принтеры могут устанавливаться в любом месте сети. К службе печати относится и служба передачи факсимильных сообщений

Серверы приложений позволяют клиентам использовать дополнительные вычислительные мощности, дорогостоящего прикладного ПО, а также обеспечивать централизованную защиту данных. Серверы приложений по технологии несколько напоминают централизованную обработку (модель, применяемую в мэйнфреймах фирмы IBM SNA).

Серверы баз данных предоставляют компьютерам доступ к мощным централизованным или распределенным базам данных. Для пользователя распределенная база данных выглядит как единое целое, хотя ее данные могут быть распределены по всей сети, обычно ближе к тем пользователям, которым нужна соответствующая информация.

Тема 3. Основные методы доступа, стандарты и протоколы локальных сетей

3.1. Основные методы доступа к среде передачи данных

Для доступа к разделяемой среде передачи данных в локальных сетях используется следующие основные виды методов доступа:

методы случайного доступа,

методы маркерного доступа.

При методе случайного доступа каждая станция сети имеет возможность получить доступ к среде в любой необходимый для нее момент времени. Если передающая среда занята, то станция повторяет попытки до тех пор, пока не получит требуемый доступ.

Принцип случайного доступа имеет различные реализации, но широкое применение получил метод случайного доступа технологии **Ethernet** (Стандарт **IEEE 802.3** -- де-юре, его модификации и **Ethernet LAN –** де-факто**,** предложенный компанией Xerox (1975 г.) и расширенный совместно Xerox, Intel и DEC). Однако истоки этого метода связывают с радиосетью **ALOHA**, в которой впервые был использован простейший метод случайного доступа (**Ether –** эфир**).**

В технологии стандарта IEEE 802.3 используется метод доступа к среде CSMA/CD (Carrier sense multiple access/collision detection) -- множественный доступ к среде с контролем несущей и обнаружением конфликтов (коллизий).

Сущность этого метода доступа состоит в следующем. Каждая рабочая станция, подключенная к сети, прослушивает сеть как до начала передачи (контроль несущей), так и во время собственной передачи (обнаружение конфликтов). Прослушивание сети до передачи позволяет ожидающей станции дождаться освобождения канала и тут же начать передачу своего пакета. Однако таких станций, ожидающих передачу (и затем начавших ее) может оказаться несколько. В результате возникает конфликт, Станция, передающая пакет, обнаружит это по характеру сигналов в канале (обнаружение конфликтов) и прекратит передачу (сокращается время занятости канала). Возобновление передачи произойдет с небольшой задержкой, время задержки для каждой станции свое. Реально конфликты приводят к уменьшению быстродействия сети в лишь том случае, если работают порядка 80 – 100 станций, а при загрузке сети на 35-40% коллизии могут существенно замедлить работу сети.

В беспроводных локальных сетях (IEEE 802.11) из-за невозможности обнаружения конфликтов вместо CSMA/CD используется модифицированный метод доступа к среде: CSMA/CA (метод множественного доступа с контролем несущей и предотвращением столкновений).

Методы маркерного доступа основаны на детерминированной передаче от одного узла сети к другому специального кадра информации — маркера доступа. Маркерные методы доступа используются в сетях **Token Ring, ArcNet** (в настоящее время потерявших актуальность) и **FDDI**. В таких сетях право на доступ к среде передается циклически от станции к станции по кольцу.

Метод доступа ArcNet (Стандарт ANSI 878.1) разработан фирмой DataPoint (начало 70 гг.), положен в основу стандарта IEEE 802.4 (Token-bus).

Методом доступа абонентов в сети является эстафетная передача маркера. Сущность этого метода доступа сводится к следующему. Каждая рабочая станция локальной сети имеет свой уникальный физический адрес. По логическому кольцу сети непрерывно передается маркер (кадр строго заданного формата), Передача маркера осуществляется от станции к станции в порядке убывания их адресов с циклическим возвратом от станции с самым младшим адресом к станции с самым старшим адресом. Такая последовательная циркуляция маркера необязательно совпадает с физическим размещением станций в сети и образует логическое кольцо, которое, вообще говоря, не зависит от конфигурации локальной сети. Станция, получившая (захватившая) маркер, имеет возможность передать собственный пакет данных, добавив его к маркеру. Когда пакет данных дойдет до станции назначения, он будет отцеплен от маркера и передан станции. Станции, не входящие в состав логического кольца, не могут передавать маркер и инициировать передачу данных, однако они могут принимать кадры от других станций, отвечать на них и включаться в логическое кольцо при получении разрешений. Реальные сети, построенные на этом методе доступа, характеризовались низкой стоимостью оборудования и низкой скоростью передачи данных (2,5 Мбит/сек). Сети ArcNet потеряли популярность из-за низкой скорости передачи данных и патентованной замкнутой архитектуры. Последующим развитием технологии ArcNet являются сети ArcNet Plus (скорость передачи данных увеличена до 20 Мбит/сек) и TCNS, которые имеют максимальную скорость передачи данных 100 Мбит/сек и недороги, особенно по сравнению сетями FDDI.

Метод доступа Token Ring разработан IBM (филиалом IBM в Цюрихе в 1986 г.), положен в основу стандарта IEEE 802.5.

Сущность метода доступа. По кольцу циркулирует маркер строго заданного формата. Станция, получившая маркер, анализирует его, при необходимости модифицирует и при отсутствии у нее передаваемых данных обеспечивает продвижение маркера к следующей станции (каждая станция действует как активный повторитель). Если же станция имеет данные для передачи, то она удерживает поступивший маркер и преобразует его в кадр данных (добавляет адресную информацию, данные и другие, необходимые поля) и выдает этот кадр в исходящую линию. Маркер удерживается до возвращения посланного кадра. Каждая станция

анализирует адресную информацию кадров и при несовпадении адреса назначения и собственного адреса копирует кадр в исходящую линию. Если кадр адресован данной станции, то она копирует его в приемный буфер и ретранслирует его в исходящую линию. Станция-отправитель пакета, обнаружив вернувшийся кадр, удаляет его из кольца. Одна из станций кольца выполняет функцию неактивного монитора, наблюдая за состоянием активного монитора, и в случае его отказа готова перейти в состояние активного монитора. Кроме того, станции определяют ошибки функционирования сети и информируют о них все остальные станции для восстановления нормального функционирования.

Дальнейшее развитие технологии Token Ring нашло отражение в сетях FDDI, в которых применяется более сложный метод доступа к сети (два кольца, несколько маркеров и т. д.).

3.2.Основные стандарты для локальных сетей. Структура стандартов Комитета IEEE 802

Развитие и внедрение локальных сетей неразрывно связано с их стандартизацией. Ведущим разработчиком стандартов в области локальных сетей является **комитет по стандартизации для локальных и городских сетей IEEE 802** (сформирован в феврале 1980 г.).

Основными целями деятельности этого комитета являются создание, сопровождение и популяризация стандартов IEEE и эквивалентных им стандартов ISO, которые относятся в основном к первому и второму уровням модели OSI. В контексте спецификаций IEEE 802 термин LAN (Local Area Network) означает кампусную сеть (сеть, охватывающая комплекс зданий), а термин MAN (Metropolitan Area Network) – сеть, действующую в пределах города.

О значимости стандартов в области локальных сетей и, в частности, вкладе Комитета 802 свидетельствует тот факт, что согласно экспертным оценкам, ежегодный доход, получаемый мировой сетевой и телекоммуникационной индустрией благодаря стандартам этого комитета превышает 18 млрд. долларов.

Вопросами стандартизации в области локальных сетей занимаются и другие организации (см. рис. 3.1).

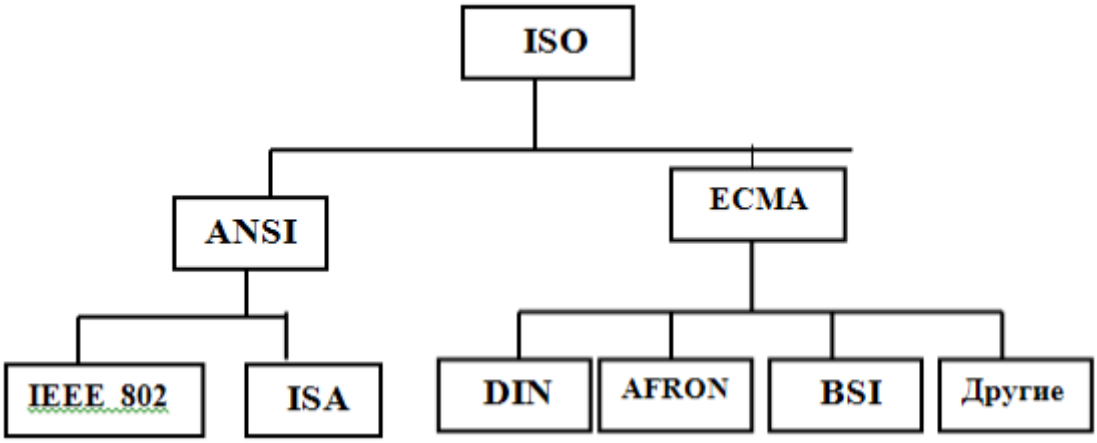

Рис. 3.1. Взаимосвязь ISO с другими организациями по стандартизации в области локальных сетей.

Сведения об организациях по стандартизации, приведенных на рис. 2.4, содержатся в п. 1.6; DIN, AFRON, BS**I** – национальные организации по стандартизации Германии, Франции и Англии соответственно. Структура стандартов Комитета 802 приведена на рис. 3.2.

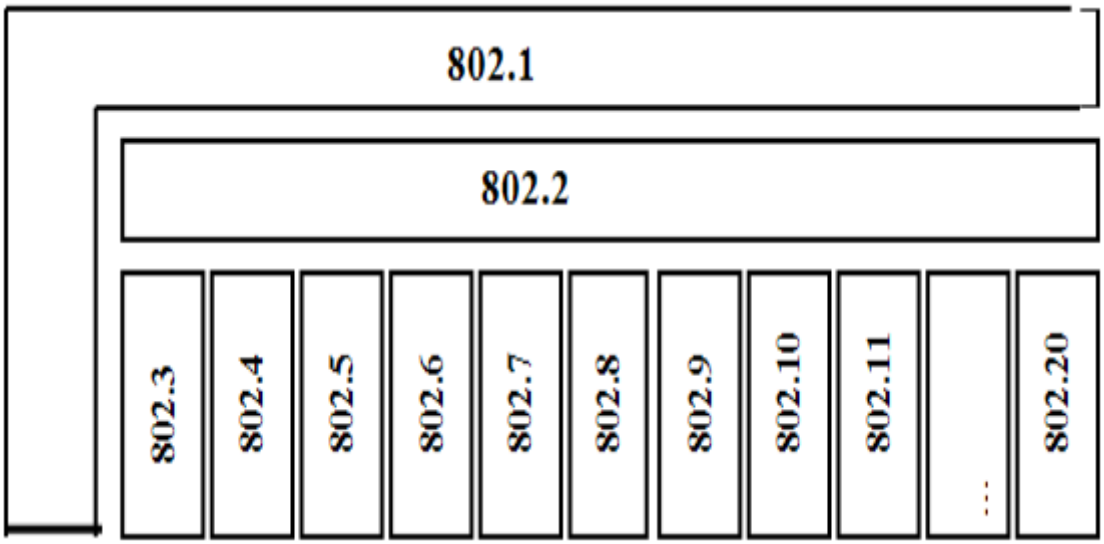

Рис.3 .2. Взаимосвязь стандартов Комитета IEEE 802

Аналогичные стандарты в области локальных сетей с несколько отличающимися обозначениями приняты ISO (ISO/DIS 8802/2.2 и т.д.) и ECMA (ECMA-81 и т.д.).

Разработка, техническая поддержка и сопровождение стандартов IEEE 802.1 – IEEE 802.22 осуществляется активными и «замороженными» рабочими группами (подкомитетами) Комитета IEEE 802. «Замороженные» рабочие группы (802.2, 802.4, 802.6, 802.7 и др.) как завершившие разработку своих стандартов осуществляют их техническую поддержку и сопровождение.

Основным приоритетом в работе Комитета IEEE 802 в настоящее время является разработка стандартов беспроводных технологий (этими технологиями занимаются восемь рабочих групп).

Назначение стандартов IEEE 802, поименованных на рис. 3.2.

IEEE 802.1 – методы объединения и архитектура управления локальными сетями, стандарты для мостовых соединений и виртуальных локальных сетей.

IEEE 802.2 – протоколы управления логическим каналом, спецификация интерфейсов с сетевым уровнем и подуровнем управления доступом к передающей среде.

IEEE 802.3 – локальные сети с методом доступа CSMA/CD

IEEE 802.4 – локальные сети с маркерным доступом и топологией шина (Token Bus).

IEEE 802.5 – локальные сети с топологией кольцо и маркерным доступом (Token Ring).

IEEE 802.6 – городские локальные сети (площадь с радиусом до 25 км; передача данных, речи, изображений).

IEEE 802.7 – широкополосные сети.

IEEE 802.8 – оптоволоконные технологии**.**

IEEE 802.9 – интегрированные сети с возможностью передачи речи и данных.

IEEE 802.10 – безопасность сетей.

IEEE 802.11 – беспроводные технологии (Wireless Local Area Network; 802.11b – WiFi)**.**

IEEE 802.12 – локальные сети с централизованным управлением доступом по приоритетам запросов и топологией «звезда» (100VC-AnyLAN).

IEEE 802.13 – обработка запросов по приоритетам,

IEEE 802.14 – кабельное телевидение**,**

IEEE 802.15 – беспроводные локальные сети учреждений и предприятий (Wireless Personal Area Network; 802.15.1 – Bluetooth, 802.15.4 – ZigBee);,

IEEE 802.16 – доступ в беспроводные широкополосные сети (Wireless Broadband Access; WiMax),

IEEE 802.17 – высокоскоростная технология динамической передачи IP-пакетов (новое поколение городских сетей).

IEEE 802.20 – беспроводной мобильный широкополосный доступ (Mobile Broadband Wireless Access; Wireless USB);

(Mobile Broadband Wireless Access, MBWA).

IEEE 802.21 – эстафетная передача радиосоединений (Media Independent Handover).

IEEE 802.22 – беспроводные региональные сети (Wireless Regional Area

Network).

Стандарты серии IEEE 802, определяющие терминологию, архитектуру и протоколы локальных сетей двух нижних уровней модели OSI, имеют определенную специфику, обусловленную особенностями этих сетей. Основное отличие, см. рис. 3.3, состоит в том, что канальный уровень разбит на два подуровня: подуровень управления логическим каналом (ПУЛК; LLC -- Logical Link Control) и подуровень управления доступом к среде (ПУДС; MAC -- Media Access Control). При этом вышележащие уровни не

специфицируются. Это объясняется тем, что физический и канальный уровни по существу и определяют локальную сеть.

Такая декомпозиция канального уровня на два подуровня обусловлена спецификой реальных локальных сетей, которые могут различаться топологией (шина, звезда, кольцо), разделяемой средой передачи данных (коаксиальный кабель, витая пара, волоконно-оптический кабель) и методами доступа к этой среде. Стандарты подуровня управления доступом к среде (ПУДС) именно и ориентирован на учет этой специфики, в то время как стандарт 802.2, специфицирующий подуровень управления логическим каналом (ПУЛК) является общим

Рис. 3.3. Взаимосвязь уровней модели OSI и модели IEEE 802

Примерами протоколов ПУДС для реальных локальных сетей являются протоколы Ethernet, Token Ring, Fast Ethernet, 100VG-AnyLAN, FDDI.

В глобальных сетях, которым не свойственна регулярная топология, канальный уровень осуществляет информационный обмен между двумя абонентами по индивидуальным каналам с использованием протоколов типа "точка-точка". К таким протоколам относятся протоколы: PPP, SLIP, LAP-B, LAP-D. Эти протоколы, не используя ПУДС, реализуют процедуры управления потоком кадров.

3.3. Стандарт IEEE 802.2

Стандарт IEEE-802.2 специфицирует:

1. Интерфейс с сетевым уровнем, определяющий услуги, предоставляемые протоколом канального уровня протоколу верхнего уровня.

2. Протокол подуровня управления логическим каналом (**ПУЛК; LLC**), определяющий сквозные процедуры передачи данных.

3. Интерфейс с подуровнем управления доступом к среде (**ПУДС; MAC**), описывающий требуемые от данного уровня услуги по передаче информации.

Протокол ПУЛК описывает виды услуг, функции канального уровня, структуру и коды кадров данного уровня. К сервису на канальном уровне относятся различные виды индикации, запросы и ответы о вводе-выводе данных.

В стандарте определены два типа протокольных процедур обмена:

1. Процедура обмена **без установления логического соединения**, предоставляющая минимальный набор услуг по передаче информации (обеспечивает дейтаграммный режим передачи данных).
2. Процедура обмена **с предварительным установлением логического соединения** в виде виртуального канала (аналогична протоколу HDLC канального уровня глобальных сетей).

Процедуры обмена службы канального уровня регламентированы примитивами. Все примитивы имеют одинаковую структуру обозначений: на первом месте указывается принадлежность примитива к тому или иному уровню модели OSI, на втором, через дефис, -- название примитива; на третьем, через точку, указывается тип примитива. Например, примитив «**К-СОЕДИНЕНИЕ. Ответ»** относится к канальному уровню и «Указывает на согласие получателя установить соединение».

Процедура обмена **без установления логического соединения** предусматривает только передачу и прием пакетов без уведомления получателя об их доставке и осуществляется с помощью двух примитивов:

"К-ДАННЫЕ. запрос" (для передачи пакета канальному уровню с целью выдачи в среду).

"К-ДАННЫЕ. индикация" (указывает верхнему уровню на прием канальным уровнем кадра из среды).

Процедура обмена с предварительным установлением логического соединения предусматривает следующие услуги:

установление соединения,
передачу данных,
разъединение соединения,
сброс соединения.

Последняя услуга используется при возникновении ошибок, не устранимых на ПУЛК.

Процедура обмена с предварительным установлением логического соединения специфицируются примитивами, которые приведены в табл. 3.1.

Таблица 3.1. Примитивы процедуры обмена с установлением логического соединения

Примитив	Назначение

К-СОЕДИНЕНИЕ. запрос	Запрашивает установление логического соединения
К-СОЕДИНЕНИЕ. индикация	Указывает, что отправитель желает установить соединение.
К-СОЕДИНЕНИЕ. ответ	Указывает на согласие получателя установить соединение.
К-СОЕДИНЕНИЕ. подтверждение	Указывает на успешное завершение соединения.
К-ДАННЫЕ. запрос	Запрашивает передачу данных по установленному логическому каналу.
К-ДАННЫЕ. индикация	Указывает на прием данных по установленному логическому каналу
К-РАЗЪЕДИНЕНИЕ. запрос	Сетевой уровень запрашивает немедленный разрыв логического канала.
К-РАЗЪЕДИНЕНИЕ. индикация	Сообщается о разрыве логического канала.
К-СБРОС. запрос	Запрашивается перевод логического канала в начальное состояние.
К-СБРОС. индикация	Уведомляется о приведении логического канала в начальное состояние.
К-СБРОС. ответ	Указывается на допустимость процедуры перевода в начальное состояние.
К-СБРОС. подтверждение	Информирует о завершении процедуры перевода в начальное состояние.
К-СОЕДИНЕНИЕ-УПРАВЛЕНИЕ. запрос	Обеспечивает управление потоком данных от канального к сетевому уровню.
К-**СОЕДИНЕНИЕ-УПРАВЛЕНИЕ. индикация**	Обеспечивает управление потоком данных от сетевого к канальному уровню.

Стандартом IEEE 802.2 определена структура и три типа протокольных кадров (блоков данных): **информационный, супервизорный** и **ненумерованный.**

Кадр (frame) -- единица данных (протокольный блок данных) канального уровня.

Формат кадров ПУЛК приведен на рис.3.4.

В восьмибитовом поле адреса точки доступа к службе получателя (ТДСП) младший бит (левый бит данного поля) определяет тип адресации:

«**0**» указывает на индивидуальный адрес,

«1» — на групповой адрес.

В первом случае адресуется одна, а во втором — несколько точек доступа. Остальные биты адреса определяют точку доступа к службе получателя.

В восьмибитовом поля адреса точки доступа к службе отправителя (ТДСО):

«**0**» (в младшем бите) -- команда,

«1» -- подтверждение.

Остальные биты поля определяют адрес точки доступа службы отправителя.

В поле «Управление» N(S) и N(R) определяют соответственно номер переданного и принятого блока данных. Эти номера используются для управления потоком в режиме "скользящего окна". Девятый бит поля управления используется для задания бита "запрос передачи/последний кадр".

В третьем и четвертом битах супервизорного кадра, а также в 3, 4, 6 - 8 битах ненумерованного кадра, в зависимости от выполняемой ими функции, содержатся управляющие коды **«команда/подтверждение».**

Рис. 3.4. Формат кадров ПУЛК (стандарт 802.2), где

N(S) – номер передаваемого блока;

N(R) – номер принимаемого блока;

P – бит запрос/ответ;

S – бит управляющего кода;

X – резервные биты;

M – бит модификатора;

N – ненулевое целое число;

ТДСП – поле адреса к точка доступа службы получателя;

ТДСО – поле адреса к точка доступа службы отправителя.

В супервизорном кадре SS может принимать следующие значения:

00 -- «Готов к приему» (RR), команда/подтверждение,

01 -- «Не готов к приему» (RNR), команда/подтверждение,
10 -- Переспрос» (REJ), команда/подтверждение.

В ненумерованном кадре MMMMM может принимать восемь значений (три команды, три подтверждения и две команды/подтверждения), например, MMMMM=00111 соответствует команде/подтверждению «Проверка» (TEST).

3.4. стандарт IEEE 802.3

Стандарт **IEEE 802.3** (ISO 8802.3, ECMA-80, -81, -82) определяет протоколы и услуги ПУДС и физического уровня локальной сети с шинной топологией. Используется метод доступа к среде: **CSMA/CD** – множественный доступ с контролем несущей и обнаружением конфликтов. Передача сигналов осуществляется с использованием манчестерского кода.

При манчестерском кодировании интервал передачи каждого бита делится пополам, при этом полярность второй половины сигнала всегда обратная полярности первой его половины. Первая половина битового сигнала «1» имеет отрицательную полярность (низкий уровень), а для сигнала «0» – положительную полярность (высокий уровень). Манчестерское кодирование обеспечивает самосинхронизацию и легко реализуется на практике.

Архитектура стандарта IEEE 802.3 приведена на рис 3.**5.**

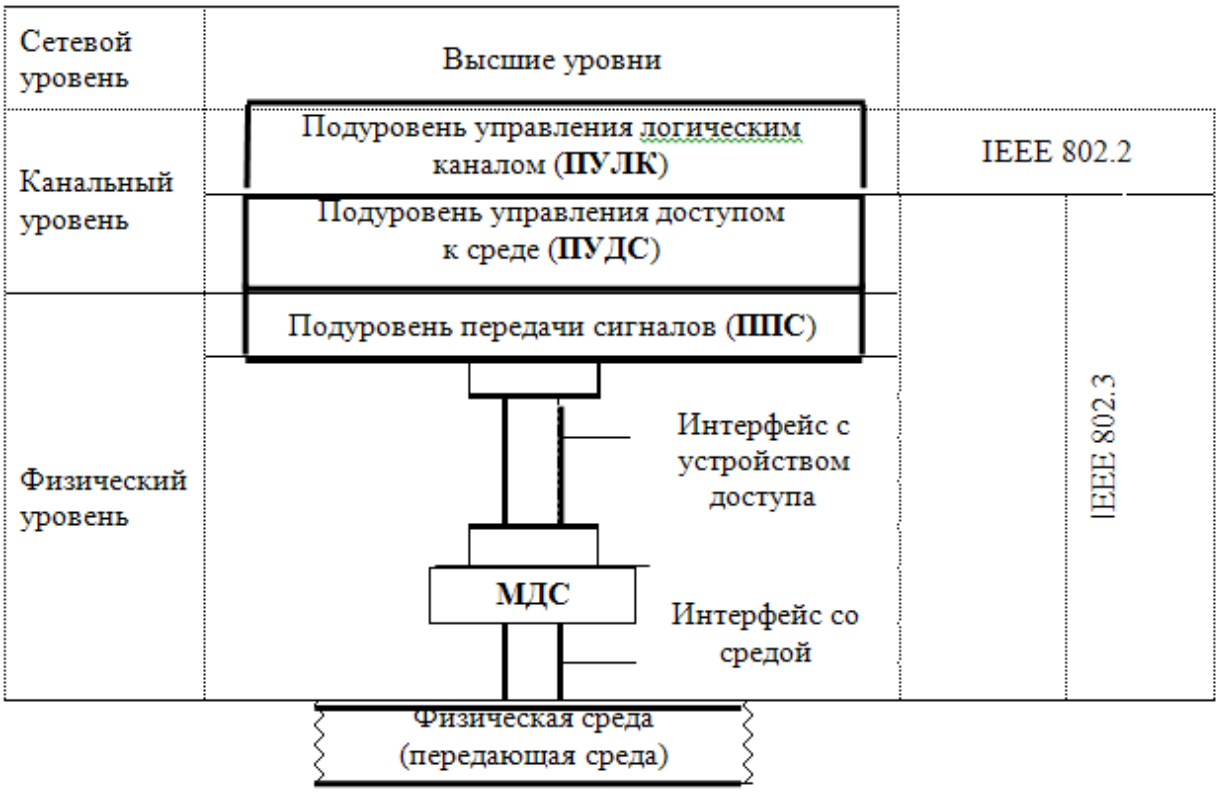

Рис.3.5. Архитектура стандарта IEEE 802.3

ПУЛК (LLC) специфицируется стандартом 802.2, который был рассмотрен в предыдущем подразделе.

ПУДС (MAC) реализует алгоритм доступа к среде и адресацию станций.

Подуровень передачи сигналов (ППС) является компонентом физического уровня. Он осуществляет кодирование сигналов, поступающих от ПУДС, и декодирование сигналов, принимаемых из среды для выдачи в ПУДС.

Интерфейс с устройством доступа (ИУД) представляет собой интерфейсный кабель, позволяющий размещать станцию на некотором удалении от физической среды.

Модуль доступа к среде (МДС) обеспечивает согласование сигналов, поступающих от ППС, с характеристиками физической среды.

Формат кадра ПУДС IEEE 802.3 приведен на рис. 3.6.

Преамбула используется для обеспечения синхронизации схем ППС с тактовыми сигналами, посылаемыми ПУДС. Разделитель начала кадров продолжает выполнять функции преамбулы и означает начало кадра.

Поля «адрес получателя» и «адрес отправителя» имеют длину 48 бит. Первый слева (младший) бит поля адреса получателя служит для различения индивидуального (0) и группового (1) адресов. При широковещательной адресации все биты поля адреса получателя устанавливаются в 1.

MAC-адрес записывается в шестнадцатеричном коде и имеет следующий формат: 02:60:8C:00:00:2F:C3. Префикс (первые три байта) — пул адресов, выданный изготовителю (например, пул 3COM начинается с 02:60:8C), остальные три байта являются уникальным номером, который присваивается карте ее изготовителем.

Длина (байт)

7	PR 10101010 ... Преамбула 10101010
1	SFD 10101011 Разделитель начала кадров
6	SA Адрес получателя (MAC-адрес получателя)
6	DA Адрес отправителя (MAC-адрес отправителя)
2	L Длина текстовой части
46…1500	Данные + заполнитель
4	FCS Контрольная последовательность кадра (КПК)

Рис. 3.6.Формат кадра ПУДС стандарта IEEE 802.3

Поле «длина текстовой части кадра» указывает на число байт в поле данных.

Поле «Данные + заполнитель» содержит передаваемые данные. Максимальная длина этого поля – 1500 байт, минимальная – 46 байт. Если число байт кадра меньше 46, то поле данных дополняется заполнителем до 46 байт. Это необходимо для обеспечения корректной работы механизма обнаружения конфликтов (коллизий). В это поле в соответствии со стандартом 802.2 должен вкладываться (инкапсулироваться) кадр ПУЛК названного стандарта.

В поле «контрольная последовательность кадра» (FCS) содержится контрольная последовательность, сформированная по полям DA, SA, L, «Данные + заполнители» циклическим кодом со стандартным полиномом 32-й степени (полином CRC-32). Получив кадр, станция получатель выполняет по тем же полям полученного кадра аналогичную процедуру и, сравнивая результат со значением поля FCS, принимает решение по данному кадру (при совпадении результатов кадр считается неискаженным).

Технологию Ethernet отличает не только популярность (85% локальных сетей используют эту технологию), но и большое разнообразие форм, в которых не трудно запутаться. В этой связи остановимся на основных модификациях кадра ПУДС стандарта IEEE 802.3.

Если в кадре ПУДС отсутствует вложенный кадр ПУЛК стандарта IEEE 802.2, то такой кадр называют кадром **Raw 802.3** ("грубый" вариант 802.3) или же **кадром Novell 802.3** (этот кадр не соответствует стандарту IEEE 802.2). Компания Novell использовала кадр **Novell 802.3** в своих сетевых операционных системах до версии NetWare 3.11 включительно. Это было оправдано, так как всегда использовался пакет протокола IPX, и не было необходимости идентифицировать тип информации, вложенной в поле данных. Начиная с версии NetWare 3.12, кадр ПУДС включает стандарт 802.2, и компания Novell стала обозначать его в своих операционных системах как **кадр** Novell **802.2** (это, как ни странно то же, что и **кадр стандарта 802.3**). Начиная с версии NetWare 5, стандартным протоколом по умолчанию становится протокол IP, который пришел на смену IPX.

Кадр Ethernet SNAP (SNAP - Sub Network Access Protocol, протокол доступа к подсетям). Кадр Ethernet SNAP определен в стандарте 802.2H и представляет собой расширение кадра 802.3 путем введения дополнительного поля идентификатора организации, которое может использоваться для ограничения доступа к сети сторонних пользователей. Кадр Ethernet SNAP содержит поле типа протокола верхнего уровня, аналогичное полю Type кадра Ethernet II.

Кадр стандарта Ethernet II представляет собой незначительно модифицированный изначальный тип кадра технологии Ethernet. Отличается от кадра Raw 802.3 в основном тем, что на месте поля длины в нем определено поле типа протокола (Type), которое предназначено по существу для тех же целей, что и поля ТДСП (точка доступа службы получателя) и ТДСО (точка доступа службы отправителя) кадра ПУЛК стандарта IEEE 802.2.

Различия в форматах кадров технологии Ethernet, ранее приводившее к несовместимости аппаратуры ныне потеряли свою остроту, поскольку большинство сетевых адаптеров, мостов и маршрутизаторов поддерживают все используемые на практике форматы кадров технологии Ethernet (возможные проблемы легко решаются путем настройки или замены драйверов сетевых карт).

3.5. Стандарт IEEE 802.5

Стандарт IEEE 802.5 (ISO 8802.5, ECMA-89) определяет протоколы и услуги подуровня доступа к среде и физического уровня локальной сети с кольцевой топологией (физической или логической) и методом доступа Token Ring.

В данном стандарте различают три основных типа кадров: данных, маркера и прерывания. Кроме названных кадров, различают также кадры: требование маркера, тест на дублирование адреса, кадр активного монитора, сигнальный кадр, кадр очистки.

Формат кадра данных ПУДС стандарта IEEE 802.5 приведен на рис. 3.7.

Заголовок кадра	1	SD Разделитель начала кадров VV0VV000	V – символ кодирования не манчестерским кодом
	1	AC Поле управления доступом PPPTMRRR	
	1	FC Поле управления кадра FFZZZZZZ	
	2 или 6	DA Адрес получателя	
	2 или 6	SA Адрес отправителя	
Любая длина, кратная байту		Данные	с учетом ограничения тайм-аута удержания маркера
Концевик кадра	4	FCS Контрольная последовательность кадров	То же, что в 802.3
	1	ED Разделитель конца кадров VV1VVIE	
	1	FS Поле статуса кадров AC00AC00	

Рис. 3.7.Формат кадра данных ПУДС стандарта IEEE 802.5.

Рассмотрим спецификацию битовых полей AC, FC, ED и FS.

Спецификация битов PPPTMRRR поля AC:

PPP – биты приоритета (8 значений, 111—высший приоритет, 000—низший);

T – бит маркера (если T = 0, то маркер, если T = 1, то передаются данные);

M – бит монитора (устанавливается в 1 после первого обращения кадра по каналу);

RRR – биты резервирования приоритета, используются для предварительного запроса требуемой приоритетности.

Спецификация битов FFZZZZZZ поля FC:

Для кадра ПУЛК FF = 01, а ZZZZZZ рассматривается как RRRYYY, где RRR – зарезервировано для будущих применений и при передаче принимает значение 000, YYY используются для переноса приоритетности.

Для кадра ПУДС FF = 00, а YYY может принимать шесть следующих значений:

011 – требование маркера;
000 – тест на дублирование адреса;
101 – кадр активного монитора;
110 – кадр неактивного монитора;
010 – сигнальный кадр;
100 – кадр очистки.

Спецификация битов VV1VVIE поля ED:

I – бит промежуточного кадра. = 1 – продолжение передачи следует,
I = 0 – последний кадр;
E – бит ошибки. E = 0 – ошибки нет, E = 1 – ошибка в кадре

Спецификация битов AC00AC00 поля FS:

A – бит опознавания адреса, устанавливается в 1 станцией, опознавшей собственный адрес, C – бит копирования кадра, устанавливается в 1 станцией, скопировавшей кадр.

Поля адрес получателя и адрес отправителя имеют одинаковую структуру и могут состоять из двух или шести байт каждый. Двухбайтный адрес имеет следующую структуру.

A	Номер кольца	Адрес Станции
Число бит 1	7	8

Здесь бит **A** = 0 указывает на индивидуальный адрес, **A** = 1 — групповой.

Шестибайтный адрес имеет следующую структуру.

A	У	Номер кольца	Адрес Станции
Число бит 1	1	14	32

В 48 разрядном адресе дополнительно вводится разряд указателя (**У**) способа назначения адресов. Значение **У** = О определяет универсальный способ назначения адресов, при **У** = 1 назначение адресов осуществляется локально в рамках каждой подсети.

Формат кадра маркера ПУДС стандарта IEEE 802.5 приведен на рис. 3.8, формат кадра прерывания имеет аналогичный вид.

SD	AC	ED

Рис. 3.8.Формат кадра маркера ПУДС стандарта IEEE 802.5.

Функционирование кольца согласно стандарту IEEE 802.5. осуществляется с использованием следующих процессов: процесса определения соседних станций, процесса управления кадрами и маркером, процесса очистки кольца, процесса за право быть активным монитором, процесса сигнализации о неисправностях, процесса подключения новой станции.

3.6. Сетевые протоколы локальных сетей

3.6.1. Назначение и особенности сетевых протоколов

Сетевые протоколы обеспечивают соответствие аппаратных и сетевых адресов, маршрутизацию и передачу данных, позволяя приложениям обмениваться данными по различным каналам вне зависимости от используемых канальных протоколов, форматов пакетов данных или аппаратных спецификаций.

В локальных сетях в основном находят (находили) применение сетевые протоколы следующих стеков: TCP/IP, Novell NetWare (IPX/SPX), Apple Talk, а также сетевые протоколы корпорации Microsoft.

Лидером сетевых технологий является стек TCP/IP. Его поддерживают все современные операционные системы. Вместе с этим в корпоративных сетях в ряде используется несколько стеков протоколов.

Протоколы стека IPX/SPX разработаны компанией Novell при создании операционной системы NetWare (использались в NetWare 4.x и в более ранних версиях), Сетевые ОС фирмы Novell отличались высокой производительностью и надежностью; доминировали на рынке сетевых ОС до конца 90-х годов прошлого века. Популярность Internet заставил компанию Novell обеспечить поддержку IP в NetWare. Вначале путем туннелирования (при этом сохранялась возможность использования IPX/SPX), а затем, начиная с NetWare 5, и в чистом виде. В NetWare 5 протокол IP является стандартным протоколом по умолчанию. При этом осталась возможность использования «чистого» IP, комбинации протоколов IP и IPX или «чистого» IPX. Достижения микропроцессорной техники практически нивелировали основные достоинства сетевых ОС фирмы Novell, а успехи сетевых технологий Microsoft привели к потере позиций фирмы Novell.

AppleTalk — это стек протоколов, разработанный компанией Apple Competers для одноранговых сетей. AppleTalk поддерживает следующие сетевые архитектуры:

LocalTalk — встроенная технология старых моделей Macintosh (не требует использования сетевых карт).

EtherTalk — реализация Ethernet для компьютеров Apple.

EtherTalk Phase 1 основывается на версии Ethernet II.

EtherTalk Phase 2 основывается на стандарте Ethernet 802.3 (поддерживается аппаратно в новых моделях Macintosh, вместо LocalTalk).

TokenTalk — реализация технологии Token Ring для компьютеров компании Apple.

FDDITalk — реализация архитектуры FDDI для компьютеров компании Apple.

3.6.2. Сетевые протоколы корпорации Microsoft

NetBEUI (NetBIOS Enhanced User Interface). Базовый сетевой протокол сетей Майкрософт. Используется в небольших локальных сетях от 1 до 200 клиентов. Необходим клиентам удаленного доступа Windows NT 3.1, LAN Manager, MS-DOS и Windows for Workgroups. Этот протокол является реализацией стандарта NetBIOS.

NetBIOS (Network Basic Input/Output System) предоставляет программам единый набор команд для запросов к службам нижнего уровня, которые требуются для управления именами, проведения сеансов и передачи данных между узлами сети.

NWLink — стандартный сетевой протокол, поддерживающий маршрутизацию и способный поддерживать приложения клиент-сервер NetWare.

3.6.3. Семейство протоколов NetWare IPX/SPX

Стек протоколов NetWare обычно называют по имени двух патентованных протоколов IPX и SPX.

Протокол IPX — протокол межсетевой передачи пакетов. Этот протокол предоставляет возможность программам, запущенным на рабочих станциях, обмениваться пакетами данных на уровне дейтаграмм (без подтверждений).Большинство задач в сети можно решать на уровне дейтаграмм. Использование протокола IPX обеспечивает наиболее быструю передачу данных при наиболее экономном использовании памяти. IPX выполняет динамический выбор маршрута с помощью протокола маршрутизации RIP, который является заданным в NetWare по умолчанию.

Протокол SPX — протокол последовательного обмена пакетами, реализован на базе протокола IPX и регламентирует сетевой и транспортные уровни локальной сети (обеспечивает гарантированную доставку пакетов в правильной последовательности).

Формат пакета IPX приведен на рис. 3.9., на котором приведены названия полей, их размеры в байтах, а также необходимые комментарии.

Пакеты могут рассылаться широковещательно, для этого поле **тип пакета** должно принять значение 0x14, адрес сети назначения должен соответствовать локальной сети, адрес узла назначения при этом принимает значение 0xFFFFFF.

Байты	**Поле заголовка**	**Назначение поля, способ формирования, комментарии**

2	Контрольная сумма	Формируется драйвером сетевого адаптера
2	Общая длина пакета	Может принимать значения от 30 до 576, если 30, то пакет состоит только из заголовка. Такой тип может использоваться программой для подтверждения приема. Формируется IPX.
1	Счетчик пройденных мостов	Перед передачей пакета устанавливается программным модулем IPX в нуль, при прохождении моста значение счетчика увеличивается на 1.
1	Тип пакета	Для IPX устанавливается значение 4, для SPX – 5. Устанавливается программно.
4	Номер сети получателя пакета	Номер сети, в которую передается пакет.
6	Адрес станции получателя	Адрес принимающей станции
2	Сокет программы получателя	Идентификатор программы на рабочей станции, которая должна принять пакет.
4	Номер сети отправителя пакета	Номер сети, из которой посылается пакет.
6	Адрес станции отправителя	Адрес передающей станции.
2	Сокет программы отправителя	Сокет программы, передающей пакет.
0-546	Данные	Передаваемые данные

Рис. 3.9. Формат пакета IPX.

Сокет (socket) идентификатор программы на рабочей станции. Распределение сокетов в сети Novell NetWare следующее: сокеты от 0 до 4000h зарезервированы и не должны использоваться в программном обеспечении пользователя; от 4000h до 8000h распределяется динамически, свыше 8000h распределяется фирмой Novell персонально - разработчиком программного обеспечения сетей.

Пакет, передаваемый при помощи **протокола SPX**, имеет более длинный заголовок. Дополнительно к 30 байтам стандартного заголовка пакета IPX добавляется еще 12 байт. Формат заголовка пакета SPX приведен на рис. 3.10.

Байты	Поле заголовка	Назначение поля, способ формирования, комментарии
30	Заголовок пакета IPX (30 байт)	
1	Управление потоком данных	Однобитовые флаги, управляющие передачей данных (0001000 – используется для сигнализации об окончании передачи данных; 00100000 – игнорируется драйвером SPX и передается в неизменном виде; 01000000 – используется драйвером SPX; 10000000 – устанавливается драйвером SPX при передаче системных пакетов; 00000001 … 00001000 – зарезервированы для дальнейшего использования)
1	Тип данных в пакете	Флаги, используемые для классификации данных: 11111110 – завершить связь и закрыть канал (при посылке драйвером SPX последнего пакета); 11111111 – подтверждение завершения связи (пакет является системным, и не передается в программу пользователя); 00000000 … 11111101 – игнорируются драйвером SPX и могут использоваться программой произвольным образом
2	Идентификатор канала отправителя	Содержит номер канала связи передающей программы, присвоенный драйвером SPX при создании канала связи.
2	Идентификатор канала получателя	Содержит номер канала связи принимающей стороны
2	Счетчик переданных пакетов	Счетчик пакетов, переданных по каналу в одном направлении (при достижении FFFF сбрасывается в нуль с возобновлением процесса счета)

2	Номер следующего пакета	Содержит номер следующего пакета, который должен быть принят драйвером SPX.
2	Количество буферов для приема	Содержит количество буферов для приема пакетов. Содержимым этого поля управляет драйвер SPX.

Рис. 3.10. Формат заголовка пакета SPX.

3.6.3. Понятие сетевого адреса

Номер сети, адрес станции и сокет составляют **сетевой адрес.** Например, **сеть: 0034**, станция: **02:60:8C:00:2F:C5**, сокет: **4545.** Номер сети определяется системным администратором при установке Novell NetWare.

Сокет используется для адресации конкретной программы, работающей на станции. На рабочей станции в сети одновременно могут быть запущены несколько программ, поэтому для того, чтобы послать данные конкретной программе, каждая программа, желающая принимать или передавать данные по сети, должна получить свой, уникальный идентификатор (сокет).

Следует заметить, что в IP-сетях под сокетом понимается совокупность IP-адреса и номер порта.

Тема 4. Стандарты, протоколы и программные средства глобальных сетей

4.1. Сетевой интерфейс стека TCP/IP

4.1.1. Особенности сетевого интерфейса стека TCP/IP

Особенностью межсетевых взаимодействий в IP-сетях является использование транспортных сетей (магистральных, городских, сетей доступа), содержащих различные средства коммутации. При этом информационный обмен между двумя абонентами (в отличие от локальных сетей) осуществляется по индивидуальным каналам с использованием протоколов типа "точка-точка" (PPP, SLIP, LAP-B, LAP-D), которые реализуют процедуры управления потоком кадров с учетом специфики средств коммутации. Разнообразие средств и способов коммутации предполагает их классификацию.

4.1.2. Классификация способов коммутации

Упрощенная классификация способов коммутации приведена на рис. 4.1.

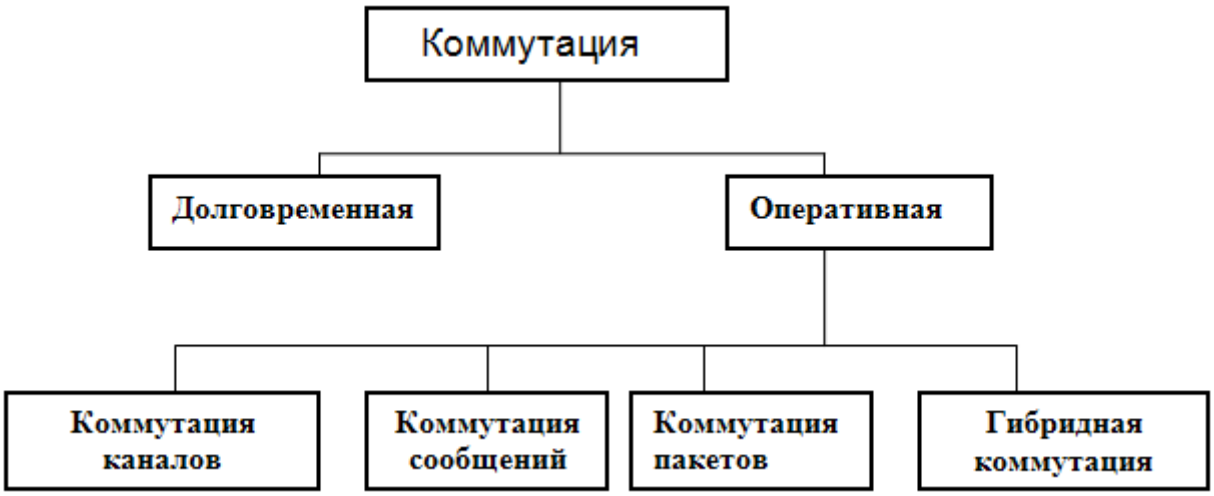

Рис.4.1. Классификация способов коммутации**.**

Долговременная (кроссовая) коммутация — это такой способ коммутации, при которой между двумя точками сети устанавливается постоянное, прямое соединение, длительность которого может измеряться часами, сутками или большими интервалами времени. Каналы, участвующие в таких соединениях, называются выделенными.

Оперативная коммутация подразделяется на следующие основные виды:

коммутация каналов,
коммутация сообщений,
коммутация пакетов,
гибридная коммутация.

При **коммутации каналов** обеспечивается прямое временное физическое соединение каналов сети между любой парой оконечных пунктов этой сети.

Коммутация каналов передачи данных — это такая коммутация, при которой обеспечивается соединение каналов вторичной сети электросвязи для образования канала передачи данных. ГОСТ 17657-79.

При **коммутации сообщений** в центре коммутации производится прием, запоминание и последующая передача полных сообщений в соответствии с адресом (**СТ ИСО 2382/9-84**).

При **коммутации пакетов,** представленное в виде адресованных пакетов сообщение, передается таким образом, что после передачи очередного пакета канал передачи данных освобождается для передачи других пакетов (**СТ ИСО 2382/9-84**).

При этом возможны два способа передачи: способ**,** основанный на организации **виртуального канала** (на время передачи сообщения), и **дейтаграммный** способ в противном случае.

Виртуальный (логический) канал — это такая форма передачи данных по сети, при которой у взаимодействующих абонентских систем возникает иллюзия наличия между ними прямого канала. Такой способ передачи данных в глобальных сетях обеспечивает протокол TCP, а в локальных сетях, например, протокол SPX. Дейтаграммный способ передачи характерен для протоколов IP, UDP в глобальных сетях и IPX — в локальных сетях.

При гибридной коммутации в одном и том же центре коммутации одна часть сообщений обслуживается в режиме коммутации каналов, а вторая часть - в режиме коммутации пакетов или коммутации сообщений.

4.1.3. Протокол SLIP

Протокол SLIP (Serial Line Internet Protocol) -- протокол для обмена данными по выделенным или коммутируемым каналам связи с использованием IP – сервиса. Этот протокол позволяет подключиться к TCP/IP по телефону с использованием модема через последовательный порт персонального компьютера. Он широко использовался ранее, поддерживается и теперь. SLIP не обеспечивает установление соединения через несколько узлов и не поддерживает адресацию, принятую в Internet. . В отличии от Ethernet, SLIP не "заворачивает" IP-пакет в свою обертку, а "нарезает" его на "куски".

4.1.4. Протокол PPP

Протокол PPP (Point to Point Protocol) -- соединение типа "точка - точка". Имеет то же назначение, что и SLIP (управление передачей данных по выделенным или коммутируемым линиям связи), но это более поздний и совершенный протокол.

Согласно RFC-1661, PPP обеспечивает стандартный метод взаимодействия двух узлов сети (обеспечивается двунаправленная

одновременная передача данных). Как и в SLIP, данные "нарезаются" на фрагменты, которые называются пакетами. Пакеты передаются от узла к узлу упорядоченно. В отличие от SLIP, PPP позволяет одновременно передавать по каналу связи пакеты различных протоколов. Кроме того, PPP предполагает процесс автоконфигурации обеих взаимодействующих сторон.

PPP состоит из трех частей: механизма инкапсуляции (encapsulation), протокола управления соединением (link control protocol) и семейства протоколов управления сетью (network control protocols).

М**еханизм инкапсуляции** PPP обеспечивает передачу пакетов различных протоколов по одному каналу путем упаковки одного протокола в формат другого протокола (вышележащий пакет вкладывается в поле данных нижележащего протокола). П**ротокол управления соединением** используется для установления, поддержки и завершения связи, а для работы с протоколами сетевого уровня. PPP содержит набор **протоколов управления сетью.** Более детально с протоколом PPP можно познакомиться в RFC-1661 и RFC-1548.

4.1.5. Протокол PPTP

В 1998 г. была создана расширенная версия PPP протокол PPTP (Point to Point Tunneling Protocol). Этот протокол предназначен для обеспечения защищенного удаленного доступа через Internet (превращает обычный телефонный вызов в защищенный канал связи между двумя компьютерами частной сети). PPTP поддерживает такие средства, как сжатие, шифрование и аутентификация (распознавание пользователя).

4.1.6. Методы согласования протоколов

При согласовании различных протоколов могут использоваться методы **инкапсуляции, трансляции и мультиплексирования**.

Инкапсуляция — это метод упаковки одного протокола в формат другого протокола (вышележащий пакет вкладывается в поле данных нижележащего). В традиционном понимании термин "инкапсуляция" означает образование капсулы вокруг чужих для организма веществ (инородных тел, паразитов и т.д.). В рамках межсетевого обмена понятие инкапсуляции имеет расширенное толкование. Это не только инкапсуляция в традиционном понимании (например, пакета IP в Ethernet-фрейм), но и наряду с добавлением служебной информации еще и, если это необходимо, разбиение пакета на более мелкие фрагменты обмена через один канал.

Инкапсуляция может быть использована для транспортных протоколов любого уровня. Например, протокол сетевого уровня X.25 может быть инкапсулирован в протокол транспортного уровня TCP, или же протокол сетевого уровня IP может быть инкапсулирован в протокол сетевого уровня X.25. Для согласования сетей на сетевом уровне могут быть использованы многопротокольные и инкапсулирующие маршрутизаторы, а также программные и аппаратные шлюзы.

Обычно инкапсуляция приводит к более простым и быстрым решениям по сравнению с трансляцией, так как решает более частную задачу, не обеспечивая взаимодействия с узлами транзитной сети.

Трансляция обеспечивает согласование двух протоколов путем преобразования (трансляции) сообщений, поступающих от одной сети, в формат другой сети. Транслирующий элемент, в качестве которого могут выступать, например, программный или аппаратный шлюз, мост, коммутатор или маршрутизатор, размещается между взаимодействующими сетями и служит посредником в их диалоге.

Мультиплексирование. Другим подходом к согласованию коммуникационных протоколов является технология мультиплексирования. Этот подход состоит в установке нескольких дополнительных стеков протоколов на одной из конечных машин, участвующих во взаимодействии. Компьютер с несколькими стеками протоколов использует для взаимодействия с другим компьютером тот стек, который понимает этот компьютер.

4.2. Межсетевой обмен в сетях TCP/IP

4.2.1. Особенности межсетевых взаимодействий в сетях TCP/IP

Уровень межсетевого обмена (3 уровень стека TCP/IP, уровень Internet) является базовым в архитектуре стека TCP/IP (Transmission Control Protocol/Internet Protocol). При этом протокол IP играет центральную роль не только на этом уровне, но в семействе протоколов TCP/IP в целом.

Особенность протокола IP, который относится к сетевому уровню модели OS/, состоит в том, что он позволяет создать единую логическую сеть путем реализации протокола IP во всех узлах и шлюзах сложной физической сети. Такая сеть может состоять из соединенных шлюзами разнородных пакетных подсетей, работающих со своими специфическими протоколами.

Протокол IP специфицирован на передачу дейтаграмм (datagram) и связан со следующими функциями межсетевого обмена: передача данных в сеть и получение данных из сети; адресация, маршрутизация и фрагментация дейтаграмм.

К уровню межсетевого обмена относятся также протоколы:

ARP — протокол разрешения адресов, отображает межсетевые адреса в физические,

RARP — обратный протокол разрешения адресов, отображает физические адреса в интерсетевые,

ICMP — межсетевой протокол, обеспечивает передачу управляющих сообщений и сообщений об ошибках между хостами и шлюзами; этот протокол является расширением уровня IP.

К уровню межсетевого обмена относятся также протоколы маршрутизации RIP (Routing Information Protocol, RFC 1058, 1988 г), OSPF (Open Shortest Path First), EGP (Exterior Gateway Protocol, RFC 904, 1984 г.),

BGP (Border Gateway Protocol, RFC 1163). Протоколы RIP и OSPF являются внутренними (протоколы автономных систем). Протокол RIP — для малых локальных сетей, а сложный OSPF — для больших и очень больших сетей.

4.2.2. Протокол IP

Существует несколько версий протокола IP. Номера версий протокола IP приведены в RFC 1700. В настоящее время широко используется версия Ipv4 (RFC 791); протокол Ipv6, за которым будущее, применяется в высокоскоростных сетях. Находит также применение протокол Ipv5, который существует под названием потокового протокола Internet (Internet Stream Protocol, RFC 1819). Протокол Ipv5 работает параллельно, а не вместо Ipv4 и ориентирован на передачу в реальном времени мультимедийной информации (пакетные потоки цифрового аудио и видео, распределенная имитация процессов и распределенные игры).

Формат пакета протокола Ipv4 приведен на рис. 4 .2.

4 бита	Версия	Версия конкретного протокола IP. Протокол представлен для версии 4
4 бита	Длина заголовка	Число 32-хразрядных слов перед полем данных
1 байт	Тип услуги	Вид услуги, например, длительность допустимой задержки
2 байта	Длина	Общий размер данного IP – пакета без заголовка
2 байта	Идентификатор пакета	16-тиразрядный идентификатор пакета, формируемый в узле источника
3 бита	Флаг	Параметр, определяющий место дейтаграммы сообщений (первое, промежуточное, последнее)
13 бит	Смещение фрагмента	Положение данного пакета (или фрагмента) в исходном блоке данных
1 байт	Время жизни	Максимальное время в секундах, в течение которого данный пакет может существовать в сети. Каждое устройство, осуществляющее обработку данного пакета, уменьшает значение этого поля
1 байт	Протокол	Протокол более высокого уровня, определяющий формат поля данных

2 байта	Контрольная сумма	Результат анализа данных в заголовке, используемый для контроля на целостность. Вычисляется только по заголовкам.
4 байта	Адрес отправителя	Адрес узла-отправителя пакета
4 байта	Адрес получателя	Адрес узла-получателя пакета
Может иметь переменную длину	Опции	Параметры не регламентированы. Различные фирмы могут использовать это поле для собственных нужд
Переменная	Заполнитель	Биты, дополняющие заголовок таким образом, чтобы он укладывался в 32-хразрядное поле
Переменная до 65 535 байт	Поле данных	Конверт, в котором содержатся пакеты, представленные в формате протокола более высокого уровня

Рис. 4.2. Формат пакета Ipv4 протокола.

Данные заголовка позволяют определить сетевой интерфейс получателя (IP-адрес получателя) пакета и направить пакет либо на сетевой интерфейс данной сети, либо на соответствующий шлюз. При этом, если пакет слишком долго "гуляет" по сети, то очередной шлюз может уничтожить этот IP-пакет и отправить на машину-отправителя уведомление (ICMP-пакет) о том, что надо использовать другой шлюз. На этом принципе работает программа ping, которая используется для определения маршрутов прохождения пакетов по сети.

Зная протокол транспортного уровня, IP-модуль производит разинкапсуляцию информации своего пакета и направляет данные на модуль обслуживания соответствующего транспорта.

При обычной процедуре инкапсуляции IP-пакет помещается в поле данных кадра (фрейма) протокола канального уровня. Если же это невозможно, то пакет разбивается на более мелкие фрагменты. Для восстановления исходного IP-пакета, его «нарезанные» фрагменты должны содержать информацию об их местоположении в исходном IP-пакете. Для этой цели используется поле «флаг» (flags) и «смещение фрагмента» (fragmentation offset). В этих полях определяется, какая часть пакета получена в данном фрейме. Размер максимально возможного фрейма, который передается по сети, определяется величиной MTU (Maximum Transsion Unit).

4.2.3. Принципы построения IP-адресов

IP-адрес — это 4-байтовая цифровая последовательность (RFC791). Принято каждый байт этой последовательности записывать в виде десятичного числа. Например, 144.106.166.32

IP-адрес состоит из двух частей: адреса сети и номера хоста (обычно под хостом понимают компьютер, подключенный к сети). В настоящее время, понятие "хост" имеет более широкое толкование. Это может быть не только компьютер с сетевой картой, но и любое устройство, которое имеет свой сетевой интерфейс (например, принтер, робот, холодильник и т.д.).

Существует 5 классов IP-адресов. Эти классы отличаются друг от друга количеством битов, отведенных на адрес сети и адрес хоста в сети. На рис. 4.3 показаны эти пять классов.

Рис. 4.3. Классы IP-адресов

Используя данные, приведенные на рис. 4.3, нетрудно подсчитать количество сетей и узлов для каждого класса сетей.

Класс	Диапазон значений первого октета	Возможное количество сетей	Возможное количество узлов
A	1 - 126	126	16777214
B	128 - 191	16382	65534
C	192 - 223	2097150	254
D	224 - 239	-	228
E	240 - 247	-	227

Рис. 4.4. Характеристики классов IP-адресов

Адреса класса A предназначены для больших сетей общего пользования. В настоящее время эти адреса распределяются по специальной схеме, в которую включены провайдеры Internet-услуг. Распределение адресов осуществляется с использование протокола **CIDR.**

CIDR (Classless InterDomain Routing, **RFC 1517-1520**) — протокол бесклассовой (классы и номера сетей не используются*)* междоменной маршрутизации. Протокол CIDR используется в маршрутных таблицах

Internet (таблицах провайдеров**).** В клиентских сетях продолжает использоваться классовая адресация**.** Различают крупных провайдеров которые, предоставляют услуги другим провайдерам и отдельным лицам, и провайдеров, которые обеспечивают доступ в Internet отдельным лицам и бизнес предприятиям. Применение CIDR позволило предотвратить экспоненциальный рост маршрутных таблиц Internet.

Адреса класса B предназначены для использования в сетях среднего размера (сети больших компаний, научно-исследовательских институтов, университетов).

Адреса класса C предназначены для использования в сетях с небольшим числом компьютеров (сети небольших компаний и фирм).

Адреса класса D используют для обращения к группам компьютеров, а **адреса класса E** зарезервированы для проведения экспериментов.

Среди всех IP-адресов имеется зарезервированных под специальные нужды (см. Рис. 4.5).

IP-адрес	Значение
все нули	данный узел сети
номер сети | все нули	данная IP-сеть
все нули | номер узла	узел в данной (локальной) сети
все единицы	все узлы в данной локальной IP-сети
номер сети | все единицы	все узлы указанной IP-сети
127.0.0.1	"петля"

Рис. 4.5. Выделенные IP-адреса

Адрес 127.0.0.1 предназначен для тестирования программ и взаимодействия процессов в рамках одного компьютера. В большинстве случаев в файлах настройки этот адрес обязательно должен быть указан, иначе система при запуске может зависнуть. Наличие "петли" чрезвычайно удобно с точки зрения использования сетевых приложений в локальном режиме для их тестирования и при разработке интегрированных систем. Сеть класса A 127.0.0.0. реально не описывает ни одной настоящей сети. 127. любая последовательность предназначена для организации циклов. Рабочая станция посылает пакеты сама себе.

Существует адресное пространство, выделенное для частного применения (эти IP-адреса называются «серыми» и используются для внутренних целей). Вот эти IP-адреса (RFC 1918).

Одна сеть класса A: 10.0.0.0.

16 сетей класса B: 172.16.0.0…172.31.0.0.

256 класса C: 192.168.0.0…192.168.255.0.

Например, BSUIR использует два сегмента с адресами: 172.16.0.0, 172.17.0.0.

Реальные адреса выделяются организациями, предоставляющими IP-услуги, из выделенных для них пулов IP-адресов. Согласно документации NIC (Network Information Centre) IP-адреса предоставляются бесплатно, но в прейскурантах наших организаций (как коммерческих, так и некоммерческих), занимающихся Internet-сервисом предоставление IP-адреса стоит отдельной строкой.

4.2.4. Подсети. Маска подсети

IP-адрес имеет два иерархических уровня (рис.4.6). Дефицит номеров сетей и экспоненциальный ростом таблиц маршрутизации в Internet привели к необходимости введения третьего уровня иерархии — уровня подсетей. Уровень подсетей вводится путем деления области номера устройства на две части: номера подсети и номера устройства, см. рис.4.7.

Префикс сети	Номер устройства

Рис.4.6. Двухуровневая иерархия

Расширенный сетевой префикс

Префикс сети	Номер подсети	Номер устройства

Рис.4.6. Трехуровневая иерархия

Такой подход к IP-адресации снимает проблему роста таблиц маршрутизации, поскольку информация о топологии корпоративных сетей становится ненужной магистральным маршрутизаторам Internet. Разбиение сети на подсети проявляется только локально и не влияет на IP-адресацию. При этом задача различения отдельных подсетей возлагается на маршрутизаторы частной сети. Это позволяет администратору частной сети вносить любые изменения в логическую структуру сети, обусловленные расширением или реорганизацией сети.

Организация подсетей рассматривается в RFC 950. RFC 950 определяет стандартный способ использования подсетей в IP-адресе.

Для передачи трафика в организацию магистральные маршрутизаторы Internet используют сетевой префикс адреса получателя (номер сети), а передача трафика индивидуальным подсетям осуществляется маршрутизаторами организации с использованием расширенного сетевого префикса. (префикс сети и номер подсети).

Понятие расширенного сетевого префикса, по существу, эквивалентно понятию маска подсети (subnet mask). **Маска подсети** — это двоичное число, содержащее единицы в тех разрядах, которые относятся к расширенному сетевому префиксу. Это четыре байта, которые накладываются на IP-адрес для

получения номера подсети (логическое умножение битов маски на биты IP-адреса).

В целях уяснения понятия «маска подсети» приведем маски стандартных сетей:

Маска сети класса А 255.0.0.0.
Маска сети класса В 255.255.0.0.
Маска сети класса С 255.255.255.0.

В качестве примера рассмотрим процесс разбиения базовой сети класса С 192.168.02.0 на 4 подсети. Для получения 4 сетей необходимо использовать два старших бита последнего 4 байта. При этом маска подсети будет иметь вид 255.255.255.192. В двоичном коде эта маска имеет вид

11111111. 11111111. 11111111.11000000.

На сеть 192.168.02.0 /24 накладываем маску 255.255.255.192:
11000000. 10101000. 00000010.00000000
11111111. 11111111. 11111111.11000000.
В результате получаем следующие подсети:

Подсеть № 0	192.168.02.0	(00)	1 …62	62
Подсеть № 1	192.168.02.64	(01)	65…126	62
Подсеть № 2	192.168.02.128	(10)	129…190	62
Подсеть № 3	192.168.02.192	(11)	193…254	62

Запишем, к примеру, номера устройств в подсети № 1:

192.168.02.65, 192.168.02.66, 192.168.02.67 …192.168.02.126.

В заключение заметим, что первоначально RFC 950 запрещал использование подсетей, у которых все биты установлены в нули или в единицы, что было обусловлено несовершенством протокола маршрутизации RIP версии 1. Протоколы OSPF, IS-IS обеспечили возможность устранения названного запрета вопреки документу RFC 950.

4.2.5. Протокол IPv6

К 1994 году номера сетей класса В оказались практически выбранными. Остались только сети класса А и сети класса С. Возник острый дефицит адресного пространства Internet. В начале 1995 года IETF, после 3-х лет консультаций и дискуссий, выпустило предложения по новому стандарту протокола IP (RFC 1752 «The Recommendation for the IP Next Generation Protocol»), фиксирующее появление протокола IPv6, который часто называют IPing.

Попытки обойти адресные ограничения предпринимались и ранее. Например, протокол BOOTP (BOOTstrap Protocol) и более совершенный, основанный на BOOTP, протокол DHCP (Dynamic Host Configuration

Protocol) реализуют простой способ решения адресной проблемы на случай ограниченного числа физических подключений к Internet по коммутируемым телефонным каналам. IP-адреса динамически выдаются пользователям из ограниченного набора адресов, закрепленных за телефонным пулом.

Появление IPv6 обусловлено не только адресной проблемой (хотя она и основная). В IPv6 введены новые типы адресов, упрощен заголовок пакета, введена идентификация типа информационных потоков для увеличения эффективности обмена данными, введены поля идентификации и конфиденциальности информации. Последующая модификация IPv6 связана с необходимостью обеспечения качества услуг по доставке данных.

IPv6 не применяет концепцию классов IP-адресов, при этом он предоставляет такое количество адресов, которое обеспечит потребности в IP-адресах всех пользователей, включая и такие экзотических, как роботы, стиральные машины, холодильники, и т.п. Адресное пространство, IPv6, составляет .

Протокол IPv6 (RFC 1883, декабрь 1995 г.) является очередной версией IP. Заголовок IPv6-пакета приведен на рис. 4.8. Пакет имеет постоянную (статическую) длину, равную 40 байтам.

4 бита	Версия
4 бита	Приоритет
3 байта	Метка потока
2 байта	Длина
1 байт	Следующий заголовок
1 байт	Ограничение переходов
16 байт	Адрес отправителя
16 байт	Адрес получателя

Рис. 4.8. Формат заголовка IPv6 (RFC 1883).

В этом заголовке:

Поле "Версия" - номер версии IP, равное 6.

Поле "Приоритет", согласно RFC 1883, может принимать значения от 0 до 15, которые делятся на два диапазона.

Коды от 0 до 7 используются для задания приоритета трафика, связанного с контролем перегрузки (в ответ на сигнал перегрузки, TCP,

например, снижает поток). Для приложений рекомендуются следующие значений приоритета:

0 – не символьная информация;
1 – информация заполнения (например, сетевые новости),
2 – не критичная ко времени передача данных (e-mail);
3 – зарезервировано,
4 - передача данных режима on-line (FTP, HTTP и т.п.);
6 - интерактивный обмен данными (telnet, X);
7 - системные данные или управления сетью (SNMP, RIP и т.п.).

Значения от 8 до15 используются для приоритета трафика, для которого не производится снижения потока в ответ на сигнал перегрузки, например, в случае пакетов «реального времени», посылаемых с постоянной частотой. Чем больше код, тем выше приоритет данных и тем быстрее они должны быть доставлены. Для мультимедийной информации уровень приоритета должен лежать в диапазоне 8-15.

В RFC 2460 (декабрь 1998 г.) поле **Приоритет** заменено полем **Класс трафика** (см. рис.4.9). Изменены и размеры полей **Класс трафика** и **Метка потока.** Изменения продиктованы требованиями документа RFC 2474, ориентированного на решение задач управления **QoS (**Quality of Service). QoS — качество и класс предоставляемых услуг передачи данных.

QoS представляет собой набор стандартов (технологий), ориентированных на предоставление клиенту необходимого по качеству уровня услуг (пропускная способность, задержка отклика и т.д.), в условиях работы поверх сетей с самыми разнообразными технологиями.

Поле **Метка потока** (рис.4.9) используется для оптимизации маршрутизации пакетов. В IPv6 вводится понятие потока, который состоит из пакетов. Пакеты потока имеют одинаковый адрес отправителя и одинаковый адрес получателя, и ряд других одинаковых опций. Это поле позволяет маршрутизаторам обрабатывать и оптимизировать процедуру пересылки пакетов, принадлежащих одному потоку.

Поле **Длина** определяет длину следующей за заголовком части пакета в байтах.

Поле **Следующий заголовок** определяет тип заголовка, который следует непосредственно за IPv6 заголовком. Заголовки расширения IPv6, связанные с опционной информацией (маршрутизация, фрагментация, аутентификация, инкапсуляция) записываются в отдельных заголовках, которые помещаются между IPv6 заголовком и заголовком пакета верхнего уровня. IPv6 пакет может иметь нуль, один или более заголовков расширения, каждый задается предыдущим полем **Следующий заголовок.**

4 бита	Версия
8 бит	Класс трафика

20 бит	Метка потока
2 байта	Длина
1 байт	Следующий заголовок
1 байт	Ограничение переходов
16 байт	Адрес отправителя
16 байт	Адрес получателя

Рис. 4.9. Формат заголовка IPv6 (RFC 2460).

Поле **Ограничение переходов** определяет число промежуточных шлюзов, которые ретранслируют пакет в сети. При прохождении шлюза это число уменьшается на единицу. При достижении значения "0" пакет уничтожается.

Поля **Адрес отправителя** и **Адрес получателя** имеют длину 16 байт.

Спецификация IPv6 предусматривает три типа адресов.

Unicast (индивидуальный): Идентификатор одиночного интерфейса. Пакет, посланный по уникастному адресу, доставляется интерфейсу, указанному в адресе.

Anycast (выборочный): Идентификатор набора интерфейсов. Пакет, посланный по эникастному адресу доставляется одному из интерфейсов, указанному в адресе (ближайший в соответствии с мерой, определенной протоколом маршрутизации).

Multicast (групповой): Идентификатор набора интерфейсов. Пакет, посланный по мультикастному адресу доставляется всем интерфейсам, указанным в адресе. В IPv6 не существует широковещательных адресов, их функции переданы мультикаст-адресам.

Адреса IPv6 записываются в 16-ричном формате в виде 8 групп по 16 бит в каждой разделенных, как и в MAC-адресах двоеточиями: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx xxxx: xxxx.

Например: 3C10:0900:0002:0000:0000:0250:97FF:FE6C**.** При записи адресов возможны сокращения. Например, адрес:

FC14:1030:0000:0000:0000:0000:0000:0013

можно записать в виде **FC14:0:0:0:0:0:0:0013** или даже так: **FC14::0013**.

Символ «**::**» можно использовать только один раз. Сжимать можно только ведущие нули.

В IPv6 классовая адресация отсутствует, но лидирующие биты адреса содержат определенную информацию. Поле переменной длины, содержащее эти лидирующие биты, называется **префиксом формата** (FP, Format Prefix). Префиксы адресации Pv6 приведены в табл. 4.1.

Таблица 4.1. Префиксы адресации Pv6.

Назначение	**Префикс**
Зарезервировано	0000 0000
Не определено	0000 0001
Зарезервировано для NSAP	0000 001
Зарезервировано для IPX	0000 010
Не определено	0000 011
Не определено	0000 1
Не определено	0001
Не определено	001
Провайдерские уникаст-адреса	010
Не определено	011
Зарезервировано для географических уникаст-адресов	100
Не определено	101
Не определено	110
Не определено	1110

Не определено	1111 0
Не определено	1111 10
Не определено	1111 110
Не определено	1111 11100
Локальные канальные адреса	1111 1110 10
Локальные адреса (site)	1111 1110 11
Мультикаст-адреса	1111 1111

Здесь NSAP (Network Service Access Point) — адресация, предложенная в модели OSI. Если FP≠11111111, то это уникастный адрес; эникастные адреса берутся из уникастного пространства и синтаксически от них неотличимы.

В IPv6 вместо прежних двух уровней (номер сети и номер узла) используется пять уровней, которые включают двухуровневую идентификацию провайдеров и трехуровневую — абонентов сети:

010	Идентификатор провайдера	Идентификатор абонента	Идентификатор подсети	Идентификатор узла

Младшие 6 байт, содержащие идентификатор узла, представляют собой MAC-адрес сетевого адаптера, что обеспечивает возможность автоконфигурации стека.

В версии IPv6 не используется классовая адресация, вместо нее применяется бесклассовая технология CIDR (Classless Inter-Domain Routing). В этой технологии каждому провайдеру назначается непрерывный диапазон IP-адресов. При таком подходе все адреса сетей каждого провайдера имеют общий префикс, так что маршрутизация в Internet может осуществляться на основе префиксов, а не полных адресов конечных абонентов. Это позволяет уменьшить объем таблиц маршрутизаторов и повысить пропускную способность Internet. Деление IP-адреса на номер сети и номер узла в технологии CIDR осуществляется посредством маски переменной длины, назначаемой провайдером.

Протокол IPv6, который в сравнении с IP4 предъявляет значительно более высокие требования к маршрутизаторам и рабочим станциям, поддерживается практически всеми современными операционными системами и производителями

сетевого оборудования. В настоящее время осуществляется постепенный переход к протоколу IPv6. Существует объединенные между собой фрагменты сети Internet, в которых маршрутизаторы поддерживают обе версии IP. Эти фрагменты образуют так называемую «шестую» магистраль **(6Bone).** 6Bone использует технику инкапсуляции пакетов IPv6 при транзитной передаче через те части Internet,, которые еще не поддерживают IPv6. Понятие 6Bone в широком смысле охватывает как сеть 6Bone, запущенную в 1996 г., так и сети 6Ren, 6Net, DREN6 и др. На IPv6 работает и американская сеть Internet 2.

Переход на IPv6 может осуществляться либо путем туннелирования *(*инкапсуляции) Pv6 в дейтаграмму IP (RFC 1933), либо посредством использования двойных стеков (мультиплексировая). Двойные стеки позволяют узлу в сети IP поддерживать обе версии протокола. Такие узлы называются IPv6/IPv4-узлами.

RFC 1933 определяет четыре конфигурации туннелей между рабочими станциями и маршрутизаторами:

маршрутизатор -- маршрутизатор;

рабочая станция — маршрутизатор;

рабочие станции — маршрутизаторы;

маршрутизатор -- рабочая станция.

4.2.6. Протоколы ARP и RARP

Протокол **ARP** (*Address Resolution Protocol,* RFC 826*)* предназначен для установления соответствия между физическими адресами сетевых интерфейсов (Ethernet-адресов, MAC-адресов) и их IP-адресов. Это соответствие отображается в ARP-таблице (ARP-кэше хостов). ARP-таблица имеет следующий вид.

IP-адрес	Ethernet-адрес
223.1.2.1	08:00:39:00:2F:C3
223.1.2.3	08:00:5A:21:A7:22
223.1.2.4	08:00:10:99:AC:54

Физический адрес «зашит» в ПЗУ сетевой карты ее изготовителем и идентифицирует сетевой интерфейс на канальном уровне. Узел (хост) может иметь несколько сетевых интерфейсов, например маршрутизатор, в то время как IP-адрес интерфейса относится к сетевому уровню и может изменяться (например, распределяться динамически).

Размер адреса Ethernet - 6 байтов (технология Ethernet появилась на рынке в 1980 г.). Адрес записывается в шестнадцатеричном коде. Первые три байта называются префиксом и закреплены за производителем карты.

Каждому производителю карт выделен свой пул адресов, в рамках которого он может выпускать сетевые карты (см. табл. 4.2).

Таблица 4.2. Префиксы адресов производителей карт

Префикс	Производитель	Префикс	Производитель
00:00:0C	Cisco	08:00:0B	Unisys
00:00:0F	NeXT	08:00:10	T&T
00:00:10	Sytek8	08:00:11	Tektronix
00:00:1D	Cabletron	08:00:14	Exelan
00:00:65	Network General	08:00:1A	Data General
00:00:6B	MIPS	08:00:1B	Data General
00:00:77	Cayman System	08:00:1E	Sun
00:00:93	Proteon	08:00:20	CDC
00:00:A2	Wellfleet	08:00:2%	DEC
00:00:A7	NCD	08:00:2B	Bull
00:00:A9	Network Systems	08:00:38	Spider Systems
00:00:C0	Western Digital	08:00:46	Sony
00:00:C9	Emulex	08:00:47	Sequent
00:80:2D	Xylogics Annex	08:00:5A	IBM
00:AA:00	Intel	08:00:69	Silicon Graphics
Префикс	Производитель	Префикс	Производитель
00:DD:00	Ungermann-Bass	08:00:6E	Exelan
00:DD:01	Ungermann-Bass	08:00:86	Imageon/QMS
02:07:01	MICOM/Interlan	08:00:87	Xyplex terminal servers
02:60:8C	3Com	08:00:89	Kinetics
08:00:02	3Com(Bridge)	08:00:8B	Pyromid
08:00:03	ACC	08:00:90	Retix
08:00:05	Symbolics	AA:00:03	DEC
08:00:08	BBN	AA:00:04	DEC

Заполнение ARP-таблицы осуществляется автоматически с использованием ARP-пакета, который «вкладывается» в поле данных Ethernet-кадра. ARP-пакет содержит пять основных полей:

тип операции (ARP-запрос или ARP-ответ),

физический адрес отправителя,

IP-адрес отправителя,
физический адрес приемника,
IP-адрес приемника.

Посланный IP-адресату IP-пакет «ищет» физический адрес получателя пакета. Если требуемого адреса в ARP-таблице нет, то реализуется следующая схема:

1. По сети передается широковещательный ARP-запрос (FF:FF:FF:FF:FF:FF).
2. IP-пакет ставится в очередь.
3. Ethernet-адрес, содержащийся в возвратившемся ARP-ответе, заносится в ARP-таблицу.
4. По ARP-таблице определяется Ethernet-адрес поставленного в очередь IP-пакета.
5. IP-пакет инкапсулируется в Ethernet-кадр и передается по сети адресату.

На широковещательный ARP-запрос: "чей это IP-адрес?", ARP-пакет, основные поля которого содержат:

IP-адрес отправителя	223.1.2.1
Ethernet-адрес отправителя	08:00:39:00:2F:C3
Искомый IP-адрес	223.1.2.2
Искомый Ethernet-адрес	<пусто>

отвечает только владелец адреса (каждый хост имеет отдельную ARP-таблицу для каждого своего сетевого интерфейса). Ответ: «Да, это мой IP-адрес, сообщаю свой Ethernet-адрес» высылается в виде ARP-пакета с аналогичными полями:

IP-адрес отправителя	223.1.2.2
Ethernet-адрес отправителя	08:00:28:00:38:A9
Искомый IP-адрес	223.1.2.1
Искомый Ethernet-адрес	08:00:39:00:2F:C3

Ответ получает хост, пославший ARP-запрос. Драйвер хоста передает ARP-пакет модулю ARP, последний добавляет запись в свою ARP-таблицу.

Некоторые реализации ARP не ставят в очередь IP-пакеты на ожидание ARP-ответа, а просто уничтожают IP-пакет. Восстановление IP-пакета реализуется модулем TCP или прикладным процессом, если используется UDP. Повторная передача IP-пакета проходит успешно, так как первая попытка позволяет добавить необходимую запись в ARP-таблицу.

Если разрешить запрос не удается, то IP-пакет будет уничтожен. Модули прикладного уровня, при этом, не смогут отличить физического повреждения сети от ошибки адресации. Если целевой узел (адресат) находится вне данной локальной сети (в сети с другим номером), для ARP-запрос будет использован маршрутизатор (в этом случае ARP-запрос используется для определения физического адреса маршрутизатора). Пакеты ARP некогда не выходят за пределы локального сегмента сети.

Протокол **RARP** (Reverse Address Resolution Protocol**)** — обратный протокол определения адреса также использует формат ARP-пакета (единственное различие — это вопрос в поле IP-адреса, вместо MAC-адреса). Пакеты RARP так же, как и пакеты ARP не могут маршрутизироваться.

Протокол RARP потерял актуальность, так как существуют другие более мощные и совершенные протоколы, реализующие возможности RARP, как одну из функций. К таким протоколам относятся BOOTP (BOOTstrap Protocol) и DHCP **(**Dynamic Host Configuration Protocol**).** DHCP по существу является расширением BOOTP и используется для облегчения администрирования больших сетей. Основное назначение DHCP динамическое назначение IP-адресов.

4.2.7. Протокол ICMP

Протокол ICMP (Internet Control Message Protocol) — протокол межсетевых управляющих сообщений (RFC 792, обязательный стандарт). Используется для рассылки информационных и управляющих сообщений. ICMP-пакеты инкапсулируются в поле данных IP-дейтаграмм (признак ICMP-пакета — «1» в поле «Протокол» заголовка IP-пакета).

К наиболее часто используемым ICMP-сообщениям (из более чем 25 стандартных значений типов ICMP-сообщений) относятся следующие сообщения:

ICMP-сообщение	Описание
Эхо-запрос (Echo request)	Определяет, доступен ли в сети IP-узел (компьютер или маршрутизатор).
Эхо-ответ (Echo reply)	Отвечает на эхо-запрос ICMP.
Адресат недоступен (Destination unreachable)	Информирует узел о том, что дейтатаграмма не может быть доставлена.
Замедление источника (Source quench)	Требует от узла снизить скорость отправки дейтаграмм, так как в сети возник затор.
Перенаправление (Redirect)	Информирует узел о наличии лучшего маршрута.
Истечение времени (Time exceeded)	Сообщает, что время жизни IP-дейтаграммы (TTL) истекло.

Для отправки эхо-запросов ICMP можно использовать команду ping. Утилита traceroute позволяет проследить трассу IP-пакета.

ICMP используется и хакерами (сканирование диапазона IP-адресов, адреса выявляются посредством ping-пробы, затем сканирование открытых портов).

При посылке пакета через Internet traceroute устанавливает значение TTL (Time To Live) последовательно от 1 до 30. TTL определяет число шлюзов, через которые может пройти IP-пакет. Если это число превышено, то шлюз, на котором происходит обнуление TTL, высылает ICMP-пакет. Traceroute сначала устанавливает значение TTL равное единице - отвечает ближайший шлюз, затем значение TTL равно 2 - отвечает следующий шлюз и т. д. Если пакет достиг получателя, то в этом случае возвращается сообщение другого типа — Detecting unreachable destination, т.к. IP-пакет передается на транспортный уровень, а на нем нет обслуживания запросов traceroute.

4.3. Транспортный уровень TCP/IP

4.3.1. Протокол UDP

Протокол UDP (User Datagram Protocol; RFC 768; август 1980, состояние: стандарт, статус: рекомендуемый) является протоколом транспортного уровня стека протоколов TCP/IP. UDP является не ориентированной на соединение ненадежной транспортной службой, не отсылающей подтверждения отправителю после получения данных. Она не сохраняет порядок входящих пакетов, может потерять пакеты или их продублировать. Так что приложение, использующее протокол UDP должно само обеспечивать как о целостность данных, так контроль доставки данных адресату.

Протокол UDP обеспечивает прикладной программе передачу сообщений с минимальными издержками. Единицей данных протокола UDP является UDP-пакет, который инкапсулируются в IP-пакет.

UDP-пакет состоит из заголовка и поля данных, в котором размещается пакет прикладного уровня.

2 байта	Номер порта процесса-отправителя
2 байта	Номер порта процесса-получателя
2 байта	Длина пакета в байтах
2 байта	Контрольная Сумма

Рис. 4.10. Заголовок UDP-пакета.

Поля **Порт отправителя** и **Порт получателя** содержат 16-битные номера портов. Если ответ не требуется, то на месте адреса отправителя могут помещаться нули.

Поле **Длина** содержит число октетов, включая заголовок UDP и данные. Минимальное значение этого поля - восемь байт (только длина заголовка).

Поле **Контрольная сумма** предназначено для контроля целостности данных (вычисляется по заголовку и полю данных). От подсчета контрольной суммы можно и отказаться (в этом случае поле будет содержать нули). Однако следует иметь ввиду, что контрольная сумма UDP единственная гарантия целостности сохранения данных (протокол IP подсчитывает контрольную сумму только для заголовка IP-пакета, игнорируя поле данных).

Протокол UDP, получая данные от прикладной программы, добавляет к ним заголовок и передает сформированный UDP-пакет IP-уровню, на котором формируется IP-пакет. Далее, IP-пакет вкладывается в область данных кадра (фрейма) канального уровня и затем этот кадр передается по физической среде IP-адресату. На стороне адресата все происходит в обратном порядке. На транспортном уровне заголовок UDP-пакета отрезается, а данные пакета направляются на номер порта процесса получателя, указанного в заголовке этого UDP-пакета.

Размер поля Номер порта равен двум байтам, так что количество возможных портов составляет 2 = 65536. Различают присвоенные (зарезервированные), зарегистрированные и динамические номера портов (RFC 1700).

Присвоенные номера располагаются в диапазоне 0 – 1023 и полностью контролируются комитетом IANA (Internet Assigned Numbers Authority). Примеры присвоенных UDP портов: 53 -- Запросы имен DNS, 69 -- Протокол TFTP, 520 -- Протокол RIP.

Диапазон от 1024 до 65535 предназначен для зарегистрированных и динамических портов. Динамические порты могут использоваться любыми процессами или пользователями произвольно (сетевое обеспечение назначает порт, в случае если программа в этом нуждается).

Порты UDP служат для указания места отправки и приема UDP-сообщений. Порт UDP функционирует как единая очередь сообщений для приема всех дейтаграмм, которые предназначены для программы, заданной номером порта (программы, использующие UDP, могут получать одновременно несколько сообщений). Серверная часть каждой программы, использующей UDP, прослушивает определенный порт в ожидании поступающих на него сообщений.

Протокол UDP ведет для каждого порта две очереди: очередь пакетов, поступающих в данный порт из сети, и очередь пакетов, отправляемых данным портом в сеть.

Процедура обслуживания протоколом UDP запросов на передачу в сеть, поступающих от различных прикладных программ, называется

мультиплексированием, **а** распределение по портам назначения пакетов, поступающих из сетевого уровня – демультиплексированием.

4.3.2. Протокол TCP

Протокол **TCP** (Transmission Control Protocol; RFC 793) работает на транспортном уровне, обеспечивает (в отличие от протокола UDP) надежную и ориентированную на установление соединения службу доставки пакетов.

Протокол TCP основан на связи точка-точка, устанавливаемой между двумя узлами сети. Данные, получаемые от прикладных программ, TCP обрабатывает как поток байтов. Байты группируются в последовательно нумеруемые сегменты (нумерация сегментов необходима для правильной их сборки на узле-приемнике). TCP-сегменты инкапсулируются и передаются в IP-пакетах также как и UDP-пакеты.

Протокол TCP реализует:

гарантированную доставку IP-дейтаграмм;

разбиение на сегменты и сборку больших блоков данных, отправляемых программами;

доставку сегментов данных в нужном порядке;

проверку целостности переданных данных с помощью контрольной суммы;

посылку положительных подтверждений, если данные получены успешно.

Формат сообщений TCP. Сегменты (сообщения) TCP состоят из заголовка и блока данных.

Формат заголовка сегмента TCP приведен на рис 4.11**.**

2 байта	Порт источника
2 байта	Порт назначения
4 байта	Последовательный номер
4 байта	Номер подтверждения
4 бита	Длина заголовка
6 битов	Резерв
6 битов	Кодовые биты
2 байта	Окно
2 байта	Контрольная сумма

2 байта	Указатель срочности
Максиму 3 байта	Опции
Переменная	Заполнитель

Рис. 4.11. Формат заголовка сегмента TCP.

Рассмотрим поля заголовка сегмента TCP.

Порт источника идентифицирует процесс-отправитель.

Порт назначения идентифицирует процесс-получатель.

Последовательный номер указывает номер байта, который определяет смещение сегмента относительно потока отправляемых данных.

Номер подтверждения содержит максимальный номер байта в полученном сегменте, увеличенный на единицу (именно это значение используется в качестве квитанции).

Длина заголовка указывает длину заголовка сегмента TCP, измеренную в 32-битовых словах (иногда это поле называют «**Смещение данных»).** Длина заголовка не фиксирована и может изменяться в зависимости от значений, устанавливаемых в поле **Опции**.

Резерв зарезервировано для последующего использования.

Кодовые биты содержат служебную информацию (флаги) о типе данного сегмента:

100000 - срочное сообщение (URG);

010000 - квитанция на принятый сегмент (ACK);

001000 - запрос на отправку сообщения без ожидания заполнения буфера (PSH);

000100 - запрос на восстановление соединения (RST);

000010 - сообщение используемое для синхронизации счетчиков переданных данных при установлении соединения (SYN);

000001 - признак достижения передающей стороной последнего байта в потоке передаваемых данных (FIN).

Окно содержит объявляемое значение размера окна в байтах.

Контрольная сумма рассчитывается по сегменту.

Указатель срочности используется только совместно с кодовым битом URG. Указывает на начало сегмента данных, который необходимо срочно принять.

Поле **Опции** имеет переменную длину и может отсутствовать, максимальная величина поля 3 байта. Это поле используется для решения вспомогательных задач, например, при выборе максимального размера сегмента;

Заполнитель может иметь переменную длину, используется для доведения размера заголовка до целого числа 32-битовых слов.

В протоколе TCP также как и в UDP, для связи с прикладными процессами используются порты. Номера портам присваиваются аналогичным образом: имеются стандартные, зарезервированные номера (например, номер 21 закреплен за сервисом FTP, 23 - за telnet), а менее известные приложения пользуются произвольно выбранными локальными номерами. Однако в протоколе TCP порты используются несколько иначе. Установление соединения выполняется в следующей последовательности**:**

1. Одна из сторон, являющаяся инициатором соединения, посылает запрос протоколу TCP на открытие порта для передачи. Протокол TCP (после открытия порта на стороне процесса-инициатора) посылает запрос процессу, с которым требуется установить соединение.

2. Протокол TCP на приемной стороне открывает порт для приема данных и возвращает квитанцию, подтверждающую прием запроса. При этом для обеспечения двунаправленного (дуплексного) режима работы он открывает также порт для передачи и посылает запрос противоположной стороне

3. Сторона-инициатор открывает порт для приема и возвращает квитанцию. Соединение считается установленным. Далее происходит обмен данными в рамках установленного соединения.

4.3.3. Квитирование в протоколе TCP

Идея квитирования состоит в следующем. Отправитель нумерует единицы передаваемых данных (кадры). Для каждого переданного кадра отправитель запускает таймер и ожидает от приемника так называемую положительную квитанцию (о получении кадра с корректными данными). Время ожидания квитанции ограничено и если по его истечении положительная квитанция не получена, то кадр считается утерянным. В некоторых протоколах приемник, в случае получения кадра с искаженными данными должен отправить отрицательную квитанцию (явное указание того, что данный кадр нужно передать повторно).

Существуют два подхода к организации процесса обмена положительными и отрицательными квитанциями: с простоями и с организацией "окна".

Метод с простоями требует, чтобы источник, пославший кадр, ожидал получения квитанции (положительной или отрицательной) от приемника и только после этого посылал следующий кадр (или повторял искаженный). Очевидно, что этот метод отличает низкая производительность обмена данными (это особенно ощутимо на низкоскоростных каналах связи).

Во втором методе (с организацией ″окна″) источнику разрешается передать определенное количество кадров в непрерывном режиме (без получения на эти кадры ответных квитанций). Количество кадров, которые разрешается передавать таким образом, называется размером окна. Обычно кадры при обмене нумеруются циклически, от 1 до N. При отправке кадра с номером 1 источнику разрешается передать еще N-1 кадров до получения

квитанции на кадр 1. Если же за это время квитанция на кадр 1 так и не пришла, то процесс передачи приостанавливается, и по истечению некоторого тайм-аута кадр 1 передается снова. Алгоритм этого метода называют алгоритмом скользящего окна.

В протоколе TCP реализована разновидность второго метода. В протоколе TCP единицей передаваемых данных является сегмент, окно определено на множестве нумерованных байт неструктурированного потока данных, поступающих с верхнего уровня и буферизуемых протоколом TCP. Квитанция посылается только в случае правильного приема данных. Отрицательные квитанции не посылаются, так что отсутствие квитанции означает либо прием искаженного сегмента, либо потерю сегмента, либо потерю квитанции.

В качестве квитанции получатель сегмента отсылает ответное сообщение, в которое помещает число, на единицу превышающее максимальный номер байта в полученном сегменте. Если размер окна равен N, а последняя квитанция содержала значение K, то отправитель может посылать новые сегменты до тех пор, пока в очередной сегмент не попадет байт с номером K+N. Этот сегмент выходит за рамки окна, и передачу в этом случае будет приостановлена до прихода следующей квитанции. Размер окна задается в поле «Окно», размер которого равен 2 байтам. Если принимающая сторона не может принимать данные, то она выставляет в «Окне» нуль и будет отсылать пакеты с нулем до тех пор, пока не сможет принимать данные.

4.4. Прикладной уровень TCP/IP

4.4.1. Основные протоколы прикладного уровня

Прикладной уровень стека **TCP/IP** играет особую роль в сетевых технологиях. Три нижних уровня этого стека (6 уровней модели OSI) по существу обеспечивают транспорт для прикладных программ и ничего более (для конечного пользователя технологии этих уровней скрыты).

Межсетевой обмен прикладных программ в стеке **TCP/IP** связан с использованием протоколов прикладного уровня, на основе которых разработаны эти прикладные программы.

Стек **TCP/IP** включает большое число протоколов прикладного уровня, ориентированных на самые разнообразные применения, в том числе и протоколы, предназначенные для реализации обеспечивающих (служебных) технологий. К таким (служебным) протоколам относятся рассмотренный ранее протокол DNS (служба DNS для поиска IP адресов), SNMP (простой протокол управления сетью), протоколы безопасности.

К числу самых распространенных протоколов прикладного уровня стека **TCP/IP** (на основе которых реализуются собственно прикладные технологии) относятся:

1. TELNET (эмуляция удаленного терминала).
2. FTP (протокол передачи файлов).
3. TFTP (простой протокол передачи файлов).
4. SMTP (простой протокол передачи почты)
5. HTTP (протокол обмена гипертекстовой информацией).
6. POP 3 (почтовый протокол).
7. IMAP 4 (то же, что и POP 3, но с более широкими возможностями).

4.4.2. Протокол TELNET

Протокол TELNET (RFC-854, RFC-855; 23 портом TCP) описывает стандартный метод взаимодействия терминального устройства ("user") и терминал-ориентированного процесса ("server"). TELNET базируется на трех фундаментальных положениях:

- концепции сетевого виртуального терминала NVT (Network Virtual Terminal);
- принципа договорных опций (согласование параметров взаимодействия);
- симметрии связи "терминал-процесс".
- Протокол TELNET может быть использован для организации взаимодействий:
- "терминал-процесс",
- "терминал-терминал" (связь),
- "процесс-процесс" (распределенные вычисления).

При этом во всех случаях user" - это сторона, инициирующая соединение, а "server" - пассивная сторона.

Сетевой виртуальный терминал NVT задает стандартное описание наиболее широко используемых возможностей реальных физических терминальных устройств. Так что (реальные, основанные на протоколе TELNET) терминальная программа ("user") и взаимодействующий с ней процесс ("server"), преобразовывая характеристики физических устройств в спецификацию NVT, обеспечивают тем самым совместимость устройств с разными характеристиками и возможностями.

Принцип договорных опций позволяет согласовать параметры взаимодействия. NVT специфицирует минимально необходимый набор параметров, который позволяет работать по telnet даже самым древним устройствам. Принцип договорных опций позволяет использовать возможности современных устройств. Например, при взаимодействии «терминал-процесс» "user", (в такой схеме инициатор всегда--"user") используя команды договора, предлагает "server"у применять Esc-последовательности. Получив такую команду "server" начинает их вставлять.

В режиме "терминал-терминал" каждая из сторон может выступать инициатором договорного процесса. При этом применяется принцип "прямого действия" (а не "запрос-подтверждение"). Состоящий в том, что если терминальная программа хочет расширить возможности представления информации, то она это делает (например, вставляет в информационный поток Esc-последовательности), если в ответ она получает информацию в новом формате, то это означает, что попытка удалась, в противном случае происходит откат к стандарту NVT.

Обычно процесс согласования форм представления информации происходит в начальный момент организации telnet-соединения. Каждый из процессов старается установить максимально возможные параметры сеанса. Однако эти параметры могут быть изменены и позже, в процессе взаимодействия (например, после запуска прикладной программы).

Симметрия взаимодействия по протоколу telnet позволяет в течение одной сессии программе-"user" и программе-"server" меняться местами, что принципиально отличает технологию telnet от традиционной схемы "клиент-сервер.

Сетевой виртуальный терминал NVT в протоколе TELNET определен как двунаправленное символьное устройство, состоящее из принтера (для отображения информации) и клавиатуры (для ввода данных).

Принтер имеет неограниченные ширину и длину страницы и может отображать все символы US ASCII (коды с 32 - 127), расширенный набор символов (коды с 128 - 255), а также распознает управляющие коды (с 0 - 31 и 127), среди которых имеются обязательные (табл. 4.4) и рекомендуемые (табл. 4.4) коды.

Таблица 4.3.Обязательные коды

Название кода	Код	Значение
NULL	0	Нет операции
Перевод строки Line Feed (LF)	10	Переход на другую строку с сохранением текущей позиции в строке
Возврат каретки Carriage Return (CR)	13	Устанавливает в качестве текущей первую позицию текущей строки

Таблица 4.4. Рекомендованные коды

Название кода	Код	Значение
Звонок (BEL)	7	Звуковой сигнал
Сдвиг на одну позицию назад (BACK SPACE)	8	Перемещает каретку на одну позицию назад в текущей строке

Горизонтальн. табуляция Horizontal Tab (HT)	9	Перемещение к следующей позиции горизонтальной табуляции
Вертикальная табуляция Vertical Tab (VT)	11	Перемещение курсора к следующей позиции вертикальной табуляции
Прогон страницы Form Feed (FF)	12	Переход к новой странице

Клавиатура должна обеспечивает возможность ввода всех символов ASCII, а также может иметь возможность генерировать стандартные специальные функции управления терминалом. Стандарт telnet определяет пять функций управления терминалом (если на реальном терминале эти функции отсутствуют, то заменяются командой NO (No-Operation).

Команда "Прервать процесс" (Interrupt Process - **IP**) реализует стандартный для многих систем механизм прерывания процесса выполнения задачи пользователя (Cntrl+C в Unix-системах или Cntrl+Break в MS-DOS).

Команда "Прервать процесс выдачи" (Abort Output - **AO**). В отличие от команды IP (при выполнении IP прерывается выполнение текущего процесса пользователя, но не происходит очистка буфера вывода, при этом вывод данных на экран или на принтер может продолжаться) происходит очистка буфера вывода, что прерывает выдачу данных.

Команда "Ты еще здесь?" (Are You There - **AYT**). Позволяет пользователю убедиться в том, что он не потерял связь с удаленной машиной.

Команда "Удалить символ" (Erase Character – **EC).** Команда EC стандартизирует так называемый символ "забой" или удаление последнего напечатанного символа.

Команда "Удалить строку" (Erase Line - **EL**). Данная команда аналогична EC, но удаляет целую строку ввода. Обычно выполнение этой команды приводит к очистке буфера ввода, т.к. при работе в режиме командной строки строка ввода только одна.

Команды telnet имеют свой формат. Команда - это 2-байтовая последовательность, состоящая из Esc-символа (255) IAC (Interpret as Command) и кода команды (240-255). Команды, связанные с процедурой согласования параметров сеанса, имеют 3-х байтовый формат: третий байт - ссылка на устанавливаемую опцию.

4.4.3. Протокол FTP

Первая спецификация **протокола FTP** (File Transfer Protocol) относятся к 1971 году (**RFC 114**). FTP подвергался многократной модификации (более15; **RFC 765** – переход на транспорт TCP; **RFC 959**, октябрь 1985 г., устранены ошибки в документации и добавлены новые команды).

Простейшая модель работы протокола **FTP** представлена на рис. 4.12 . В протоколе FTP используются два канала:

канал управления (КУ), по которому осуществляется управление информационным обменом в стандарте протокола TELNET;

канал передачи данных (КПД), который может быть использован как для приема, так и для передачи данных.

FTP соединение инициируется интерпретатором протокола пользователя (ИПП). Команды FTP генерируются ИПП и передаются на интерпретатор протокола сервера (ИПС), установить контакт, с которым пользователь может и другими средствами. Ответы сервера отправляются пользователю также по КУ. Сервер FTP «слушает» 21 порт TCP, находясь постоянно в состоянии ожидания соединения.

Рис. 4.12. Простая модель работы протокола FTP.

Команды FTP определяют параметры канала и процесса передачи данных, а также характер работы с файловыми системами, а именно:

роль участников соединения: активный, пассивный;

порт соединения как для модуля Программа передачи данных пользователя (ППДП), так и для модуля Программа передачи данных сервера (ППДС);

тип передачи;

тип передаваемых данных;

структуру данных и управляющие директивы, обозначающие действия, которые пользователь хочет совершить, например, сохранить, считать, добавить или удалить данные или файл и другие.

После согласования параметров канала передачи данных, один из участников соединения, который является пассивным (например, ППДП), становится в режим ожидания открытия соединения на заданный для передачи данных порт. После этого активный модуль (например, ППДС) открывает соединение и начинает передачу данных.

После окончания передачи данных, соединение между ППДС и ППДП закрывается, но управляющее соединение ИПС и ИПП остается открытым. Пользователь, не закрывая сессии FTP, может еще раз открыть канал передачи данных.

В случае передачи данных на третий компьютер (три компьютера, из них два сервера, ни один из которых не расположен на локальном хосте пользователя) пользователь организует канал управления с двумя серверами с прямым каналом данных между ними. Команды управления идут через пользователя, а данные напрямую между серверами (рис. 4.13).

Рис. 4.13. Модель работы протокола FTP с передачей передачи данных на третий компьютер.

Алгоритм работы такой схемы, на примере передачи данных от сервера 1 к серверу 2, сводится к следующему.

1. ИПП указал модулю ИПС 1 работать в пассивном режиме. После этого ИПС 1 отправил пользователю адрес и номер порта (N), который он будет слушать.

2. ИПП назначил ИПС 2 активным участником соединения, указав ему передавать данные на порт (N) ИПС 1.

3. ИПП подал ИПС 1 команду “сохранить поступившие данные в указанном файле”**, а ИПС 2 — “**передать содержимое заданного файла**”.**

4. Между ИПС 1 и ИПС 2 образуется поток данных, который управляется клиентским хостом.

Команды протокола FTP

Команды управления контролем передачи данных, которыми обмениваются ИПС и ИПП, можно разделить на три достаточно большие группы:

- Команды управления доступом к системе.
- Команды управления потоком данных.
- Команды FTP-сервиса.

Команды управления доступом к системе

USER. Как правило, эта команда открывает сессию FTP между клиентом и сервером. Аргументом команды является **имя (идентификатор)** пользователя для работы с файловой системой. Команда может подаваться не только в начале, но и в середине сессии, если, например, пользователь желает изменить идентификатор, от имени которого будут проводиться действия. При этом все переменные, относящиеся к старому идентификатору, освобождаются. Если во время изменения идентификатора происходит обмен данными, обмен завершается со старым идентификатором пользователя.

PASS. Подается после ввода идентификатора пользователя, в качестве аргумента содержит **пароль пользователя**. При этом данные аутентификации FTP передаются по сети открытым текстом.

CWD. Позволяет работать с различными каталогами удаленной файловой системы. Аргументом команды является строка, указывающая путь требуемого каталога удаленной файловой системы.

REIN. Команда реинициализации. Очищает все переменные текущего пользователя, сбрасывает параметры соединения, но позволяет завершить передачу данных с прежними параметрами.

QUIT. Закрывает управляющий канал. Если в момент подачи команды происходит передача данных, то канал закрывается после окончания передачи данных.

Команды управления потоком данных

Команды управления потоком (устанавливают параметры передачи данных) могут подаваться в любом порядке, но все они должны предшествовать командам FTP-сервиса. К основным командам управления потоком данных относятся следующие:

PORT. Команда назначает адрес и порт хоста, который будет использоваться как активный участник соединения по каналу передачи данных. Аргументами команды являются 32-битный IP адрес и 16-битный номер порта соединения. Эти значения разбиты на шесть 8-битных полей и представлены в десятичном виде: h1, h2, h3, h4, p1, p2, где hN - байты адреса (от старшего к младшему), а pN - байты порта (от старшего к младшему).

PASV. Эта команда отправляется модулю, который будет играть пассивную роль в передаче данных (“слушать” соединение). Ответом на данную команду должна быть строка, содержащая адрес и порт хоста, находящиеся в режиме ожидания соединения в формате команды PORT — “h1, h2, h3, h4, p1, p2”.

Команды **TYPE, STRU, MODE** определяют, соответственно, тип передаваемых данных (**ASCII, binary, Image** и другие), структуру или формат передачи данных (**File, Record, Page),** способ передачи (**Stream, Block** и другие). Использование этих команд необходимо для организации взаимодействия в гетерогенных средах.

Команды FTP-сервиса

Это команды определяющие действия с файлами. Как правило, аргументом команд этой группы является путь к файлу. Синтаксис указанного пути должен удовлетворять требованиям формата файловой системы обработчика команды. К основным командам данной группы относятся следующие:

RETR. Команда указывает модулю “Программа передачи данных сервера” передать адресату копию файла, заданного параметром этой команды.

STOR. Указывает модулю “Программа передачи данных сервера” принять данные и сохранить их как файл, имя которого задано параметром этой команды. Если такой файл уже существует, он будет замещен новым, если нет, будет создан заново.

Команды **RNFR и RNTO** должны следовать одна за другой. Первая команда содержит в качестве аргумента старое имя файла, вторая - новое. Последовательное применение этих команд переименовывает файл.

ABOR. Команда предписывает серверу прервать выполнение предшествующей сервисной команды (например, передачу файла) и закрыть канал передачи данных.

Команда **DELE** удаляет указанный файл.

Команды **MKD и RMD**, соответственно, создают и удаляют указанный в аргументе каталог.

При помощи команд **LIST и NLST** можно получить список файлов в указанном каталоге.

Все команды FTP-протокола отправляются **интерпретатором протокола пользователя** (ИПП) в текстовом виде - по одной команде в строке. Каждая строка команды (идентификатор и аргументы) заканчиваются символами <CRLF>. Имя команды отделяется от аргумента символом пробела.

Обработчик команд возвращает код обработки каждой команды, состоящий из трех цифр. Коды обработки составляют определенную иерархическую структуру и, как правило, определенная команда может возвратить только определенный набор кодов. За кодом обработки команды следует символ пробела, затем следует текст пояснения. Например, строка успешного завершения операции выглядит следующим образом: “200 Command okay”.

4.4.4. Протокол TFTP

Тривиальный протокол передачи файлов TFTP (Trivial File Transfer Protocol , RFC 1350, июль 1992 г., порт 69 UDP) является упрощенной вариантом протокола FTP.

TFTP ориентирован на транспортные услуги UDP и поэтому не обеспечивает надежной передачи данных. Программная реализация TFTP обычно используется для начальной загрузки бездисковых сетевых рабочих станций (записывается в чипе ПЗУ рабочей станции), мостов и маршрутизаторов.

Протокол TFTP значительно проще протокола FTP. TFTP поддерживает 5 типов пакетов:

- запрос чтения,
- запрос записи,
- данные,
- подтверждения,
- ошибки.

Формат пакетов описан в RFC 1350. Первый пакет, передаваемый от клиента серверу, является управляющим. Этот пакет определяет имя файла, а также действия с ним на удаленной станции (запись или чтение: GET или PUT--те же, что и в FTP). Затем передаются пакеты данных, каждый размером 512 байт; при этом начальный пакет данных помечается номером 1. Номер каждого следующего пакета увеличивается на единицу. Принимающая сторона на каждый полученный пакет передает подтверждение. Любой пакет размером меньше 512 байт означает конец передачи данных.

Порядковая нумерация и подтверждение принятых пакетов реализуется TFTP, а не службой транспортного уровня UDP. (UDP, как нам известно, обеспечивает только ненадежную, не ориентированную на соединение службу). При этом TFTP не использует принцип скользящего окна (как в TCP), так что можно сказать, что TFTP пользуется окном размером 1. TFTP в отличие от FTP поддерживает толь одно соединение.

4.4.5. Протокол SMTP

Протокол обмена почтовыми сообщениями в Internet SMTP (Simple Mail Transfer Protocol, порт 25 TCP) описан в RFC 821 (август 1982 г., 68с.). Расширяющие дополнения содержатся в RFC 1870 (ноябрь 1995 г., 9с.), в RFC 974 описано взаимодействие SMTP с системой доменных имен DNC.

Схема взаимодействия по протоколу SMTP следующая. Между отправителем (клиентом), который инициирует соединение, и получателем почтового сообщения (сервером), устанавливается двусторонняя связь (см. рис. 4.14). Далее между клиентом и сервером устанавливается информационный обмен, продолжающийся до тех пор, пока соединение не будет закрыто или прервано.

Рис. 4.14. Схема взаимодействия по протоколу SMTP.

При такой схеме взаимодействия (режим on-line) почта доставляется клиенту практически незамедлительно (секунды, возможно минуты из-за очереди). Это принципиально отличает протокол SMTP от теряющего актуальность протокола UUCP (Unix-Unix-CoPy), используемого в Unix-системах. В UUCP почта передается по цепочке: от одного сервера к другому, пока не достигнет машины абонента-получателя (так называемый принцип "stop-go").

Протокол SMTP предусматривает ряд процедур, которые реализуются соответствующими командами. К основным процедурам SMTP относятся:

- передача почты (Mail Procedure);
- форвардинг почты (Mail Forwarding), т.е. перенаправление почтового сообщения;
- проверка имён почтового ящика и вывод списка почтовых групп (Verifying and Expanding);
- открытие и закрытие канала передачи (Opening and Closing).

Команды SMTP состоят из ключевых слов, за которыми следует один или более параметров. Ключевое слово состоит из 4-х символов и разделено от аргумента одним или несколькими пробелами. Каждая командная строка заканчивается символами CRLF (перевод строки).

Команды протокола SMTP

HELO *hostname*

Первая командой сеанса, *hostname* - доменное имя отправителя (вызывающего клиента).

MAIL FROM: *email_адрес_от_кого*
Обратный адрес (адрес отправителя).

RCPT TO: *email_адрес_кому*
Адрес получателя (в случае нескольких адресатов команда повторяется для каждого адресата).

DATA
Команда вводится без параметров и обозначает начало ввода сообщения **(б**азовая структура сообщения определена в RFC-822). Сервер посылает промежуточный положительный отклик 354, после чего воспринимает все последующие строки как сообщение. Концом ввода сообщения является новая строка, состоящая из одной точки в первой позиции. Сообщение состоит из заголовка (который регламентируется RFC-822) и тела. Между заголовком и телом сообщения должна быть *одна пустая строка*. Сообщение укладывается в конверт, который не виден получателю.

RSET
Сброс сеанса к начальному состоянию (состояние, как после ввода HELO).

VRFY *email_адрес*
Команда серверу: проверить подлинность введенного *email_адреса.* В случае успеха выдается положительный отклик (250,251 или 252), иначе выдается отклик 550. При этом адекватность положительного отклика (существование *email_адреса)* гарантирована только для локальных адресов на сервере.

EXPN email_addr
Команда по которой сервер выводит локальные адреса списка рассылки, в котором содержится и адрес *email_addr.* Если *email_addr не локальный адрес, то* поведение команды не определено (просто выдается отклик 250). Действия этой команды в стандарте четко не определены. Ее реализация не является обязательной. Команда по соображениям секретности может не поддерживаться сервером

SEND FROM: *email_адрес*

Используется вместо команды MAIL, указывая на то, что почта должна быть доставлена на терминал пользователя.

SOML FROM: *email_адрес*
Комбинации команд SEND или MAIL (или на терминал или в ящик).

SAML FROM: *email_адрес*
Комбинации команд SEND и MAIL (успех, если хотя бы в ящик).

HELP

Запросить у сервера помощь о переданной в качестве аргумента команде.

NOOP

На эту команду сервер должен дать положительный ответ. Команда ничего не делает и никак не влияет на указанные до этого данные.

QUIT

Конец связи.

Существуют также команды Расширенного SMTP **(ESMTP**). Однако не все серверы их поддерживают или поддерживают некоторое подмножество ESMTP-команд, включая и нестандартные команды (это можно выяснить, если вместо HELO ввести команду EHLO).

4.4.6. Протокол POP 3

Протокол **POP 3** (Post Office Protocol v.3; RFC 1939, май 1996; TCP, порт 110) используется для получения почты с сервера на рабочую станцию пользователя (для передачи используется SMTP). Протокол **P**OP 2 (RFC 937) устарел и по набору команд несовместим с POP 3.

После установления соединения с сервером POP 3 появляется строка, начинающаяся с символов "+OK". Затем сервер POP3 переходит в стадию авторизации, в процессе которой пользователю необходимо ввести имя и пароль. После успешной авторизации, сервер POP-3 входит в транзакционное состояние, временно блокируя почтовый ящик пользователя для внешних транзакций.

В этом состоянии у пользователя (посредством клиента POP-3) появляется возможность узнать количество сообщений в его почтовом ящике, принять сообщения, удалить сообщения из почтового ящика. Сообщения после их приема клиентом удаляются из почтового ящика.

После посылки со стороны клиента команды **quit,** сеанс связи будет закрыт. Затем на сервере будет выполнен необходимый процесс *обновления* (удаление сообщений и т.п.).

Команды протокола POP 3.

USER *имя_пользователя.*
Имя пользователя (идентификатор почтового ящика).

PASS *пароль.*
Пароль пользователя.

STAT.

Команда выводит два числа: число сообщений и их общий объем в байтах.

LIST *n.*

Если *n* указано, то выводит размер **n-го** сообщения в байтах. Если *n* не указано, то выводит список из двух колонок, содержащих номера сообщений и размер сообщений в байтах.

RETR *n.*

Выводит сообщение под номером *n* .

DELE *n.*

Удаляет из почтового ящика ***сообщение n*** без изменения нумерации сообщений. Все удаленные ***в данном сеансе*** сообщения могут быть восстановлены командой **REST**.

TOP *n m.*

Выводит заголовок и ***m*** первых строк сообщения номер ***n***.

RSET.

Отменяет удаление всех сообщений, удаленных в данном сеансе.

NOOP

Нет операции (то же, что и в SMTP),

QUIT

Конец связи.

4.4.7. Протокол IMAP 4

Протокол IMAP 4 (Internet Mail Access Protocol; **RFC 2060**, декабрь 1996 г; 143 порт TCP.) является протоколом, поддерживающим возможность управления электронной почтой непосредственно на почтовом сервере. MAP4, обеспечивая те же функции что и POP3, дополнительно позволяет:

- выборочно загружать с сервера отдельные сообщения или фрагменты сообщений;
- просматривать заголовки сообщений и выбрать для загрузки только избранные сообщения;
- осуществлять поиск по ключевым словам в заголовках письма, и в самом сообщении;

и т.д.

При этом все сообщения, а также организованная пользователем структура папок, останутся на сервере неизменными до тех пор, пока не будут удалены или изменены пользователем явным образом.

IMAP обеспечивает надежный механизм идентификации пользователя, поддерживает Kerberos и другие протоколы безопасности, включает поддержку адресной книги и ссылок на отдельные электронные документы.

Тема 5. Аппаратные средства компьютерных сетей

5.1. Классификация аппаратных средств

К аппаратным средствам компьютерных сетей относятся:

1. Компьютеры (IBM PC, Sun, Next, Macintosh и др.).

2. Сетевые адаптеры, адаптеры локальных радиосетей.

3. Соединительные средства:

3.1. Сетевые соединительные средства (коннекторы, трансиверы, репитеры, концентраторы, коммутаторы мультиплексоры, мосты);

3.2. Межсетевые соединительные средства (повторители, мосты, маршрути-заторы, брандмауэры, шлюзы, модемы).

4. Передающая среда:

4.1.Проводная передающая среда (коаксиальный кабель, витая пара, волоконно-оптический кабель).

4.2. беспроводная передающая среда (широкополосные сигналы, маломощное СВЧ-излучение, инфракрасные лучи).

5. Периферийное оборудование общего назначения (принтеры, плоттеры, сканеры и т.д.).

5.2. Сетевые адаптеры

Сетевой адаптер (сетевая карта, карта сетевого интерфейса, Network Interface Card; NIC) реализует протоколы физического и канального уровней; может быть встроен в материнскую плату или является отдельным периферийным устройством. Сетевой карта (см. рис. 5.1) вставляются в свободное гнездо шины расширения материнской платы компьютера и подсоединяются с помощью разъема к кабелю сети (таких разъемов на плате адаптера может быть несколько).

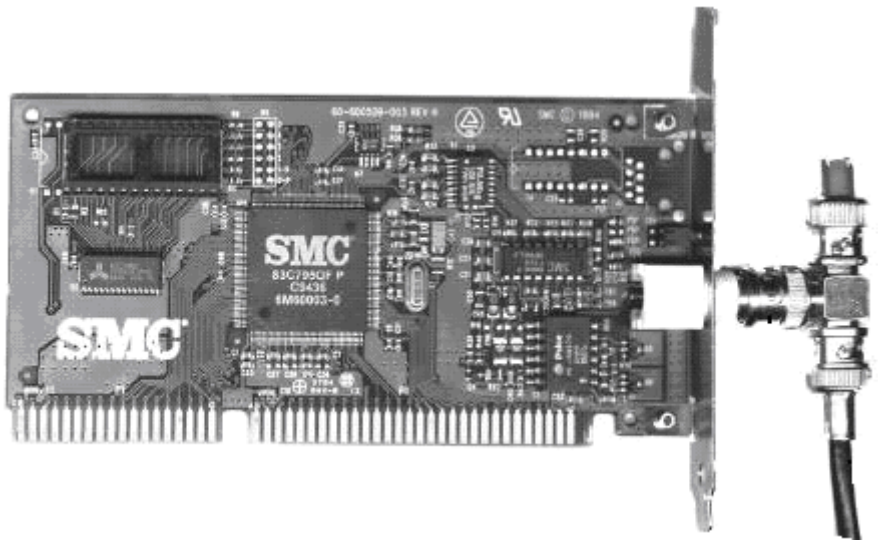

Рис. 5.1. Сетевая карта с Т-коннектором.

На сервере может быть установлено несколько сетевых адаптеров. Сетевой адаптер работает под управлением драйвера этого адаптера, который играет роль посредника между адаптером и операционной системой (драйвер «знает» конкретные особенности устройства). Распределение функций между сетевым адаптером и драйвером может изменяться от реализации к реализации.

Сетевой адаптер обычно выполняет следующие функции:

- Формирование передаваемой информации в виде кадра определенного формата. Кадр, включает несколько служебных полей, среди которых адрес компьютера назначения и контрольная сумма.
- Обеспечение доступа к среде передачи данных. Доступ к среде осуществляется по специальному алгоритму (по методу случайного или маркерного доступа или их комбинации).
- Кодирование бит кадра последовательностью электрических сигналов при передаче данных и декодирование при их приеме.
- Преобразование информации из параллельной формы в последовательную и обратно. Сигнал передается по широкополосному кабелю без использования модуляции сигнала в последовательно бит за битом, а не побайтно, как внутри компьютера.
- Синхронизация битов, байтов и кадров, необходимая для устойчивого приема сигнала и поддержания синхронизма приемника и передатчика информации. Битовая синхронизация осуществляется посредством манчестерского кода, кадровая — последовательностью байт преамбулы кадра.

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных: ISA, EISA, PCI, PCNCIA, USB и др.

Сетевые адаптеры различаются также по типу используемой сетевой технологии (по типу протокола канального уровня): Ethernet, Token Ring, FDDI и т.п. В связи с тем, что для каждой технологии возможно использование различных сред передачи данных сетевой адаптер может поддерживать как одну, так и одновременно несколько сред: коаксиальный кабель, неэкранированную витую пару, оптоволоконный кабель (для этого имеются специальные разъемы).

Драйверы сетевых адаптеров инсталлируются отдельно при подключении сетевых адаптеров к компьютеру. Драйверы должны находиться на жестком диске компьютера или в ПЗУ. Изначально сетевые адаптеры поддерживали лишь один из протоколов определенного метода доступа (Ethernet, ArcNet, Token Ring), что создавало определенные проблемы (сервера в ряде случаев должны работать с несколькими протоколами). Для устранения этого недостатка были разработаны интерфейсы драйверов, позволяющие привязывать платы к различным протоколам. Существует два несовместимых интерфейса:

ODI (Open Drive Interface) — открытый сетевой интерфейс, разработанный фирмами Novel, Apple и другими крупными сетевыми фирмами.

NDIS (Network Driver Interface Specification) — спецификация интерфейсов сетевых драйверов компании Microsoft и 3COM.

5.3. Коннекторы и трансиверы

5.3.1. Коннекторы

Т-коннектор (T-connector) – небольшой тройник (см. рис. 5.1), который с одной стороны подключается к сетевому адаптеру, а с двух других сторон к нему присоединяются отрезки тонкого коаксиального кабеля с разъёмами на концах. Тип кабеля – 10 Base 2.

В-коннектор (BNC-connector) – цилиндрический соединитель для двух отрезков тонкого коаксиального кабеля.

RJ-45 – разъём для витой неэкранированной пары. (Кабель - 10 Base T). Его не следует путать с разъёмом для телефонной линии RJ-11.

5.3.2. Трансиверы

Трансивер это интерфейсное устройство, обеспечивающее необходимые преобразования и приемопередачу сигнала между компьютером (устройством) и общей сетевой средой. Различают внутренние (встроенные в схему контроллера сетевой карты) и внешние трансиверы. В локальных сетях, основанных на технологии Ethernet, на долю которых приходится 85% мирового парка локальных сетей, внешние трансиверы применяются для подключения: толстого коаксиального кабеля 10Base 5, волоконно-оптического кабаля (оптический трансивер), а также для стыковки кабеля витая пара и волоконно-оптического кабеля.

Различают также КВ/УКВ трансиверы (радиостанции в широком смысле) и спутниковые трансиверы. Такие устройства являются многофункциональными.

Изначально трансиверы использовались для подключения рабочей станции к толстому коаксиальному кабелю (тип кабеля 10 Base5). На корпусе такого трансивера имеется 3 разъёма: два для подключения к толстому коаксиальному кабелю, один – для трансиверного кабеля. Трансиверный кабель, длиной до 50 метров, представляет собой многожильный экранированный кабель, соединяющий сетевой адаптер с трансивером. В нужных местах толстый коаксиальный кабель прокалываются вампирами, к которым подключается трансивер.

5.4. Повторители

Повторитель (Repeater) — устройство, предназначенное для соединения сегментов сети. Повторитель копирует (пересылает) все пакеты из одного сегмента во все другие, подключенные к нему. Основной задачей

повторителя является восстановление электрических сигналов для передачи их в другие сегменты.

Длина сегмента сети не должна превышать определенной величины. При нарушении этого условия можно использовать повторитель. Повторитель работает на физическом уровне модели OSI. Выполняется либо в виде карты, вставляемой в слот расширения материнской платы (в этом случае можно соединять только сегменты на тонком коаксиальном кабеле), либо в виде отдельного устройства со своим источником питания. Такой повторитель стоит дороже, но позволяет подключать сегменты на различных физических средах. Повторители используются также и как самое простое средство соединения однотипных локальных сетей. Такие повторители являются устройствами локального действия и обычно используются для соединений двух высокоскоростных локальных сетей, Удобны тем, что могут соединять различные типы физических средств передачи сигналов (коаксиальные, волоконно-оптические кабели и витые пары). Но повторители не могут транспортировать пакеты и кадры между сетями, имеющими различные форматы кадров и пакетов.

5.5. Концентраторы

Концентраторы (Hubs) начали широко использоваться при переходе технологии Ethernet на витую пару в конце 80-х гг. прошлого столетия. В настоящее время концентраторы потеряли актуальность.

Различают пассивные и активные концентраторы.

Пассивный концентратор представляет собой устройство, к которому подключается несколько рабочих станций (обычно не больше трёх). Пассивный концентратор не обеспечивает усиление сигнала. Применяется на расстоянии не больше 30 метров. Такие концентраторы не пригодны в высокоскоростных сетях.

Активный концентратор имеет автономный источник питания и за счет усиления сигнала обеспечивает, надёжную работу на расстоянии до 600 метров. Количество подключаемых станций — 4, 8, 16 и т.д. При небольшом количестве каналов (3-4 канала) активный концентратор может быть выполнен в виде платы, вставляемой в сервер. Активный концентратор может функционировать как простой усилитель (при этом вместе с полезным сигналом усиливаются и шумы, что является существенным недостатком) или как генератор (повторитель сигналов). В последнем случае их называют многопортовыми повторителями. Кроме основной функции концентраторы могут выполнять и дополнительные функции, такие как, объединение сегментов с различными физическими средами, автосегментацию портов, поддержку резервных связей и т.д.

Посредствам концентраторов из отдельных физических сегментов образуется общая среда передачи данных, которая представляет собой логический сегмент (домен коллизий), такой, что при одновременной передаче данных любыми двумя компьютерами этого логического сегмента, даже принадлежащих разным физическим сегментам, возникает, коллизия,

приводящая к блокировке передающей среды. Это один из существенных недостатков концентраторов, приведших к тому, что они потерями актуальность и в настоящее время не выпускаются.

5.6. Коммутаторы

Коммутаторы появились в конце 80-х годов. Вначале коммутаторы использовались исключительно для сегментации сети. В настоящее же время они широко применяются для непосредственного подключения к хостам и являются эффективным средством наращивания локальных сетей, позволяя устранить сетевую перегруженность.

Коммутатор (switch) в отличие от концентратора направляет поступивший пакет не ко всем узлам сети, а к конкретному узлу (по адресу получателя пакета).

Коммутаторы подразделяются на ряд категорий от простейших, предназначенных для сетей рабочих групп (внутренний трафик для сегмента и один мост для связи с другими сегментами сети) до коммутаторов масштаба предприятия, обеспечивающих диспетчеризацию трафика, поддержку большого количества логических соединений и трансляцию протоколов и т.д. Коммутаторы работают на 2 и 3 уровне модели OSI. Коммутаторы 3 уровня позволяют осуществлять маршрутизацию пакетов. Существуют также коммутаторы 7-го уровня (коммутаторы информации), которые работают на прикладном уровне с такими приложениями, как FTP, HTTP, Telnet и др. Коммутаторы информации позволяют разрешить ряд проблем, связанных с созданием и функционированием современных информационных систем, например, таких как Google.

Различают ненастраиваемые, настраиваемые, неуправляемые и управляем-ые коммутаторы.

Настраиваемые коммутаторы позволяют производить некоторые настройки (например, конфигурирование VLAN). Такие коммутаторы могут быть управляемыми и неуправляемыми. Пример неуправляемых, но настраиваемых коммутаторов - серия DES-12xx.

Неуправляемые коммутаторы не обеспечивают поддержку управления по протоколу SNMP. Неуправляемые коммутаторы могут быть настраиваемыми. К неуправляемым и ненастраиваемым коммутаторам относятся DES-1005, DES-1008 и др.

Управляемые коммутаторы поддерживают протоколы сетевого управления и могут управляться по сети с использованием специального программного обеспечения (D-Link DView, HP Openview). К ним относятся DES-32xx и выше.

Функционирование коммутатора основано на поддержке таблицы (табл. 5.1), которая связывает порты коммутатора с адресами подключенных к ним устройств. Таблица создается либо вручную администратором сети, либо автоматически в процессе обучения коммутатора. Используя таблицу

адресов и содержащийся в пакете адрес получателя, коммутатор организует виртуальное соединение порта отправителя с портом получателя и передает пакет через это соединение. Виртуальное соединение между портами коммутатора сохраняется в течение передачи одного пакета, так что для каждого пакета виртуальное соединение организуется заново.

Таблица 5.1. Таблица коммутатора

MAC-адрес	Номер порта
A	1
B	2
C	3
D	4
E	5
F	6
G	7

Различают следующие основные типы функциональной структуры коммутаторов:

С коммутационной матрицей.

С общей шиной.

С разделяемой многовходовой памятью.

Коммутаторы с коммутационной матрицей имеют ограниченное число портов (сложность реализации пропорциональна квадрату числа портов).

Коммутаторы с общей шиной используют высокоскоростную шину, связь портов осуществляется в режиме разделения времени.

В коммутаторах с разделяемой многовходовой памятью между входными и выходными портами используется управляемая разделяемая память.

В сложных коммутаторах обычно используется комбинация рассмотренных архитектур, что позволяет компенсировать их недостатки.

Различают прозрачные (transparent) и не прозрачные коммутаторы. Прозрачный коммутатор после завершения обучения (создания таблицы адресов) при появлении на его входе кадра с неизвестным адресом назначения повторяет этот кадр на всех портах. Достоинство таких коммутаторов в том, что их появление в сети совершенно не заметно для ее конечных узлов (это удобно при модернизации сети). Недостаток очевиден – возрастает трафик (засорение сети). Другой недостаток – возможность наличия в сети замкнутых петель (замкнутых маршрутов, сеть засоряется зацикливающимися пакетами).

Для устранения этого недостатка используется алгоритм покрывающего дерева (Spanning Tree Algorithm, STA). Алгоритм позволяет коммутаторам адаптивно строить дерево связей с помощью специальных тестовых кадров (при обучении). При обнаружении замкнутых контуров некоторые связи контура объявляются резервными. Коммутатор может

использовать такую резервную связь только при отказе какой-либо основной. В результате сеть обладают некоторым запасом надежности.

Для построения сетей, в которых существует несколько параллельных путей (петель) используется протокол STP (Spanning Tree Protocol, IEEE 802.1D). Этот протокол используется не только в коммутаторах и мостах, но и в маршрутизаторах.

Непрозрачные коммутаторы, работающие по алгоритму маршрутизации от источника (source routing), передают кадры между сегментами на основе полной информации о межсегментном маршруте. Эту информацию записывает в кадр станция-источник кадра. При такой маршрутизации конечные узлы должны знать топологию сети, а сетевые адаптеры иметь программный компонент, реализующий выбор маршрута кадров.

5.7. Мосты

Мосты, как и повторители, соединяет локальные сети или сегменты локальных сетей на аппаратном уровне, но, в отличие от повторителей, на более высоком уровне (на MAC-уровне).

Разница между мостом (bridge) и коммутатором состоит в том, что мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, в то время как коммутатор одновременно поддерживает потоки данных между всеми своими портами (если они не заняты). Так что, если мост передает кадры последовательно, то коммутатор параллельно. Мосты различаются многочисленными алгоритмами передачи и фильтрации пакетов. В этом плане они схожи с коммутаторами.

Мосты подразделяются на:

Внутренние, которые реализуется на сервере, связанном с двумя или более сетями.

Внешние в виде отдельные сетевые станции или устройства, реализующие функции моста.

Локальные, которые связывают локальные сети или сегменты посредством кабельной системы.

Удаленные, обеспечивающие связь посредством телефонной или другой линии.

Выделенные (станции, которые используются только как сетевые мосты).

Невыделенные (совмещают функции моста и рабочей станции).

В настоящее время локальные мосты практически вытеснены коммутаторами. Мосты используются в основном для связи локальных сетей с глобальными, как средство удаленного доступа, т.е. там, где нет необходимости в параллельной передаче данных.

5.8. Маршрутизаторы

Маршрутизаторы позволяют объединять сети с различными принципами организации в единую сеть. Коммерческое применение маршрутизаторов относится к 70 гг. прошлого столетия.

Маршрутизаторы подразделяются на три класса: верхнего, среднего и нижнего уровня. В качестве маршрутизатора нижнего уровня может использоваться рабочая станция или сервер, имеющий несколько сетевых интерфейсов и специальное программное обеспечение. Маршрутизатор верхнего класса является сложным специализированным и дорогостоящим устройством, объединяющим в отдельном корпусе множество маршрутных модулей.

Маршрутизаторы направляют пакеты или кадры в нужные межсетевые каналы с учетом адресов получателей. Маршрутизатор, в отличие от моста, является адресуемым элементом сети. Он выбирает только предназначенные ему кадры (пакеты) и направляет их в межсетевые каналы согласно адресам получателей. Маршрутизаторы используются как в глобальных, так и в локальных сетях. В локальных сетях маршрутизаторы взаимодействуют на подуровне управления логическими каналами (ПУЛК), а в глобальных сетях взаимодействие осуществляется на сетевом уровне.

Маршрутизаторы фильтруют и пересылают сетевой трафик на основе алгоритмов и правил, существенно отличающихся от тех, что используются мостами и коммутаторами. Маршрутизация предполагает два основных процесса: определение оптимального маршрута и транспортировку пакетов (коммутацию).

Если транспортировка пакетов относительно проста, то определение маршрута может представлять собой очень сложный процесс. Эта сложность обусловлена многочисленными и к тому же изменяющимися во времени параметрами, которые должен учитывать маршрутизатор при выборе оптимального маршрута. Для обеспечения процесса определения маршрута, алгоритмы маршрутизации инициализируют и поддерживают таблицы маршрутизации. В общем случае таблица маршрутизации содержит: действительные адреса устройств в сети, служебную информацию протокола маршрутизации, адреса ближайших маршрутизаторов.

Различают методы, алгоритмы и протоколы маршрутизации.

Методы маршрутизации можно подразделить на три группы: простая, статическая и адаптивная маршрутизация.

Простая маршрутизация характеризуется неизменностью алгоритма при изменении топологии или состояния сети. Ее разновидности:

- случайная (по любому случайному направлению, кроме того, от куда пришло),
- лавинная (по всем направлениям, кроме того, от куда пришло),
- по предыдущему опыту (обеспечивается коррекция первоначально случайно выбранных маршрутов).

Статическая маршрутизация осуществляется по заранее разработанной таблице маршрутов. Разновидности статической маршрутизации:

- одно путевая (одна таблица: от отправителя к получателю),
- много путевая (несколько таблиц с выбором по определенному признаку, например по типу сервиса).

Адаптивная (динамическая) маршрутизация реализуется с учетом состояния сети (учитываются: топология сети, интенсивность потоков данных, задержки в узлах коммутации и т.д.). К разновидностям адаптивной маршрутизации относятся:

- Локальная (узел маршрутизации сам выбирает маршруты, не получая информации от других узлов).
- Распределенная (соседние маршрутизаторы обмениваются информацией о своих локальных состояниях).
- Централизованная (маршрутизаторы передают свои состояния центральному маршрутизатору, который корректирует маршруты для каждого маршрутизатора).
- Гибридная (комбинация из трех вышерассмотренных).

Процесс функционирования маршрутизатора основан на определенном алгоритме маршрутизации, который формирует вектор стоимостей путей доставки и, в качестве оптимального, выбирают путь с наименьшей стоимостью. Простейшие из алгоритмов определяют путь на основе наименьшего числа транзитных узлов. Более сложные алгоритмы в понятие «стоимость» закладывают несколько показателей (например, задержку передачи пакетов, пропускную способность каналов связи, или денежную стоимость связи). К алгоритмам маршрутизации предъявляются следующие требования: оптимальность выбора маршрута, простота реализации, устойчивость, быстрая сходимость, гибкость реализации.

Протоколы маршрутизации

1. Протокол RIP (Routing Information Protocol) — дистанционно-векторный протокол маршрутизации. Существуют две версии: RIPv1 **(**RFC 1058) и RIPv2 **(**RFC 2453). В RIPv2 реализована поддержка сетей переменной длины**.** RIP-маршрутизаторы используют UDP-транспорт, порт 520. Протокол RIP еще не потерял актуальность в Internet. В середине 1980 гг. самым популярным протоколом маршрутизации. RIP был повсеместно принят производителями персональных компьютеров.

2. EIGRP (Enhanced Interior Gateway Routing Protocol) — расширенный протокол шлюзовой маршрутизации. Протокол является обновленной в начале 1990-х гг. версией протокола IGRP **(**IGRP разработан в 1980 гг. компанией Cisco Systems). Ориентирован на обеспечение живучего протокола для маршрутизации в пределах автономной системы (AS).

3. OSPF **(**Open Shortest Path First, RFC 2328) — открытый протокол, базируется на алгоритме поиска наикратчайшего пути. **Р**азработан для IP

сетей рабочей группой IETF. Является наиболее распространенным во внутренних сетях TCP/IP.

4. EGP **(**Exterior Gateway Protocol**,** RFC 904, 1984 г.) — протокол внешних роутеров. Являясь первым протоколом внешних роутеров. EGP сыграл важную роль в Internet. Из-за этих присущих ему недостатков EGP заменяется другими внешними протоколами роутеров, такими, как BGP и IDRP

5**.** BGP **(**Border Gateway Protocol, RFC 1163 — версия 3; RFC 1771 — версия 4) является протоколом маршрутизации между AS. Создан для применения в Internet. BGP можно назвать следующим поколением EGP. BGP и другие протоколы маршрутизации между AS постепенно вытесняют EGP из Internet.

6**.** IDRP **(**IS-IS Inter-Domain Routing Protocol, ISO 10747) — протокол междоменной маршрутизации промежуточных систем. IDRP является протоколом OSI. Предназначен для обмена информации между доменами. IDRP базируется на протоколе BGP.

5.9. Брандмауэры

Брандмауэр по существу представляет собой систему, которая в целях безопасности накладывает ограничения на проходящий через нее поток данных. Брандмауэр позволяет разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую. Для каждого проходящего пакета брандмауэр принимает решение пропускать его или отбросить, опираясь на определенный набор правил. Как правило, эта граница проводится между локальной сетью предприятия и Internet, но может быть проведена и внутри локальной сети. Брандмауэры получили признание вначале 1990-х в связи развитием Internet.

Работа брандмауэра предполагает соблюдение следующих условий:

- весь трафик должен проходить через одну точку;
- брандмауэр должен контролировать и регистрировать весь проходящий трафик;
- сам брандмауэр должен быть неприступен» для внешних атак.

Брандмауэры подразделяются на следующие виды:

- брандмауэры *с* фильтрацией пакетов (packet-filtering firewall);
- шлюзы сеансового уровня (circuit-level gateway);
- шлюзы прикладного уровня (application-level gateway).

Наибольшее распространение получили брандмауэры с фильтрацией пакетов, реализованные на маршрутизаторах и сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Такие брандмауэры работают на сетевом уровне OSI.

Фильтры пакетов просматривают поля поступающих IP-пакетов, а затем пропускают или удаляют их в зависимости, например, от IP-адресов отправителя и получателя, номеров портов отправителя и получателя протоколов TCP или UDP и других параметров. Фильтр сравнивает полученную информацию со списком правил фильтрации для принятия решения о разрешении или запрещении передачи пакета.

Технология фильтрации пакетов является самым «дешевым» способом реализации брандмауэра. Такой брандмауэр может проверять пакеты различных протоколов, причем с большой скоростью, так как он анализирует на сетевом уровне модели OSI только заголовок пакета.

В настоящее время, несмотря на то, что фильтры пакетов получили широкое распространение они мало подходят для внешней защиты сети; но хорошо подходят для обеспечения безопасности внутри сети (с их помощью можно разбить сеть на защищенные сегменты).

К достоинствам брандмауэров с фильтрацией пакетов относятся:

- относительно невысокая стоимость,
- гибкость в определении правил фильтрации,
- небольшая задержка при прохождении пакетов.

Недостатки у данного типа брандмауэров следующие:

- локальная сеть видна (маршрутизируется) из Internet;
- правила фильтрации пакетов трудны в описании, требуются хорошие знания технологий TCP и UDP;
- при нарушении работоспособности брандмауэра все, расположенные за ним компьютеры становятся либо полностью незащищенными, либо недоступными;
- аутентификацию с использованием IP-адреса можно обмануть использованием IP-спуфинга, т.е. когда атакующая система выдает себя за другую, используя ее IP-адрес;
- отсутствует аутентификация на пользовательском уровне.

Шлюзы сеансового уровня представляет собой транслятор TCP соединения. Пользователь образует соединение с определенным портом на брандмауэре, после чего последний производит соединение с местом назначения по другую сторону от брандмауэра. Во время сеанса этот транслятор копирует байты в обоих направлениях. Такой тип брандмауэра позволяет создавать транслятор для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису, сбор статистики по его использованию.

К достоинствам шлюзов сеансового уровня следует отнести их низкую стоимость, незначительное влияние на скорость маршрутизации, а также невидимость компьютеров локальной сети из вне. Основной недостаток — не способны осуществлять фильтрацию отдельных пакетов.

Брандмауэры прикладного уровня (шлюзы прикладного уровня или прокси-брандмауэры) используют сервера конкретных сервисов FTP, HTTP, SMTP и

т.д., запускаемые на брандмауэре и пропускающие через себя весь трафик, относящийся к данному сервису. При этом между клиентом и сервером образуются два соединения: от клиента до брандмауэра и от брандмауэра до места назначения.

Преимущества брандмауэров прикладного уровня:

- локальная сеть невидима из Internet;
- при нарушении работоспособности брандмауэра пакеты перестают проходить через брандмауэр, тем самым не возникает угрозы для защищаемых им машин;
- защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, снижая тем самым вероятность взлома с использованием дыр в программном обеспечении;
- аутентификация на пользовательском уровне может быть реализована система немедленного предупреждения о попытке взлома.

К недостаткам этого типа брандмауэров следует отнести: более высокая, чем для пакетных фильтров стоимость; невозможность использовании протоколов RPC и UDP; более низкую, чем для пакетных фильтров производительность.

Различают также SPI-брандмауэры (Statefull Packet Inspection — SPI) объединяющие в себе все рассмотренные выше разновидности брандмауэров. Это так называемые многоуровневые брандмауэры. SPI-брандмауэры обеспечивают наиболее надежную защиту сетей. Они применяются в современных маршрутизаторах. Большинство современных маршрутизаторов поддерживают протокол NAT (Network Address Translation), который базируются на сеансовом уровне.

5.10. Шлюзы

Шлюз – межсетевой преобразователь, обеспечивающий соединение компьютерных сетей, имеющих различную архитектуру или протоколы. Так что под шлюзом в широком смысле понимают не только средства, обеспечивающие соединение сетей с различной архитектурой, например SNA и TCP/IP, но и средства, транслирующие различные протоколы канального и физического уровня. Трансляцию протоколов могут осуществлять мосты, коммутаторы, маршрути-заторы, программные и аппаратные шлюзы.

5.11. Мультиплексоры

Мультиплексор – это устройство, которое обеспечивает эффективное использование среды передачи данных, пропускная способность которой значительно выше пропускной способности устройств, участвующих в коммутации.

Различают три основных вида мультиплексирования:

- Частное мультиплексирование.
- Временное мультиплексирование.
- Статистическое мультиплексирование.

Частотное и временное мультиплексирование основано на частотном и временном разделении каналов. Сущность статистического мультиплексирования состоит в том, что мультиплексор в процессе работы учитывает активность устройств, участвующих в информационном обмене и может применять приори-теты для определенных устройств.

Мультиплексоры находят широкое применение в цифровых транспортных сетях (см п.1.5).

В транспортных сетях находят применение следующие виды мультиплексоров:

- Первичные мультиплексоры для ввода/вывода абонентских сигналов с аналоговыми и цифровыми интерфейсами в/из цифрового потока Е1 (МП-1, МП-2, МП-4).
- Мультиплексоры сигналов: 4Е1 > Е2, 16Е1 > Е3, 4Е3 > Е4 (МКСС 2/8/34/(34/140)).
- Мульдексы – устройства, которые осуществляют как мультиплекси-рование, так и демультиплексирование цифровых сигналов (МД2/8, МД2/34).

5.12. Модемы

5.12.1. Типовая система передачи данных

Схема типовой системы передачи данных (СПД) приведена на рис. 5.1.

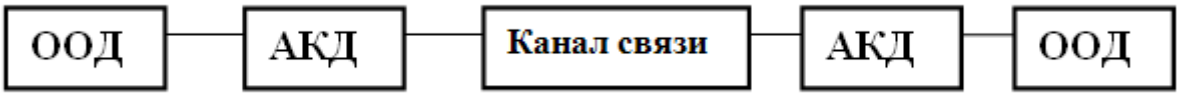

Рис. 5.2. Схема типовой системы передачи данных, где:

ООД -- оконечное оборудование данных;

АКД -- аппаратура канала данных.

Международный термин ООД — Data Terminal Equipment (DTE). ООД (DTE) может представлять собой персональный компьютер, мэйнфрейм, терминал, кассовый аппарат и т.д.

Международный термин АКД — Data Communications Equipment (DCE). АКД (DCE), называемая также аппаратурой передачи данных (АПД), предназначена для передачи информации между двумя или большим числом ООД. АКД по существу и представляет собой модем в широком смысле слова.

В 60—70-х годах прошлого столетия модемы осуществляли только модуляцию/демодуляцию, так что в состав АКД входили и другие устройства, такие как устройства защиты от ошибок (УЗО), автоматические

вызывные устройства (АВУ) и др., а сами модемы относились к устройствам преобразования сигналов (УПС). При этом дополнительно использовались стыки С3 и Сву**.** Современные модемы реализуют функции не только упомянутых выше устройств, но и ряд других сложных функций.

Под модемами в настоящее время понимают не только широко известные модемы для коммутируемых телефонных каналов, но также и такие устройства как сотовые модемы, пакетные радиомодемы, модемы ISDN, цифровые модемы.

Взаимодействие (стыковка) ООД и АКД осуществляется по одному из стандартных интерфейсов (стыков С2, в русской интерпретации), а подключение АКД к каналу связи (или среде распространения) по одному соответствующих стандартных интерфейсов (стыков С1). Стандартный интерфейс специфицирует входящие/исходящие цепи, разъемы и соединительные кабели.

5.12.2. Методы передачи данных

Методы передачи данных можно классифицировать по следующим признакам:

- по направлению передачи;
- по способу передачи (последовательный – по одному проводнику, параллельный – по нескольким проводникам, каждый бит по своему проводу);
- по способу группирования данных;

По направленности передачи различают следующие режимы информационного обмена:

- симплексный (однонаправленный), который обеспечивает передачу только в одном направлении;
- полудуплексный – обеспечивает передачу в обоих направлениях, но в каждый данный момент времени передача может быть только в одном направлении;
- дуплексный режим, который обеспечивает передачу данных в обоих направлениях одновременно.

По способу группирования данных различают два основных метода передачи: асинхронный **(**старт-стопный) и синхронный**.**

Асинхронная передача зародилась в телеграфии, в конце 50-х гг. прошлого столетия. В начале 60-х годов получила распространение как способ передачи данных. При асинхронной передаче символы (байты) передаются поочередно. Каждый передаваемый байт обрамляется стартовым (для синхронизации) и одним или несколькими стоповыми битами.

Асинхронный режим передачи используется в основном в случае, когда передаваемые данные генерируются в случайные моменты времени, например пользователем. Асинхронный режим часто применяется при передаче данных по интерфейсу DTE-DCE. При этом модем может работать с компьютером в асинхронном режиме, а с удаленным модемом (по каналу связи) в синхронном и наоборот.

Передача данных по каналу связи в асинхронном режиме малоэффективна (используются простые методы модуляции, такие как амплитудная и частотная). Современные же методы модуляции (ОФМ, КАМ и др.) требуют применения синхронного метода передачи.

Асинхронный способ передачи используется в интерфейсе RS-232 (стыке С2). Для передачи символов по интерфейсу RS-232 наибольшее распространение получил следующий формат. Каждый старт-стопный символ содержит один стартовый бит, 7 бит us ASCII (например, латинская буква А имеет код 1000001*)*, один бит паритета (проверка на четность) и два стоповых бита. Стартовый бит всегда имеет низкий уровень напряжения. Бит паритета устанавливается в "1" или "О" так, чтобы общее число единиц в 8-ми битной группе было нечетным или четным. Стоповые биты имеют высокий уровень напряжения. При передаче информации в расширенной кодировке ASCII используется формат, состоящий из одного стартового бита, восьми информационных и одного стопового бита. При этом бит паритета не используется.

Таким образом, для передачи 7 (8) информационных бит при асинхронном способе передачи необходимо 10 (11) бит (бит паритета может не использоваться).

Достоинство асинхронной передачи – простота (простые схемы формирования тактовых импульсов). Основной недостаток – большой объем избыточной информации, который может превышать 25%.

При синхронной передаче данные передаются кадрами достаточно большой длины (кадры Ethernet, Token Ring и др.). Такой кадр (см. рис. 5.3) содержит признак начала кадра (ПН), заголовок кадра (ЗАГ), данные, проверочные символы (ПС) и признак конца кадра (ПК).

ПН	ЗАГ	Данные	ПС	ПК

Рис. 5.3. Состав кадра передачи данных.

Признаки начала и конца кадра должны обеспечивать возможность выделения границ кадров. Способ формирования этих комбинаций зависит от конкретного способа передачи, определяемого используемым протоколом.

Различают следующие подходы к формированию признаков границ:

- использование указателя длины кадров (в одном из полей заголовка кадра указывается длина кадра);
- использование специальных символов, например, символов не манчестерского кода;
- использование запрещенных для передачи комбинаций двоичных символов.

Последний способ самый простой, однако он приводит к так называемой непрозрачной передаче, так как пользователь не может использовать некоторые последовательности двоичных символов (запрещено использовать ПН и ПК). Этот недостаток устраняется в знак-ориентированной прозрачной передаче и бит-ориентированной передаче.

При знак-ориентированной прозрачной передаче перед каждым из управляющих кодов ставится специальный знак АР1. Если встречается информационная комбинация совпадающая с АР1, то пред ней также вставляется АР1 (это так называемый байтстаффинг). Наличие двух подряд идущих АР1 говорит о том, что вторая АР1 — информационная комбинация.

При бит-ориентированной прозрачной передаче передача ведется кадрами переменной длины, при этом в качестве границ кадра используется фиксированная комбинация двоичных символов, называемая флагом. Если в поле кадров (между ПН и ПК) на передающей стороне встречается комбинация, совпадающая с флагом, то она преобразуется путем вставки символов таким образом, чтобы исключить подобную ситуацию. Такая процедура называется битстаффингом. Например, если в качестве флага используется комбинация 01111110, то упомянутое преобразование сводится к следующему. Последовательность между флагами просматривается и, если в ней встречается 5 единиц идущих подряд, то после них вставляется дополнительный (служебный) символ 0.

5.12.3. Классификация модемов

К основным классификационным признакам модемов обычно относят:

- область применения;
- функциональное назначение;
- тип используемого канала;
- конструктивное исполнение;
- поддержка протоколов модуляции,
- исправления ошибок и сжатия данных.

По области применения различают:

- модемы коммутируемых телефонных каналов;

- модемы выделенных телефонных каналов;
- модемы физических соединительных линий (модемы низкого уровня, модемы основной полосы);
- модемы (терминальные адаптеры) цифровых систем передачи;
- модемы сотовых систем связи;
- кабельные модемы;
- модемы пакетных радиосетей;
- модемы локальных радиосетей.

Подавляющее большинство выпускаемых модемов предназначено для использования на коммутируемых телефонных каналах.

Модемы для физических линий подразделяются на: модемы низкого уровня (линейные драйверы), использующие цифровые сигналы, и модемы "основной полосы". В последних используются методы модуляции, аналогичные применяемым в модемах для телефонных каналов. В качестве передающей среды могут использоваться: экранированная и неэкранированная витая пара, коаксиальный кабель и др.

Модемы для цифровых систем (ISDN и xDSL модемы) обеспечивают подключение к стандартным цифровым каналам, таким как E1/T1 и поддерживают функции соответствующих канальных интерфейсов.

Модемы для сотовых систем связи отличаются компактностью исполнения, поддержкой специальных протоколов модуляции и исправления ошибок, позволяющих эффективно передавать данные в условиях сотовых каналов с высоким уровнем помех и постоянно изменяющимися параметрами.

Кабельные модемы представляют собой широкополосные устройства, обеспечивающие высокоскоростной доступ к Internet по сети кабельного телевидения.

Пакетные радиомодемы предназначены для передачи данных по радиоканалу между мобильными пользователями. При этом несколько радиомодемов используют один и тот же радиоканал в режиме множественного доступа.

Модемы локальных радиосетей (адаптеры локальных радиосетей) – это специализированные радиомодемы. Такие модемы обеспечивают передачу данных на небольшие расстояния (до 300 м) со скоростью от 2 до 54 Мбит/с. Работают в определенном диапазоне частот с применением сигналов сложной формы.

По интеллектуальным возможностям различают модемы:

- без системы управления;

- поддерживающие набор АТ-команд;
- поддерживающие команды V. 25bis;
- поддерживающие фирменную систему команд;
- поддерживающие протоколы сетевого управления.

Большинство современных модемов поддерживает широкий спектр интеллектуальных возможностей. Стандартом де-факто является множество АТ-команд, разработанных фирмой Hayes, позволяющее управлять характеристиками модема и параметрами связи. Модемы, поддерживающие АТ-команды, называются Hayes-совместимых модемами.

Набор команд рекомендации ITU-T V. 25bis, позволяет управлять режимами установления соединения и автовызова. Специализированные модемы промышленного применения часто имеют фирменную систему команд, отличную от набора АТ-команд. Промышленные модемы часто поддерживают протокол сетевого управления SMNP, позволяющий администратору управлять сетевыми средствами (включая модемы) с удаленного терминала.

По конструктивным особенностям модемы различаются на:

- внешние,
- внутренние,
- портативные,
- групповые.

Внешние модемы представляют собой автономные устройства, подключаемые к компьютеру или другому DTE посредством одного из стандартных интерфейсов DTE-DCE. Внутренний модем — это плата расширения, вставляемая в слот материнской платы компьютера.

Портативные модемы предназначены для использования мобильными пользователями совместно с компьютерами класса Notebook. Они отличаются малыми габаритами и высокой ценой. Их функциональные возможности, как правило, не уступают возможностям полнофункциональных модемов. Часто портативные модемы оснащены интерфейсом PCMCIA.

Групповые модемы представляют собой совокупность отдельных модемов, объединенных в общий блок. Они имеют общий блок питания, общие средства управления и отображения. Отдельный модем группового модема представляет собой плату с разъемом, устанавливаемую в блок, и рассчитан на один или небольшое число каналов.

5.13. Передающая среда

5.13.1. Кабель типа «витая пара»

Различают два типа кабеля "витая пара": неэкранированная витая пара (UTP – Unshielded Twisted Pair; рис. 5.4) и экранированная витая пара (STP – Shielded Twisted Pair; рис. 5.5).

Рис. 5.5. Неэкранированная витая пара.

Существуют 7 категорий витой пары: Категории 1, 2 (разъем RJ–11) относится к телефонному кабелю; категории 3-5, 6, 7 применимы в компьютерных сетях (коннектор RJ–45). Чем выше номер категории, тем более высокую скорость передачи поддерживает кабель. Категории 3, 4 из-за низкого качества в настоящее время не применяются. Используемый в компьютерных сетях кабель "витая пара" состоит из 4-х покрытых оболочкой скрученных медных проводов (синий/синий-белый, оранжевый/ оранжевый-белый, зеленый/зеленый-белый, коричневый/корич-невый-белый).

UTP благодаря низкой стоимости, гибкости и простоте инсталляции является в настоящее время наиболее популярной передающей средой для офисных локальных сетей. Становление технологии Gigabit Ethernet (GE; скорость передачи 1000 Мбит/с) привело к появлению "витой пары" UTP Категорий 5e и 6. Категория 6 имеет полосу пропускания до 250 МГц, что в 2,5 раза больше, чем у Категории 5. Категория 7 (до 600 МГц) относится к STP (в STP 7 каждая пара индивидуально защищена). Основным недостатком UTP является низкая помехозащищенность, поскольку такой кабель подвержен сильному влиянию электромагнитных помех.

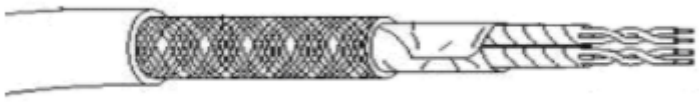

Рис. 5.6. Экранированная витая пара.

Витая пара STP отличается от UTP тем, она более дорогая, более жесткая, экранирована и должна заземляться. Витая пара STP применяется при высоком уровне радиопомех.

5.13.2. Коаксиальный кабель.

Коаксиальный кабель похож на телевизионный кабель. В течение примерно 10 лет с момента появления технологии Ethernet он был единственным типом кабеля, который применялся для создания локальных сетей. После появления витой пары в новых инсталляциях коаксиальный кабель практически не применяется.

В локальных сетях использовались 2 типа коаксиального кабеля: кабель спецификации 10BASE-5 – толстый коаксиальный кабель (диаметр медного провода – 2,17 мм; рис. 5.7), и кабель 10BASE-2 – тонкий коаксиальный кабель (диаметр провода – 0,89 мм; рис. 5.8).

Рис. 5.7. Толстый коаксиальный кабель

Спецификации 10BASE-5 удовлетворяет 50-омный RG8 и RG11 (магистральный кабель); в СНГ это кабели РК – 50 – 6 – 11 и РК – 50 – 6 – 13;

Рис. 5.8. Тонкий коаксиальный кабель

Спецификации 10BASE-2 удовлетворяет семейство 50-омных кабелей RG-58; в СНГ РК–50-3-11.

5.13.3. Волоконно-оптический кабель

Волоконно-оптический кабель (рис. 5.9) передает не электрические, а световые сигналы. Кабель может содержать одно светопроводящее волокно, но обычно их несколько (от 4 до 216). Волоконно-оптический кабель компактнее и легче медного, диаметр одного волокна примерно соответствует человеческому волосу. Различают многомодовые (ступенчатые и градиентные) и одномодовые волокна.

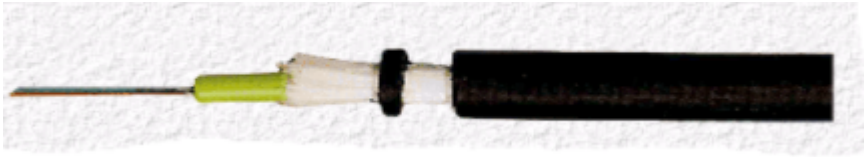

Рис. 5.9. Волоконно-оптический кабель.

В многомодовом волокне для передачи применяется светодиод, с помощью которого невозможно получить однородный сигнал и точно направить его внутрь светопроводящей жилы. Поэтому при передаче светового сигнала, он, многократно отражаясь от стенок оптоволокна, трансформируется в серию мод (лучей), которые, проходя различные расстояния, попадают в точку приема не одновременно, что порождает так называемую межмодовую дисперсию. При этом, чем больше длина оптоволокна, тем меньше полоса пропускания оптоволокна.

Посредством сложного легирования оптоволокна можно добиться плавного уменьшения показателя преломления от центра к оболочке волокна

(так получают градиентное волокно) и тем самым, уменьшая межмодовую дисперсию, расширить полосу пропускания волокна до 100-1000 МГц/км. Диаметр многомодового волокна составляет 50-65 мк , диаметр оболочки — 125 мк.

В одномодовом волокне для передачи сигнала используется лазер. Лазер использует одну длину волны, поэтому на дальность передачи сигнала влияет только величина затухания. Диаметр одномодового проводника составляет 8,3 микрона, а оболочки – 125 мк. Количество мод зависит и от диаметра волокна. Если диаметр волокна сравним с используемой длиной волны, то по волокну будет распространяться только одна мода и действовать будут уже законы не геометрической, а волновой оптики.

Оптоволоконную технологию отличают следующие достоинства:

- огромная пропускная способность,
- устойчивость к электромагнитным воздействиям;
- отсутствие излучения;
- защищенность от несанкционированного доступа.
- отсутствие зависимости величины потерь от скорости передачи данных в одномодовых оптоволоконных линиях.

5.13.4. Беспроводная передающая среда

Для организации беспроводной связи используют следующие виды сигналов:

1. Широкополосные радиосигналы в до СВЧ-диапазоне (до 1 Ггц). В такой среде можно передавать данные в свободном пространстве с направленной антенной до 30 км; со всенаправленной антенной – до 200 – 250 м.

2 Маломощное СВЧ-излучение. Скорость передачи от 0,64 до 54 Мб/с.

3. Инфракрасное излучение. Приемопередатчики могут находиться на расстоянии друг от друга до 25 м, но для достижения максимальной скорости должны беспрепятственно видеть друг друга (инфракрасные лучи не проходят даже простые перегородки).

Беспроводные системы работают в следующих диапазонах частот:

902 – 928 МГц,
2,4 – 2,5 ГГц,
3.2 – 3,6 ГГц,
5,15 – 5,25 ГГц
7,725 – 7,85 ГГц.

С 1998 г. диапазон 2,4–2,4835 в республике Беларусь выделен для использования в беспроводных источниках связи.

Тема 6. Базовые компьютерные сети

6.1. Ethernet на толстом коаксиальном кабеле

Локальная сеть Ethernet на толстом коаксиальном кабеле (стандарт 10Base-5) представляет собой классическую Ethernet (она соответствует экспериментальной сети Ethernet фирмы Xerox; 1973 г; скорость передачи данных 2,94 Мбит/с). В качестве передающей среды в этой сети, обеспечивающей скорость передачи данных до 10 Мбит/с, используется кабель спецификации 10BASE-5 (см. п. 5.13.2); в качестве доступа к среде — метод CSMA/CD (см. п. 3.1).

Конфигурация Ethernet на толстом коаксиальном кабеле приведена на рис. 6.1. Сетевые карты компьютеров подключаются к кабелю посредством трансиверов (см. п. 5.3). Трансивер устанавливается непосредственно на кабеле и питается от сетевого адаптера компьютера. Трансивер соединяется с сетевым адаптером трансиверным кабелем AUI (Attachment Unit Interface) длиной до 50 м, состоящим из 4 витых пар. Две пары проводников этого кабеля используются для передачи и приема сигнала, одна пара для — обнаружения конфликтов и четвертая пара — для подачи питания на трансивер.

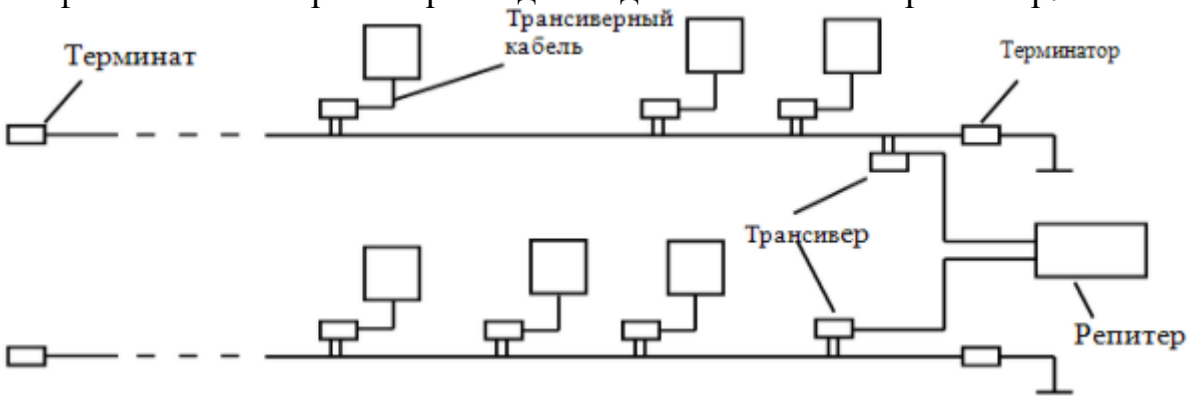

Рис. 6.1. Конфигурация Ethernet на кабеле 10 BASE 5.

Сегмент кабеля 10BASE-5 (длиной до 500 м) для предотвращения отражения сигнала имеет на концах терминаторы (R=50 Ом), корпус одного из которых должен быть заземлен. Для увеличения длины локальной сети сегменты кабеля соединяются с помощью репитеров (см. п. 5.4). Ограничения для Ethernet на толстом коаксиальном кабеле приведены в табл. 6.1.

Таблица 6.1. Ограничения для Ethernet на толстом кабеле

Максимальная длина сегмента	500 м
Максимальное количество сегментов в сети	5
Максимальная длина сети	2,5 км
Максимальное количество станций, подключенных к одному сегменту (если в сети есть репитеры, они тоже считаются как станции)	100
Минимальное расстояние между точками подключения рабочих станций	2,5 м
Максимальная длина трансиверного кабеля	50 м

Максимальное число репитеров	4

К достоинствам Ethernet на толстом кабеле относятся:

хорошая защищенность кабеля от внешних воздействий,

сравнительно большое расстояние между узлами,

возможность простого перемещения рабочей станции в пределах длины кабеля AUI.

Недостатки Ethernet на толстом кабеле:

высокая стоимость кабеля,

сложность прокладки кабеля,

наличие специального инструмента для формирования кабельного хозяйства.

6.2. Ethernet на тонком коаксиальном кабеле

Локальная сеть Ethernet на тонком коаксиальном кабеле (стандарт 10Base-2) использует в качестве передающей среды коаксиальный кабель спецификации 10Base-2 (см. п. 5.13.2); скорость передачи данных 10 Мбит/с; метод доступа к среде — CSMA/CD.

Линейная и разветвленная конфигурации Ethernet на тонком коаксиальном кабеле приведены на рис. 6.2 и на рис. 6.3 соответственно. Сетевые адаптеры компьютеров, которые в этой сети выполняют и функции трансивера, подключаются к гибкому тонкому кабелю с помощью Т-коннекторов (см. п. 5.3). Кабель в такой сети висит на сетевом адаптере, что не только затрудняет физическое перемещение компьютеров, но и чревато нарушением работоспособности сети. Разрыв (по неосторожности, например, уборщицей) приводит не только к нарушению работоспособности сети, но может привести и к «выгоранию» сетевых карт. Эта особенность сети Ethernet на тонком кабеле является главным ее недостатком.

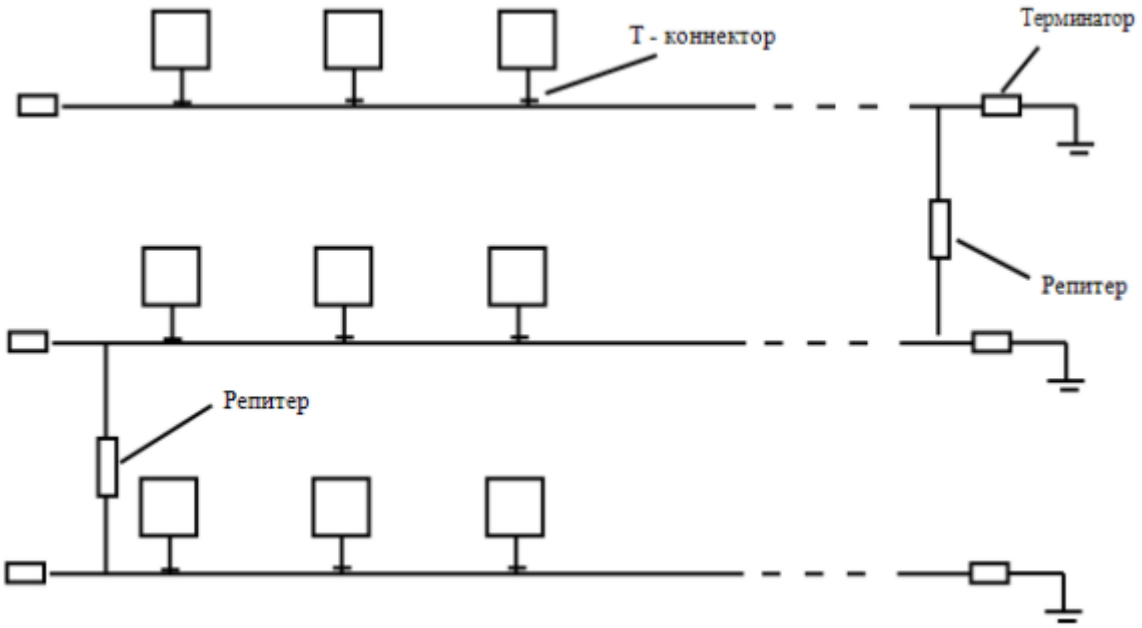

Рис. 6.2. Линейная конфигурация Ethernet 10BASE-2.

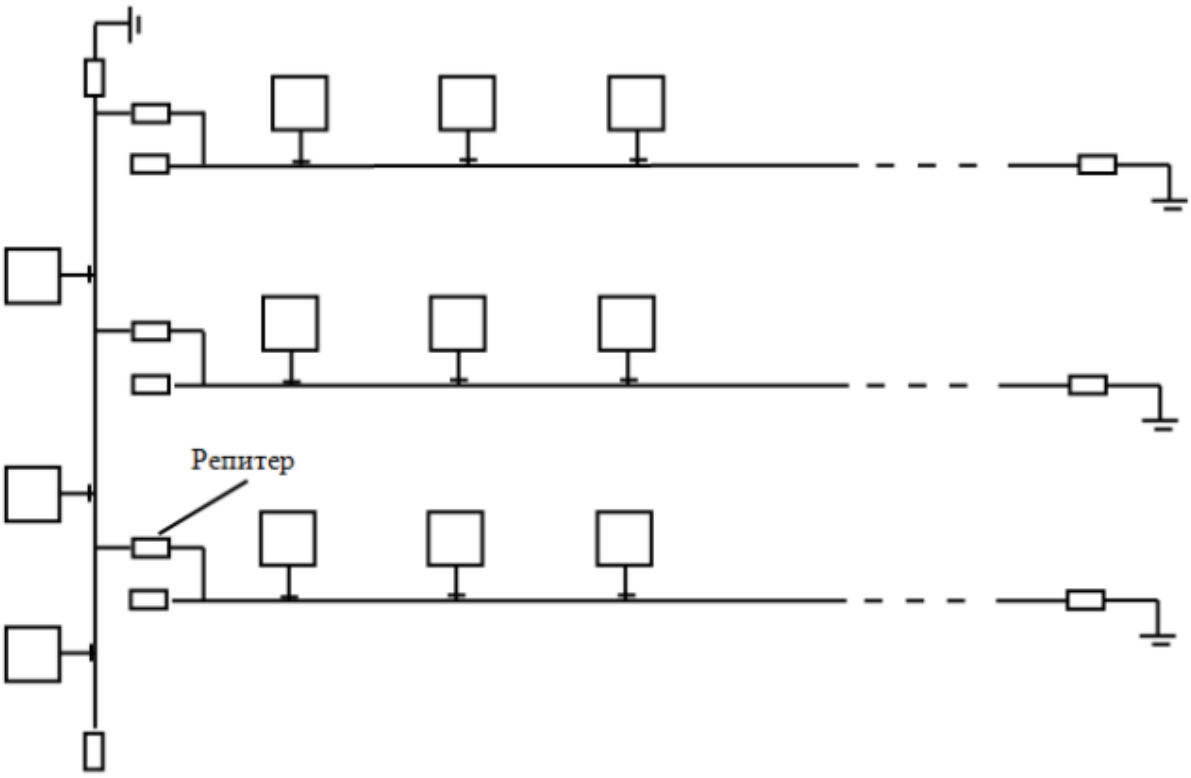

Рис. 6.3. Разветвленная конфигурация Ethernet 10BASE-2

Ограничения для Ethernet на тонком кабеле приведены в табл. 6.2.

Таблица 6.1. Ограничения для Ethernet на тонком коаксиальном кабеле

Максимальная длина сегмента	185 м
Максимальное количество сегментов в сети	5

Максимальная длина сети	925 м
Максимальное количество станций, подключенных к одному сегменту (если в сети есть репитеры, они тоже считаются как станции)	30
Минимальное расстояние между точками подключения рабочих станций	0,5 м
Максимальное число репитеров	4

Главный недостаток Ethernet на тонком коаксиальном кабеле: высокая вероятность повреждения кабеля; при разомкнутых контурах заземления возможно выгорание сетевых адаптеров.

6.3. Ethernet 10BASE–T

Локальная сеть Ethernet на основе стандарта 10Base-T (IEEE 802.3i; 1991г.) использует в качестве передающей среды витую пару UTP (см. п.5.13.1); скорость передачи данных 10 Мбит/с; метод доступа к среде — CSMA/CD. Конфигурации Ethernet 10BASE–T приведены на рис. 6.4. Соединение компьютеров с концентратором осуществляются посредством двух витых пар: одна пара используется для передачи данных от компьютера к концентратору, другая от концентратора к компьютеру, так что физически 10BASE–T имеет топологию «звезда», логически же 10BASE–T представляет собой топологию шины.

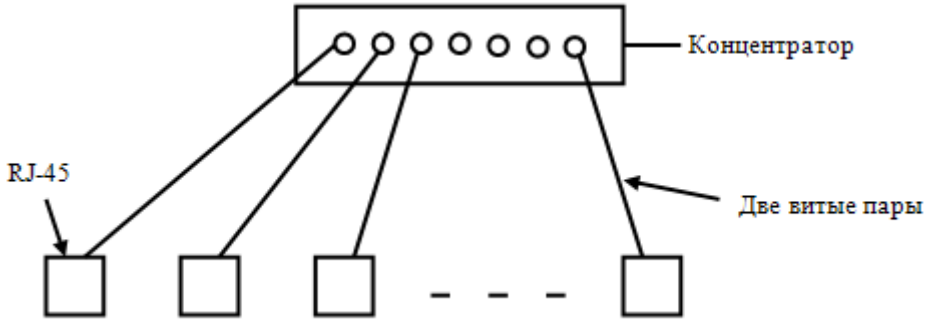

Рис. 6.4. Конфигурация Ethernet 10Base-T.

Ограничения для Ethernet 10Base-T приведены в табл. **6.3.**

Таблица 6.3. Ограничения для Ethernet 10Base-T

Максимально допустимое число сегментов	1024
Максимальное число сегментов с узлами	1024
Максимальная длина сегментов	100 м.
Максимальное число узлов на сегменте	2
Максимальное число узлов в сети	1024
Максимальное число концентраторов цепочки (между двумя компьютерами)	4

Концентраторы и коммутаторы в сети Ethernet 10Base-T можно объединять между собой с помощью тонкого коаксиальном кабеля. При расширении сети ключевую роль играют коммутаторы; они позволяют выйти за рамки спецификации Ethernet, так как подсчет концентраторов в цепочке после прохождения коммутатора начинается с нуля

К достоинствам Ethernet 10Base-T относятся:

- простота наращивания сети;
- простота эксплуатации;
- более высокая живучесть сети;
- простота локализации неисправностей;
- возможность применение нескольких типов кабеля.

6.4. Ethernet 10base–F

Функционально сеть стандарта 10Base-F состоит из тех же элементов, что и сеть 10Base-T. Используется та же топология и функциональные элементы, что и в 10Base-T: концентратор, к портам которого с помощью кабеля подключаются сетевые адаптеры компьютеров. Однако в качестве среды передачи данных применяется оптоволокно. Для соединения адаптера с концентратором используются два оптоволокна: одно на передачу, другое на прием сигнала. Существует несколько разновидностей 10Base-F: FOIRL, 10Base-FL, 10Base-FL, 10Base-FP.

Первым стандартом Комитета 802.3 для оптоволокна в сетях Ethernet был предложенный в1987 году Стандарт FOIRL (Fiber Optic Inter-Repeater Link). Он был предназначен для обеспечения информационного взаимодействия повторителей, находящихся на значительном расстоянии друг от друга (до 1000 м). В последующем потерял актуальность в связи с появлением других сетевые технологий семейства 10 Base F.

Стандарт 10Base-FL предназначен для соединения конечных узлов с концентратором и работает с сегментами оптоволокна длиной не более 2000 м при общей длине сети не более 2500 м. Максимальное число повторителей — 4. Концентратор в сети может быть активным (содержит электронные схемы для обнаружения и ретрансляции сигналов) или пассивным (с оптикой, расщепляющей световой сигнал – небольшое число каналов).

Стандарт 10Base-FB предназначен для магистрального соединения концентраторов. Он позволяет иметь в сети до 5 повторителей при максимальной длине одного сегмента 2000 м и максимальной длине сети 2740 м. Концентраторы стандарта 10Base-FB могут поддерживать резервные связи, переходя на резервный порт при обнаружении отказа основного. Концентраторы этого стандарта передают данные и сигналы простоя линии синхронно, поэтому биты синхронизации кадра не нужны, и они не передаются. Поэтому стандарт 10Base-FB, называют также синхронный Ethernet. Стандарты 10Base-FL и 10Base-FB не совместимы между собой.

Стандарт 10 Base FP (Fiber Passive) предназначен для обеспечения взаимодействия конечных узлов локальной сети с использованием принципа пассивного оптического разветвителя. Стандарт позволяет обеспечить взаимодействие 33 рабочих станций находящихся на удалении до 500 м.

Ограничения для Ethernet 10Base-FL приведены в табл. 6.4.

Таблица 6.4. Ограничения для Ethernet 10Base-FL

Максимально допустимое число сегментов	1024
Максимальное число сегментов с узлами	1024
Максимальная длина сегментов	2000 м.
Максимальное число узлов на сегмент	2
Максимальное число узлов в сети	1024
Максимальное число концентраторов в цепочке (между двумя компьютерами)	4

Достоинства и недостатки сети 10Base-FL обусловлены достоинствами и недостатками оптоволоконной технологии (см. п. 5.13. 3). Из-за низкой скорости передачи данных сеть 10Base-FL потеряла актуальность. На начальном этапе **она** была привлекательна большим размером сегмента и высокой помехозащищенностью.

6.5. Ethernet 100 Base–T (Fast Ethernet)

Fast Ethernet (быстрый Ethernet, скорость передачи 100 Мбит/с) принят в качестве стандарта 802.3u Комитетом IEEE 802 в мае 1995; использует тот же протокол и то же звездообразное соединение, что и 10BASE–T. Вместе с этим Fast Ethernet имеет более сложную структуру физического уровня, обусловленную тем, что в этом стандарте предусмотрено использование трех вариантов кабельных систем. Передача данных в сети 100 BASE–T может осуществляться как в полудуплексном режиме, так и в полнодуплексном режиме

Стандарт IEEE 802.3u 100 BASE–T специализирует три типа кабеля:

- 100 BASE – T4 (4-х парный кабель UTP категорий 3, 4, 5 либо STP (экранированная витая пара));
- 100 BASE – TX (2-х парный кабель UTP категории 5 или STP);
- 100 BASE – FX (2-х проводной многомодовый оптоволоконный кабель).

Основные достоинства технологии Fast Ethernet:

- увеличение пропускной способности сегментов сети до 100 Мб/с;
- сохранение метода доступа Ethernet;
- сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных – витой пары и оптоволоконного кабеля.

Существенным отличием Fast Ethernet от Ethernet 10BASE-T является то, что в 100 BASE–T между двумя компьютерами допускается не более двух кабельных сегментов, т.е. один концентратор (в то время как в 10 BASE их не более **5).**

6.6. Gigabit Ethernet

Работа над стандартом Gigabit Ethernet (GE) началась в 1995 году. В 1998 году был принят стандарт IEEE 802.3z (1000BASE-SX, 1000BASE-LX и 1000BASE-CX), а в 1999 году – стандарт IEEE 802.3ab (1000BASE-T).

Обобщенные характеристики спецификаций 1000BASE-SX, 1000BASE-LX, 1000BASE-CX приведены в табл. 6.5 – табл. 6.7 соответственно.

Таблица 6.5. Обобщенные характеристики технологии1000BASE-SX

Скорость передачи данных	1000 Мбит/сек
Тип используемого кабеля	(50 или 62.5) мкм
Тип используемого излучателя	850 нм
Максимальная длина сегмента	До 500 м

Таблица 6.6. Обобщенные характеристики технологии 1000BASE-LX

Скорость передачи данных	1000 Мбит/сек
Тип используемого кабеля	5-8 мкм
Тип используемого излучателя	1310 нм
Максимальная длина сегмента	До 5000 м

Таблица 6.7. Обобщенные характеристики технологии 1000BASE-CX

Скорость передачи данных	1000 Мбит/сек
Тип используемого кабеля	STP 150 Ом
Максимальная длина сегмента	До 25 м

Спецификация 1000BASE-SX предполагает использование в качестве передающей среды многомодовое оптоволокно (с короткой длиной волны, S – short); 1000BASE-LX – одномодовое оптоволокно (с длинной волной, L – long). Спецификация 1000Base-CX предполагает использование в качестве среды передачи данных кабель типа экранированную витую пару STP.

Спецификация IEEE 802.3ab 1000 Base-T предполагает использование кабеля UTP категории 5e или категории 6. Для передачи данных используется все 4 пары кабеля UTP. Максимальная длина сегмента 100 метров.

В технологии Gigabit Ethernet сохраняются форматы кадров Ethernet. Внесены изменения в физический уровень. Разрешается передавать несколько кадров подряд, не освобождая физическую среду. В Gigabit Ethernet используется метод кодирования, построенный по тому же принципу, что и код 4B/5B в сети FDDI, позволяющий сохранить самосинхронизацию и не требующий удвоения полосы частот, как в случае манчестерского кода. Передача данных в сети Gigabit Ethernet может осуществляться как в полудуплексном режиме (с сохранением метода доступа CSMA/CD), так и в более быстром полнодуплексном режиме (аналогично сети Fast Ethernet), который обеспечивает отсутствие конфликтов.

Основные достоинства Gigabit Ethernet:

1. Низкая стоимость по сравнению с другими технологиями.

2. Низкие затраты на обучение персонала, в сравнении с другими технологиями.

3. Поддержка стандарта многими производителями.

4.Соединение коммутаторов Fast Ethernet по Gigabit Ethernet позволяет резко увеличить пропускную способность магистрали ЛВС.

5. Установка сетевой платы Gigabit Ethernet на сервер дает возможность расширить канал с сервером и увеличить производительность пользователей мощных рабочих станций.

6.Простота перехода от существующих сетей к Gigabit Ethernet.

7. Низкие эксплуатационные затраты.

Стандарт Gigabit Ethernet находит применение в корпоративных сетях (см. рис. 6.5). Нижние уровни таких сетей работают на 100 Мбит/с и ниже, а магистральные и их объединения на Gigabit Ethernet. технология Gigabit

Ethernet позволяет увеличить скорость передачи в восемь (при замене ATM, работающей на скорости 155 Мб/с) или в 10 раз (при замене Fast Ethernet). Стандарт Gigabit Ethernet используется также для построения городских оптических сетей.

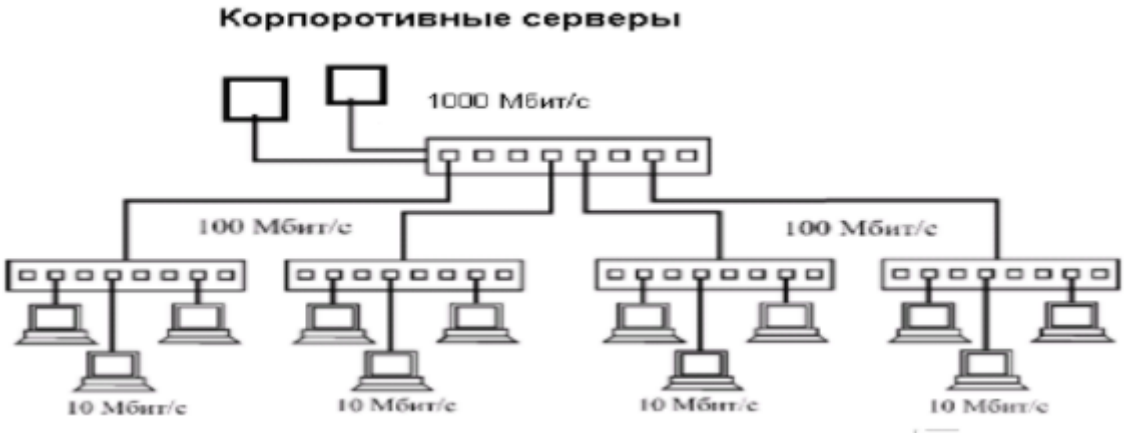

Рис. 6.5. Применение технологии Gigabit Ethernet

Развитие GE привело к появлению маршрутизирующих коммутаторов (малое время задержки; 7 млн. пакетов в секунду при маршрутизации и коммутации) и стало хорошей альтернативой дорогостоящей технологии ATM.

6.7. 10 Gigabit Ethernet

Технология 10 Gigabit Ethernet (10GE) обеспечивает передачу данных со скоростью 10 Гбит/с. Стандарт **IEEE 802.3ae** (утвержден 15 июня 2002 г.) определяет для оптоволокна три семейства физических уровней: **10GBASE-X, 10GBASE-R и 10GBASE-W**. Эти семейства различаются методами кодирования, наличием или отсутствием интерфейса WAN для согласования с сетями SONET OC-192, а также реализацией PMD (Physical Medium Dependent), отвечающего за передачу сигналов в физической среде.

10GBASE-X использует схему кодирования сигнала 8 b/10. Подуровни интерфейса WAN отсутствуют. 10GBASE-X предусматривает одну спецификацию PMD: 10GBASE-LX4**.**

10GBASE-R базируется на схеме кодирования 64 b/66 b. Имеет подуровень интерфейса WAN и три типа PMD: 10GBASE-SR, 10GBASE-LR и 10GBASE-ER**.**

10GBASE-W определяет инкапсуляцию 64b/66 b-кодированных данных во фрейм SONET OC-192. Имеет следующие спецификации PMD: 10GBASE-SW, 10GBASE-LW **и** 10GBASE-EW**.**

Максимальная дина сегмента (оптической линии) зависит от вида оптоволокна, а так же от типа излучателя и изменяется от 65 метров для 10GBASE-SR до 40 000 м для 10GBASE-EW.

Существует также стандарт 10 Gigabit Ethernet по меди (IEEE 802.3ak): 10GBASE-CX4. Он применяется в центрах обработки данных (на расстояния до 20 метров). Двунаправленный канал образуется с помощью 4-х отдельных экранированных пар в каждом направлении. Применение этого стандарта в

центрах обработки данных обусловлено дороговизной оптических трансиверов (до 15 тыс. долларов).

В 10GE не применяется метод CSMA/CD, который сдерживал производительность сетей Ethernet. Физический уровень стандарта 10GE имеет интерфейс как для локальных, так и интерфейс для глобальный сетей. Последний интерфейс по существу является расширением первого. Различие между этими интерфейсами проявляется лишь на уровне кодирования.

10GE в основном ориентирован на крупные транспортные и магистральные сети и может применяться для объединения локальных сетей офисов (расположенных на расстоянии до 40 километров друг от друга). Объединение локальных сетей удаленных офисов с использованием 10GE может быть реализовано двумя способами:

- Темное волокно (Dark Fiber).
- Технология оптического мультиплексирования (DWDM) .

В первом случае оптическое волокно используется для подключения офисов по принципу точка–точка. Поэтому для образования структуры, которая обеспечивает связь каждого компонента с каждым, потребуется дополнительные линии и дополнительные порты.

Использование технологии DWDM (см. п. 1.5) позволяет существенно уменьшить затраты на построение структуры каждый–с каждым. В данном случае удаленные офисы подключаются к кольцу (оптическому облаку), по которому передается одновременно несколько информационных потоков. Один из этих кольцевых потоков используется для организации виртуального информационного канала между подразделениями.

Существенной особенностью стандарта IEEE 802.3ae является способность оборудования 10GE взаимодействовать с сетями SONET/SDH. Так что имеется возможность передавать пакеты Ethernet по каналам SONET/SDH. В результате экспансия технологии Ethernet на распределенные городские сети, которая началась с появлением стандарта Gigabit Ethernet, теперь распространятся и на глобальные сети.

6.8. Сеть 100VG-AnyLan

Эта сеть имеет скорость передачи данных 100 Мб/с и комбинирует элементы сетей Ethernet и Token Ring. ПУЛК (LLC) сети 100VG-AnyLAN соответствует стандарту IEEE 802.2, а ПУДС (MAC) -- специально разработанному стандарту 802.12 (1995 г.). Основное отличие данной сети от других ЛС заключается в методе доступа. В технологии 100VG-AnyLAN определены новый метод доступа DDP (Demand Priority Protocol) и новая схема квартетного кодирования Quartet Coding. Метод доступа DDP позволяет, в отличие от метода доступа Ethernet, обеспечить отсутствие коллизий, а в отличие от маркерного метода доступа Token Ring – сократить время доступа (за счет исключения задержек маркера на его вращение по кольцу).

Корневой (родительский) концентратор (см. рис. 6.6), связан с узлами сети по топологии «звезда» и представляет собой интеллектуальный контроллер, который циклически сканирует порты, проверяя наличие запросов на передачу кадров. Концентратор принимает кадр от узла, выдавшего запрос, и передает его по адресу.

При наличии на всех абонентских системах (АС) запросов только одного уровня приоритета (высокого или обычного) обслуживание заявок осуществляется в следующем порядке (рис. 6.6):

AC_{11} -> AC_{21} -> AC_{22} -> AC_{23} -> AC_{24} -> AC_{13} -> AC_{14}

AC_{11} -> AC_{21} -> AC_{22} -> AC_{23} -> AC_{24} -> AC_{13} -> AC_{14}

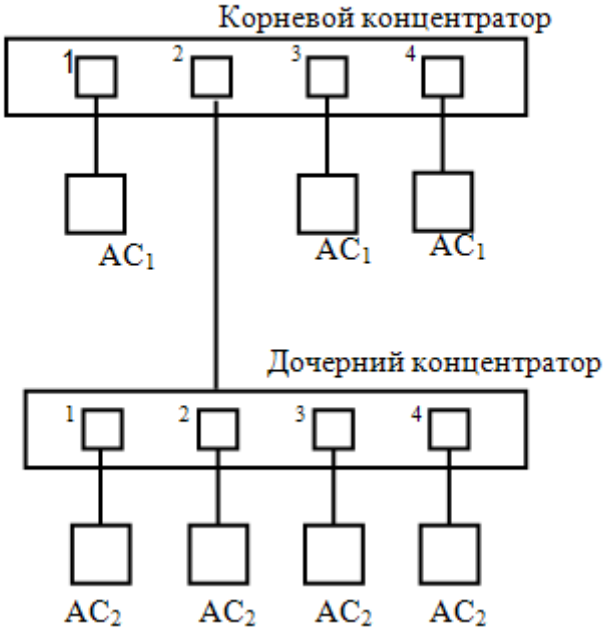

Рис. 6.6. Конфигурация сети 100VG-AnyLAN

Если же будет послан запрос с более высоким приоритетом, то концентратор обслужит высокий приоритет вне очереди, а затем продолжит работу по вышеописанному алгоритму.

Каждый концентратор (допускается каскадирование до 5 уровней) может быть сконфигурирован на поддержку либо кадров Ethernet (802.3), либо кадров Token Ring (802.5). Все концентраторы, расположенные в одном и том же логическом сегменте должны быть сконфигурированы на поддержку кадров одного типа. Для соединения логических сегментов 100VG-AnyLAN, использующих разные форматы кадров, нужен мост, коммутатор или маршрутизатор. Максимальный размер сети составляет 8000 м, длина сегмента для UTP 5 категории 200 м, для оптоволокна — 2000 м.

6.9. Локальная сеть Token Ring

Сеть Token Ring разработана фирмой IBM в 1970-х годах. Она практически идентична спецификации IEEE 802.5, в основу которой положен маркерный метод доступа Token Ring (см. п.3.1). Сети Token Ring работают с двумя скоростями: 4 Мбит/с и 16 Мбит/с. Первая скорость (4.16 Мбит/с)

заложена в стандарте 802.5, а вторая является стандартом де-факто (результат модернизации технологии Token Ring).

Сеть Token Ring рассчитана на кольцевую топологию или топологию физической звезды с логическим кольцом, оконечные станции которой подключаются к концентраторам MSAU (Multi Station Access Unit), см. рис. 6.7.

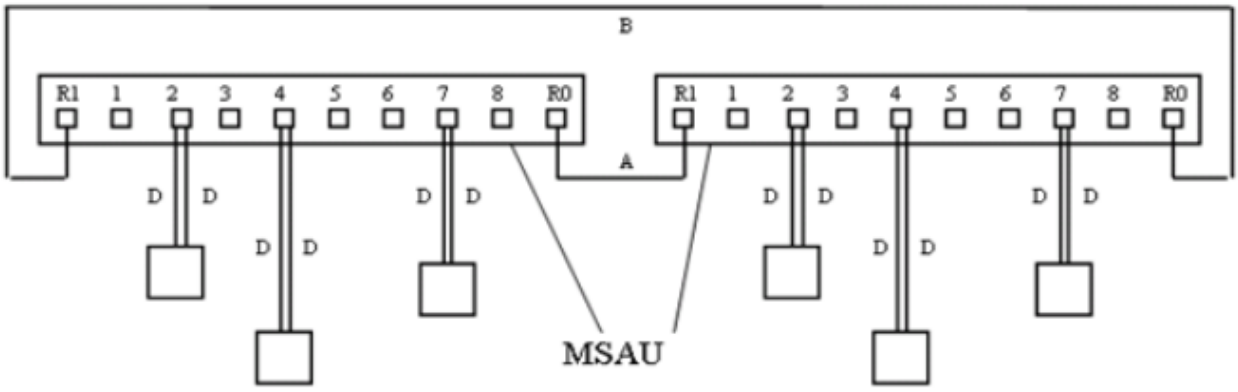

Рис. 6.7. Конфигурация сети Token Ring.

Устройства многостанционного доступа MSAU, объединяются друг с другом, образуя кольцо, при этом если станция отключится, то MSAU зашунтирует ее, обеспечивая прохождение пакетов. Стандарт IEEE 802.5 (в отличие от Ethernet) гарантирует стабильность пропускной способности. Сети Token Ring имеют встроенные средства диагностики, они более приспособлены для решения задач реального времени, но в то же время и более дороги.

Стандарт IEEE 802.5 использует систему приоритетов, которая позволяет некоторым станциям пользоваться сетью чаще остальных. Для этих целей кадры IEEE 802.5 имеют в поле управления доступом биты приоритета и резервирование приоритета (см. п.3.4). Только станции с приоритетом равным или выше, чем приоритет маркера, могут им завладеть. Сети Token Ring имеют несколько механизмов для обнаружения и предотвращения влияния сетевых сбоев и ошибок.

Ограничения на сети Token Ring приведены в табл. 6.8.

Таблица . 6.8. Ограничения на сети Token Ring

Тип кабеля	UTP, STP, оптоволокно
Максимальное количество MSAU	33
Максимальное расстояние между узлами	Для UTP – 45,5 м, оптоволокно и STP – до 100 м
Максимальная длина соединительного кабеля между MSAU	Для UTP – 45,5 м, оптоволокно и STP – 200 м

Минимальная длина кабеля, соединяющего MSAU (A)	2,5 м
Максимальная общая длина кабеля, соединяющего все MSAU (A+B)	121,2 м для UTP, для волоконно-оптического кабеля – до нескольких км

Для подключения к магистральному кабелю могут использоваться: пассивное устройство (для подключения одной станции), устройства многостанционного доступа (MAU, MSAU), интеллектуальное устройство многостанционного доступа SMAU.

К достоинствам Token Ring относятся:

- высокая надежность сети в условиях
- интенсивной перегрузки; наличие встроенных механизмов диагностики и восстановления;
- упрощенное подключение Mainframe IBM к локальной сети.

Недостатки сети: дорогое оборудование, сложность в диагностике и высокая профессиональная подготовка обслуживающего персонала.

6.10. Сети FDDI

В основе сети лежит набор сетевых стандартов ANSI X3T9.5 (неформально закрепилось название FDDI — Fiber Distributed Data Interface). FDDI обеспечивает широкополосную передачу данных по оптоволоконному кабелю со скоростью 100 Мбит/с. В последующем стандарт FDDI был признан в качестве международного стандарта ISO 9314.

Сеть FDDI по существу представляет собой усовершенствованную Token Ring. В сети FDDI (см. рис. 6.7) используется два кольца с циркуляцией маркеров в противоположных направлениях, что позволяет FDDI работать вопреки отказам сети. Максимальная длина сети (без мостов) 200 км (100 км на кольцо); максимальное расстояние между узлами 2 км; максимальное количество узлов 500.

При отказах устройства или при разрыве кабеля одно из колец будет разорвано. В этом случае данные маршрутизируются во вспомогательное кольцо и направляются по нему в противоположное направление. При достижении разрывов в сети маршрутизация изменится на обратную.

В FDDI применяется более сложный метод доступа к сети, чем в Token Ring. Как и в Token Ring, по кольцу передается маркер, и владельцу маркера разрешается передавать кадры FDDI. В отличие от Token Ring, в сети FDDI может одновременно циркулировать несколько кадров. Владельцу маркера разрешается передавать следующий кадр, не дождавшись возвращения первого кадра, при этом владельцу маркера разрешается после передачи

своего кадра освободить маркер и передать его следующей станции в кольцо, не дожидаясь полного оборота маркера по кольцу.

В сетях FDDI может использоваться метод резервирования регулярных интервалов передачи для отдельных станций (так называемый синхронный режим передач). В такие регулярные интервалы отправлять данные могут только эти станции (им не надо захватывать маркер). Это факультативное средство стандарта FDDI.

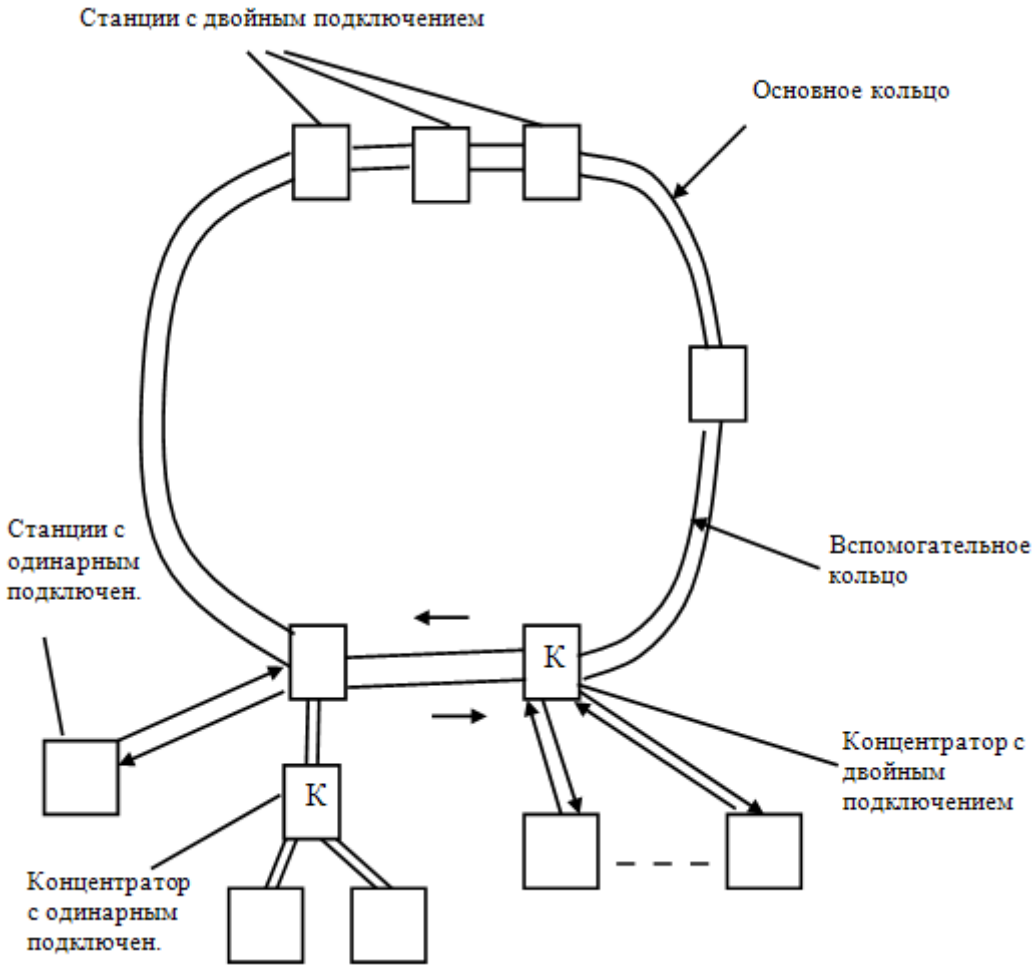

Рис. 6.7. Конфигурация сети FDDI

В сетях FDDI могут использоваться и так называемые многокадровые диалоги (факультативное средство). Они позволяют станции с маркером передавать ограниченный маркер (маркер, допускающий ответ только станции – отправителю). Такой маркер посылается конкретной станции, которой разрешается передавать ограниченные маркеры и кадры первой станции.

Большинство сетевых технологий в настоящее время поддерживают оптоволоконные кабели в качестве одного из вариантов физического уровня, однако FDDI остается наиболее отработанной высокоскоростной, прошедшей проверку технологией.

6.11. Сети ATM

В технологии асинхронного режима передачи данных ATM (Asynchronous Transfer Mode) данные любой природы передаются пакетами (ячейками) фиксированной и малой длины (53 байта, 5 из которых занимает заголовок; вместо адресов в этих ячейках указывается маршрут потока данных). Небольшая длина пакетов позволяет обеспечить небольшие задержки при передаче пакетов, требующих постоянного темпа передачи, характерного для мультимедийного трафика.

Сеть ATM является коммутируемой с соединениями точка-точка, ее структура похожа телефонную сеть (конечные станции соединяются с коммутаторами нижнего уровня, которые в свою очередь соединяются с коммутаторами более высоких уровней и т.д.). В этой сети существует 2 типа каналов: постоянный виртуальный канал (канал, который создается между коммутатором один раз и обслуживает все коммуникации между двумя устройствами) и временный канал, устанавливаемый только на период обмена данными между устройствами. В ATM используются волоконно-оптические кабели или витая пара 5-й категории.

Сети ATM хорошо масштабируются и обеспечивают скорости передачи данных в диапазоне от 25 Мбит/с до 39.81 Гбит/с (см. табл. 6.9). Такой широкий диапазон скоростей позволяет применять ATM в самых различных конфигурациях сетей. При совместном использовании технологий ATM и SONET (для передачи трафика сети ATM) скорость передачи может достигать 39.81 Гбит/с.

Таблица 6.9. Скорости передачи данных ATM.

Поставщики коммуникационных услуг: T1/E1	1.544/2.048 Мбит/с
ATM – 25	25 Мбит/с (по витой паре)
Поставщики телекоммуникационных услуг T3/E3	44.736/34.368 Мбит/с
OC – 1 SONET	51.84 Мбит/с
OC – 3 SONET	155 Мбит/с
OC – 12 SONET	622 Мбит/с
OC – 48 SONET	2,4 Гбит/с
OC – 192 SONET	9.953 Гбит/с
OC – 768 SONET	39.81 Гбит/с

Сетевая технология ATM находит применение в магистральных и корпоративных сетях. Однако ATM является дорогой и сложной технологией, требующей высокой квалификации обслуживающего персонала.

Нишу, занимаемую ATM, сильно потеснили технологии Gigabit Ethernet и 10Gigabit Ethernet, которые примерно раз в пять дешевле ATM и сравнительно просты в эксплуатации.

Тема 7. Программные средства компьютерных сетей

7.1. Классификация сетевых программных средств

Программное обеспечение (ПО) компьютерной сети включает определенную совокупность программных средств, которые необходимы для коллективного доступа к ресурсам этой сети, а также реализации сетевых служб и эффективного управления сетевыми ресурсами. ПО сети включает следующие компоненты:

- общее (базовое) ПО, составляемое базовым ПО компьютеров, входящих в состав сети;
- системное сетевое ПО, которое состоит из программных средств, обеспечивающих необходимое взаимодействие компонентов сети;
- специальное ПО, обеспечивающее реализацию задач, связанных со спецификой предметной области и обусловленные целевым назначением компьютерной сети.

Системное сетевое ПО сети создается посредством использования сетевых операционных систем, драйверов, программных средств маршрутизаторов и шлюзов, сетевых утилит (операционных утилит, утилит администрирования и смешанных утилит.)

Центральную роль в компьютерной сети играет системное сетевое программное обеспечение, функции которого реализуются распределенной операционной системой сети, содержащей набор управляющих и обслуживающих программ. Распределенная операционная система обеспечивает: организацию связей между прикладными программами, реализуемыми в узлах компьютерной сети; доступ прикладных программ к ресурсам сети; синхронизацию работы прикладных программных средств; обмен информацией между программами; выполнение терминальных команд и т. д.

7.2. Сетевые операционные системы

Компьютер в локальной сети, участвуя в сетевом взаимодействии, «вынужден» терять часть своей автономии. При этом программные средства компьютера, участвующие в сетевом взаимодействии, составляет часть сетевой операционной системы в широком смысле слова. Так что под сетевой операционной системой в широком смысле понимают совокупность операционных систем отдельных компьютеров, обеспечивающих обмен сообщениями и разделение ресурсов по единым правилам (протоколам). В узком же смысле слова сетевая ОС (NOS — Network Operating System) — это такая операционная система отдельного компьютера, которая обеспечивает ему реализацию необходимых сетевых функций и взаимодействий (совместную работу с файлами и приложениями, разрешение конфликтов, маршрутизацию и т.д.)

Вначале сетевые ОС создавались как надстройка над базовой ОС (минимум необходимых сетевых функций встраивался в базовую ОС, как,

например, в старших версиях MS DOS). На этом же принципе построены и такие сетевые ОС, как LANtastic, Personal Ware и др. В последующем появились сетевые ОС, изначально предназначенные для работы в сети. У этих сетевых ОС сетевые функции органически встроены в архитектуру ОС. Это обеспечивало таким сетевым ОС логическую стройность, высокую производительность, простоту модификации и эксплуатации. Примерами таких ОС являются семейство сетевых ОС Novell NetWare, Windows NT фирмы Microsoft. сетевые ОС

Сетевые операционные системы делятся на одноранговые и двухранговые (или серверные). Сеть, на компьютерах которой установлены одноранговые ОС, обеспечивает этим компьютерам потенциально равные сетевые возможности. Ресурс любого из этих компьютеров, объявленный разделяемым, становится доступным всем компьютерам сети. Примеры одноранговых сетевых ОС: ОС LANtastic, Personal Ware, Windows for Workgroup, Windows NT Workstation, Windows 95, Windows 98, Windows 2000 Professional, Windows XP, Windows Vista, Windows 7. Серверные сетевые ОС, которые устанавливаются на одном или нескольких компьютерах сети, обеспечивают централизованный доступ к ресурсам этих компьютеров. К таким сетевым ОС относятся: семейство Banyan Vines, семейство Novell NetWare, IBM LAN Server, Sun NFS, Windows NT Server, Windows 2000 Server (семейство), Windows 2003 Server (семейство), Windows 2008 Server (семейство).

Семейство сетевых ОС фирмы Novell содержит версии NetWare 1.x, 2.x, 3.x, 4.x, 5.x, 6.x. В основе сетевых протоколов ОС NetWare лежит стек протоколов корпорации Xerox XNS (Xerox Network Systems; конец 1970-х начало 1980 гг.). Этот же стек положен и в основу сетевых протоколов сетевой ОС Banyan VINES. Сетевые ОС NetWare заняли вначале 1990-х существенную долю рынка и выдержали конкуренцию с Windows NT, после выпуска которой прекратили существование многие другие конкурирующие сетевых ОС. Сервера компании Novell отличались высокой надежностью; они могут работать годами без участия человека.

Компанией Novell также разработаны UnixWare (на основе Unix System V; UnixWare продана в 1995 г. компании Santa Cruz Operation; UnixWare 7.1 имеет 7 вариантов), openSUSE (дистрибутив Linux, существует более 600 дистрибутивов Linux), Open Enterprise Server (включает Novell NetWare, openSUSE и пакет сетевых служб). В 2010 году компания Novell была приобретена холдингом Attachmate Group за 2.2 миллиарда долларов.

История развития сетевых технологий в Microsoft берет начало в 1984 г. (программа MSNet в MS DOS v.3.1), но активная игра на рынке сетевых технологий начинается с появлением Windows NT 4.0 (Windows NT Workstation 4.0 и Windows NT Server 4.0), которая имела интерфейс аналогичный Windows 95 (появилась в 1995 г.). ОС Windows 95 обладала возможностями одноранговой сетевой ОС и позволяла работать в Интернет без использования дополнительных программ.

Следующим этапом в развитии сетевых технологий в Microsoft стало появление семейства Windows 2000, которое было разработано на основе Windows NT и унаследовало от нее высокую надежность и защищенность информации. К названному семейству относятся Windows 2000 Server (Windows NT Server 5.0), а также более мощные представители семейства: Windows 2000 Advanced Server и Windows 2000 Datacenter.

Дальнейшее развитие сетевых технологий в Microsoft получило воплощение в семействе ОС Windows Server 2003, которое включает: Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition, Windows Server 2003 Web Edition и Windows Small Business Server 2003. Семейство Windows Server 2003 предназначено для управления сетевыми серверами разного масштаба. Продукты этого семейства существенно различаются по количеству поддерживаемых процессоров, объемов оперативной памяти и целевому назначению.

К семейству ОС Windows Server 2008 относятся: Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition, Windows Server 2008 Datacenter Edition, Windows Server 2008 Web Edition.

7.3.Сетевые операционные системы фирмы Novell

7.3.1. Архитектура сетевой ОС NetWare

Сетевые операционные системы NetWare имеют модульную архитектуру, позволяющую подключать необходимые загружаемые модули. Локальная сеть, в которой установлена операционная система NetWare, включает следующие компоненты:

- Сетевую операционною систему, работающую на сервере.
- Клиентское программное обеспечение, работающее на каждой рабочей станции.
- Службу каталога Novell (базу данных, содержащую информацию о каждом сетевом объекте и ресурсе).
- Служебное программное обеспечение, обеспечивающее доступ к сетевым службам.
- Утилиты операционной системы NetWare, позволяющие системным администраторам и пользователям решать широкий круг задач.
- Драйверы, обеспечивающие взаимодействие различных аппаратных устройств с программным обеспечением компьютеров.
- Маршрутизаторы и шлюзы.

7.3.2. Основные компоненты сетевой среды NetWare

Сетевая операционная система NetWare является системой коллективного пользования. Эффективность ее функционирования во многом зависит от организации (планирования и создания) сетевой среды, основными компонентами которой являются:

- структура пользователей сети,
- структура каталога сети,
- система защиты сети.

Организация сетевой среды осуществляется с использованием специальной базы данных – базы данных объектов сети. Такая база данных имеется на каждом файл-сервере сети. Она содержит список объектов (пользователи, группы, каталоги, файлы и т.д.) и их свойства (пароли, права, сетевые адреса и т.д.). С помощью этой базы данных операционная система NetWare осуществляет управление структурой пользователей сети и организует систему защиты сети.

В NetWare имеются следующие категории пользователей:

1. Супервизор сети(системный администратор сети). Выполняет административные функции в сети. Имеет неограниченные права и может делегировать часть своих функций менеджерам и операторам сети.

2. Менеджеры сети (администраторы групп). Выполняют административные функции, которые делегирует Супервизор сети. Могут управлять группой пользователей либо отдельными пользователями.

3.Операторы сети. Выполняют текущее оперативное управление сетью. В их распоряжении имеются средства управления с консоли сервера, альтернативной или удаленной консолей. Операторы управляют сервером печати и очередями печати в сети.

4.Обычные пользователи сети. Используют ресурсы сети для решения своих задач.

Группы пользователей. В группу обычно включаются:

- пользователи, выполняющие одну и ту же задачу;
- пользователи, работающие в рамках одного проекта;
- пользователи, использующие одни и те же прикладные программы.

Объединение пользователей в группы позволяет упростить функции администрирования сетью (привилегии доступа к ресурсам сети предоставляются группе, а не отдельным пользователям).

С точки зрения системы группа пользователей является таким же объектом, как и пользователь сети. Ей дается определенное имя, и система присваивает ей соответствующий идентификатор в базе данных объектов сети. Как пользователь, так и группа могут быть созданы либо Супервизором, либо менеджерами сети. Они же определяют, какие пользователи могут входить в ту или иную группу, присваивают ей определенные права в каталогах или права доступа к определенным файлам. Пользователь может быть одновременно членом нескольких групп.

Супервизор сети (администратор системы) — это особый пользователь с именем SUPERVISOR. Он несет ответственность за функционирование сети,

организует структуру пользователей сети, создает структуру каталога сети, обеспечивает необходимый уровень системы защиты сети, следит за рациональным использованием ресурсов сети, определяет политику развития сети и выполняет другие административные функции.

Система автоматически создает Супервизора и назначает ему как объекту базы данных сети идентификатор с номером 1, предоставляя ему на файловом сервере неограниченные права, которые не могут быть никем отменены. Супервизор сети может передать часть своих административных функций другим пользователям путем предоставления им эквивалента прав Супервизора. Супервизор сети может делегировать часть своих административных функций менеджерам сети, которые получают супервизорные права только на определенную часть сетевой среды и пользователей сети.

Менеджеры сети. Менеджеры сети выполняют административные функции, которые делегирует им Супервизор сети. Различают два типа менеджеров сети: менеджер среды пользователей и менеджер рабочей группы.

Менеджер среды пользователей (Account Manager) может устанавливать или изменять ограничения, распространяемые на пользователей, назначать им права, устанавливать эквивалент прав и пароли, назначать для них других менеджеров и т.д.

Менеджер рабочей группы (Workgroup Manager) управляет рабочей группой пользователей сети. Он может быть назначен только Супервизором сети, который делегирует ему свои привилегии для управления группой. Менеджер рабочей группы создает свою группу. Он формирует ее состав и наделяет пользователей необходимыми правами. Менеджер рабочей группы автоматически становится менеджером среди пользователей этой группы Менеджер рабочей группы, в отличие от менеджера среды пользователей, может создавать и удалять объекты сети (группы, пользователей). Менеджер рабочей группы может иметь в каталоге только те права, которые ему предоставит Супервизор.

Если же какой-либо пользователь создан Супервизором сети, а не менеджером группы, то только Супервизор становится менеджером среды этого пользователя. И если он не назначит менеджера рабочей группы менеджером среды этого пользователя, то не сможет включать его в свою группу и управлять им.

Пользователь и группа как объекты сети в определенной степени идентичны. Поэтому менеджером рабочей группы может быть назначен как пользователь, так и группа. В последнем случае любой член такой группы становится менеджером группы, и может формировать свою группу. Такой прием позволяет Супервизору упростить работу по созданию аппарата менеджеров сети.

Операторы сети. Операторы сети осуществляют оперативное управление сетью; в их задачи входит выполнение текущей эксплуатационной

работы сети. По умолчанию все операторские функции выполняет Супервизор сети, но он может назначить для реализации этих функций специальных пользователей сети: оператора консоли файлового сервера, оператора сервера печати, оператора очереди печати.

7.3.3. Структура каталога сети

Пользователь сети может хранить свои программы и данные, как на локальных дисках рабочей станции, так и на сетевых дисках файловых серверов сети.

Организация дисковой памяти и файловой системы в NetWare отличаются от их организации в DOS. Но для пользователя, выполняющего свою работу на рабочей станции под управлением DOS, эти отличия в значительной степени скрыты. Для него сетевое дисковое пространство представляется как бы расширением локального дискового пространства рабочей станции. А структура сетевого каталога практически соответствует структуре каталога DOS.

Структура каталога. Основной единицей сетевого дискового пространства является том (Volume). Жесткий диск файлового сервера может содержать несколько дисковых томов. Но дисковый том не ограничивается размером диска, он может перекрывать дисковое пространство нескольких жестких дисков.

Том является логической единицей дисковой памяти. С точки зрения пользователей рабочих станций, он в определенной степени соответствует локальному диску отдельной компьютерной системы. Каждый том имеет каталог, описываемый своей таблицей каталога тома. Структура этого каталога точно такая же, как структура каталога на локальном диске пользователя, она включает каталог, подкаталоги и файлы.

В структуре дискового пространства сети, где может быть несколько файловых серверов, можно выделить следующие уровни сетевого каталога:

- - файловый сервер,
- - том,
- - каталог,
- - подкаталог,
- - файлы.

Термины каталог и подкаталог относительны: каталог является подкаталогом по отношению к каталогу выше его уровнем. Каждый каталог может содержать неограниченное количество подкаталогов; ограничения определяются только лишь имеющимся в наличии объемом доступного пространства.

Начиная с NetWare 4.x, в сетевых продуктах фирмы Novell применяется технология **NDS** (**Novell Directory Services**). NDS содержит объекты трех типов: корень, конечные объекты (сетевые ресурсы: пользователи, серверы и т.д.) контейнеры (объекты, содержащие либо конечные объекты, либо другие

контейнеры). Существует три типа контейнерных объектов: страна, организация, подразделение. В Netware 5 и выше NDS использоваться как для доступа к объектам, так и для обеспечения отказоустойчивости.

В NetWare 6.0 версия NDS 8.5 (eDirectiry) является полностью независимым кросс-платформенным продуктом, который может быть приобретен отдельно и установлен на Windows NT/2K, Linux, Solaris, Unix и Tru64. Создание и управление структурой объектов в NDS 8.5 осуществляется с помощью утилиты ConsoleOne

Посредством ConsoleOne можно создавать, перемещать, переименовывать, удалять и модифицировать любой тип объектов eDirectory, расширять схему дерева, просматривать контейнеры, выполнять поиск или фильтрацию по имени и типу объекта; контролировать наследование прав, управлять файловой системой на томах NetWare, а также расширять возможности Web-сервера и выполнять административные задачи NDS eDirectory через стандартный Web-браузер.

7.3.4. Система защиты сети

Система защиты NetWare имеет следующие уровни:

1. Защита входа в сеть с использованием списка имен и паролей.
2. Защита файлов и каталогов с предоставлением прав пользователю.
3. Защита файлов и каталогов с использованием их атрибутов.
4. Защита доступа к файловому серверу с консоли.
5. Защита ресурсов сети.

Защита входа в сеть (Login Security). Организацию защиты входа в сеть осуществляют Супервизор и менеджеры, которые назначают пользователям сети имена, пароли и устанавливают определенные ограничения на вход в сеть.

Имена пользователей (User name) являются основой системы защиты на первом уровне. Для входа в сеть пользователь должен ввести свое имя и пароль. Пароли пользователей (Passwords) являются опционными. Пароль может быть назначен пользователю Супервизором или менеджером или введен самим пользователем.

Защита файлов и каталогов с предоставлением прав пользователям сети. На этом уровне защиты определяется доступ пользователя к каталогам и файлам с предоставлением ему необходимых прав для работы. Это осуществляется путем назначения пользователям Опекунских прав (Trustee Rights Assignments) и установки Маски унаследованных (Inherited Rights Mask) в соответствующих каталогах.

Опекунские права дают возможность пользователю выполнять определенные действия с файлами и каталогами. Они могут быть предоставлены на уровне каталога или на уровне файла. Если опекунские права даются пользователю на уровне каталога, то они распространяют свое действие на все файлы в этом каталоге. На уровне же файлов - относятся

только к определенным файлам. Опекунские права могут быть предоставлены как пользователю, так и группе. В последнем случае эти права, группе распространятся на всех пользователей данной группы.

Опекунские права пользователя в каталоге автоматически распространяется на его подкаталоги. Для этих целей в NetWare введен механизм управления наследованием прав в подкаталогах — **Маска унаследованных прав** (Inherited Rights Mask).

В системе имеется восемь прав, каждое из которых имеет название и идентифицируется соответствующей буквой.

S	Supervisory	Супервизорные
R	Read	Чтение
W	Write	Запись
C	Create	Создание
E	Erase	Удаление
M	Modify	Модифицирование
F	File Scan	Сканирование файлов
A	Access Control	Управление доступом

Права в каталоге отображаются строкой вида **[SRWCEMFA]**, в которой буквы соответствуют назначенным правам. Права в каталоге имеют следующее действие.

Супервизорные. Предоставляют пользователю все права в каталоге, его файлах и его подкаталогах независимо от того, какие ограничения в подкаталогах вносит Маска унаследованных прав. Значение прав Супервизорные в Маске не может быть отменено никем, и это право распространяется на все подкаталоги.

Чтение. Предоставляет право открывать файлы в каталоге читать их содержимое или запускать программы.

Запись. Дает право открывать и модифицировать файлы.

Создание. Позволяет создавать файлы и подкаталоги в каталоге. Пользователь может создать файл, открыть его и записать в него информацию. Но после того, как файл будет закрыт, пользователь не сможет видеть его и писать в него, если ему не предоставлены такие права.

Удаление. Дает право удалять каталог, его файлы, его подкаталоги и файлы в них.

Модифицирование. Позволяет изменять атрибуты каталога и файлов, переименовывать каталог и файлы. Но оно не предоставляет право модифицировать содержимое файла.

Сканирование. Дает право пользователю видеть файлы и подкаталоги файлов данного каталога.

Управление. Дает право пользователю назначать и модифицировать опекунские права в данном каталоге и в его файлах другим пользователям, а также модифицировать Маску унаследованных прав в них. Пользователем могут устанавливаться любые права, кроме Супервизорных.

Права доступа к файлам назначаются для определенных файлов в каталоге. Обычно это нужно чтобы изменить какие-либо из прав доступа к некоторым файлам, предоставленных пользователю на уровне каталога. Права доступа к файлам позволяют выполнять следующие действия.

Супервизорные. Предоставляют пользователю все права доступа к файлу. Пользователь, имеющий это право, может давать любые права доступа к этому файлу другим пользователям.

Чтение. Позволяет открывать, читать и выполнять файл.

Запись. Дает право открывать и выполнять запись в файл

Создание. Дает возможность восстановить (Salvage) файл после его удаления.

Удаление. Дает возможность удалить файл.

Модифицирование. Дает право изменения атрибутов файла и его переименования.

Сканирование. Дает право видеть файл при выдаче списка файлов каталога. Если такое право доступа к файлу предоставляется пользователю в одном из подкаталогов, он может видеть всю цепочку подкаталогов, ведущую к корневому каталогу.

Управление доступом. Позволяет изменять значение права доступа к файлу и Маску унаследованных прав. Дает возможность пользователю предоставлять другим пользователям все права доступа к этому файлу, кроме Супервизорных.

Действительные эффективные права (Effective rights) определяют те реальные права, которые пользователь имеет в каталоге или файле. Действительные права в подкаталоге определяются как результат операции логического умножения действительных прав в родительском каталоге (учитывая групповые права в этом каталоге) на Маску унаследованных прав. Действительные права доступа к отдельным файлам определяются аналогичным образом.

Защита файлов и каталога с использованием их атрибутов.

Атрибуты файла и каталога являются средством их защиты. Они и имеют более высокий приоритет по отношению к действительным правам пользователей. Так, например, если файл имеет атрибут **Только для Чтения**, то даже в случае, если пользователь имеет право **Записи** в этот файл, он не сможет это сделать (ему будет доступно только чтение этого файла). Список атрибутов файлов и атрибутов каталога приведен в табл. 7.1 и табл. 7.2 соответственно.

Таблица 7.1. Список атрибутов файлов

Архивируемый	Archive needed	A
Некопируемый	Copy Inhibit	C
Неудаляемый	Delete Inhibit	D

Только для исполнения	Execute Only	X
Скрытый	Hidden	H
Индексный	Indexed	I
Стираемый	Purge	P
Контролируемый по чтению	Read Audit	Ra
Только для чтения/ чтение запись	Read Only/ read write	Ro/Rw
Непереименуемый	Rename Inhibit	R
Разделяемый	Shareable	S
Системный	System	Sy
Транзактный	Transactional	T
Контролируемый по записи	Write Audit	Wa

Таблица 7.2. Список атрибутов каталога

Неудаляемый	Delete Inhibit	D
Скрытый	Hidden	H
Стираемый	Purge	P
Непереименуемый	Rename Inhibit	R
Системный	System	Sy

Архивируемый. Атрибут Архивируемый (более соответствует смыслу Требующий Архивирования) может быть(Archive Needed) назначен только для файлов. NetWare автоматически назначает этот атрибут любому файлу , который был модифицирован после его последнего резервного копирования (Back Up). Этот атрибут соответствует биту Archive в DOS.

Некопируемый. Этот атрибут может быть назначен только для файлов. Даже если пользователи имеют права Чтения и Сканирования файлов в каталоге или на уровне файлов, они не смогут копировать файл с таким атрибутом.

Неудаляемый. Этот атрибут может быть назначен каталогам и файлам. Он не позволяет пользователям удалять каталоги и файлы, даже если им предоставлено право Удаления на уровне файла или на уровне

каталога. Если пользователям было предоставлено право Модификации, они могут удалить атрибут Неудаляемый и только затем уже удалить файл или каталог.

Только для исполнения. Атрибут может быть назначен только для файлов. Этот атрибут защищает программы от копирования. Только Супервизор может назначить этот атрибут файлу, но даже он не может удалить его. Атрибут **Только для исполнения** следует назначать файлу, если существует резервная копия его. Утилиты резервного копирования не копируют файлы с таким атрибутом. Некоторые программы с таким атрибутом не будут правильно выполняться.

Скрытый. Атрибут Скрытый может назначаться каталогам и файлам. Этот атрибут позволяет скрыть файл или каталог от сканирования командой DOS DIR и запрещает удалять или копировать его. Однако, файлы и каталоги с таким атрибутом могут сканироваться командой NetWare NDIR, если пользователь имеет право Сканирования файла.

Индексный. Этот атрибут может назначаться только для)файлов. NetWare автоматически назначает этот атрибут, когда файлы имеют свыше 64 элементов в FAT-таблице. Индексирование увеличивает скорость доступа к большим файлам.

Стираемый. Атрибут Стираемый может быть назначен каталогам и файлам. Когда он назначается файлам, файл стирается во время его удаления (т.е. полностью удаляется с дисковой памяти). Когда этот атрибут назначается каталогу, все файлы, удаляемые в этом каталоге, сразу же стираются.

Контролируемый по чтению. Атрибут назначается только для файлов и непосредственно связан с системой NetWare Audit Trail System, которая осуществляет контролирование обращений к файлам по записи и по чтению. В контрольных файлах системы сохраняется информация о том, кто читает и записывает в файлы базы данных. Сохранение информации о записи в файлы делает возможным длительное резервное копирование файлов, а комбинация информации контроля по записи и по чтению файлов обеспечивает более высокую степень их защиты.

Только для чтения. Атрибут назначается только для файлов. При его назначении файлу автоматически назначается также атрибуты **Неудаляемый** и **Непереименуемый,** так что, пользователи не могут писать, удалять или переименовывать файл, даже при наличии права **Чтения Записи** и **Удаления** на уровне каталога или файла.

Непереименуемый. Атрибут может быть назначен каталогам и файлам. Этот атрибут не позволяет пользователям переименовывать каталоги и файлы.

Разделяемый.. Атрибут назначается файлам, которые используются несколькими пользователями; для программных файлов используется в комбинации с атрибутом **Только для чтения**.

Системный. Атрибут может быть назначен и каталогам, и файлам. Файлы и каталоги с таким атрибутом не могут сканироваться с помощью команды DOS DIR,но они могут сканироваться командой NDIR, если пользователь имеет право Сканирования файлов.

Транзактный. Атрибут может быть назначен только файлам. Этот атрибут указывает на защиту файлов системой TTS. Система TTS обеспечивает корректное выполнение транзакций, что защищает файлы данных от разрушения.

Контролируемый по записи Атрибут может быть назначен только для файлов.

Средства защиты NDS. Основным понятием в системе защиты NDS является опекун (объект, имеющий какие-либо права на другой объект). Каждый объект NDS имеет свойство ACL (Access Control List — список опекунов объекта), в котором хранятся имена всех опекунов и их права. Существует два типа прав: права на объект и права на его свойства. Так, например, пользователь может иметь право удалить объект, но не иметь права просматривать свойства этого объекта.

В NDS существует пять прав на объект:

Supervisor (S). Дает все права на объект (опекун с правом Supervisor имеет доступ ко всем свойствам объекта).

Browse (B). Дает право просмотра объекта в каталоге.

Create (C). Дает право создания новых объектов ниже данного объекта в дереве каталога (действует только для контейнерных объектов)

Delete (D). Дает право на удаление объекта из каталога

Rename (R). Дает право на переименование объекта.

Защита ресурсов сети

Супервизором или менеджером могут быть установлены ограничения, связанные с использованием ресурсов сети. К таким ограничениям относятся:

- ограничения на время работы пользователя (дни недели и часы);
- ограничения на место работы пользователя (количество станций, с которых пользователь может войти в сеть);
- бюджетные ограничения.

На файл-сервере может быть включена функция учета бюджетов. В этом случае, по установленным тарифам с пользователей взимается плата за услуги (количество информации, прочитанной или записанной на диск, количество запросов, сделанных рабочей станцией и т.д.). Система периодически проверяет остаток средств на счету пользователя и отключает его от сети при превышении размеров кредита.

7.3.5. Novell Open Enterprise Server 2

Open Enterprise Server 2 (OES 2) имеет встроенные сервисы операционной системы NetWare 6.5, обеспечивает 64-битную поддержку, поддерживает виртуализацию и корпоративные системы хранения данных. В основу OES 2 «положена» ОС Suse Linux Enterprise Linux 10 SP1. Позиционируется OES 2 как полноценная замена Novell NetWare и Windows Server 2003.

В OES 2 осуществлен окончательный перевод служб NetWare на Linux. Novell Open Enterprise Server 2 позволяет исполнять NetWare 6.5 в качестве гостевой операционной системы на SUSE Linux Enterprise Server 10; которая позволяет исполнять на одном физическом сервере множество отдельных виртуальных машин с использованием технологии виртуализации на базе Xen.

Службы Domain Services for Windows обеспечивая авторизацию и аутентификацию пользователей на сервере, позволяет клиентам Windows обращаться к серверу Novell с применением стандартных протоколов Windows. Кроме того, эта же служба позволяет работать в среде Windows, пользуясь преимуществами служб и технологий Novell без установки на рабочую станцию Novell Client.

7.4. Сетевые технологии компании Microsoft

7.4.1. Понятие Windows NT и сетевые технологии компании Microsoft

Во второй половине 90-х гг. прошлого века содержание понятия Windows NT включало два вида операционных систем. Первый вид ориентирован на роль клиента, второй – на роль сервера сети. Для четвертой версии **(**Microsoft становится активным игроком на рынке сетевых технологий) это, соответственно, – Windows NT Workstation 4.0 и Windows NT Server 4.0.

Изделия пятой версии Windows NT вначале назывались Windows NT Workstation 5.0 и Windows NT Server 5.0; но в последующем стали называться Windows 2000 Professional и Windows 2000 Server соответственно. К семейству серверов этой версии относятся также и более мощные системы Windows 2000 Advanced Server и Windows 2000 Datacenter.

Дальнейшее развитие сетевых технологий в Microsoft (см. п.7.2) получило воплощение в семействах ОС Windows Server 2003, и Windows Server 2008.

7.4.2. Регистрация в Windows NT

Для получения доступа к ресурсам сети пользователь должен зарегистрироваться (идентифицировать себя в домене или на компьютере). Для успешной регистрации необходимо в диалоговом окне **Logon Information** (Вход в систему) ввести в полях **User Name** и **Password** учетную запись пользователя (имя пользователя, присвоенное администратором) и пароль (пароль, присвоенный учетной записи). В поле **Domain** (домен) необходимо выбрать имя домена, в котором находится учетная запись пользователя, или имя локального компьютера. Если компьютер входит в состав рабочей группы, то поле Domain содержит только имя локального компьютера. Имя пользователя и пароль должны содержаться в локальной базе данных каталогов. Аутентификация учетных записей пользователей возможна только в этой базе данных.

Для успешной регистрации пользователь должен указать правомочную глобальную или локальную учетную запись. Если пользователь указывает правомочную глобальную учетную запись, то имя пользователя и пароль проверяются контроллером домена. Если же пользователь указывает правомочную локальную учетную запись, то имя пользователя и пароль проверяются локальным компьютером. Пользователь может зарегистрироваться в домене или на локальном компьютере с любого компьютера, работающего под управлением Windows NT Server, только если администратор присвоил ему привилегию **Logon Locally** (Локальная регистрация) или пользователь сам имеет полномочия администратора сервера.

Важным средством безопасности системы является использование комбинации клавиш Ctrl+Alt+Delete, открывающей доступ к диалоговому окну Windows NT Security (Безопасность Windows NT), которое включает следующие средства:

Lock Workstation (Блокировка) — позволяет блокировать компьютер без выхода из системы. Все программы при этом продолжают работать. Для разблокирования необходимо ввести свой пароль.

Change Password (Смена пароля) — позволяет пользователю изменить пароль своей учетной записи. .

Logoff (Выход из системы) — осуществляет выход пользователя из системы, при этом операционная система Windows NT продолжает работать и пользователи сети могут по-прежнему подключаться к данному компьютеру и использовать его ресурсы.

Task Manager (Диспетчер задач) — содержит список приложений и процессов, работающих в данный момент. Task Manager позволяет получить и ряд других сведений (загруженность процессора и памяти, использование программами ресурсов процессора и памяти и т.д.).

Shut Down (Выключение системы) — закрывает все файлы, сохраняет все данные операционной системы и подготавливает компьютер к отключению питания.

Cancel (Отмена) — закрывает диалоговое окно Windows NT Security.

7.4.3. Администрирование сети Microsoft Windows NT 4.0

7.4.3.1. Операционные системы Windows NT 4.0

Операционная система Windows NT Workstation 4.0 специфицирована на применение в качестве защищенного сетевого клиента и корпоративной операционной системы рабочих станций, которая может использоваться как в одноранговой среде рабочей группы, так и в среде домена Windows NT Server 4.0. Эта система может использоваться и как операционная система на автономных компьютерах.

Операционная система Windows NT Server 4.0 специфицирована для применения в качестве сервера файлов, печати и приложений с широким спектром применений: от небольших рабочих групп до корпоративных сетей.

Сети Microsoft Windows NT организуются на основе доменной модели или модели рабочей группы. И Windows NT Server 4.0, и Windows NT Workstation 4.0 могут работать в любой из этих двух моделей. Административные различия версий Windows NT зависят от используемой модели.

Доменная модель (domain model) характеризуется наличием в сети как минимум одного компьютера, работающего под управлением Windows NT Server и выполняющего роль контроллера домена (domain controller). Домен (domain) — группа компьютеров, объединенных общей базой учетных записей пользователей и единой политикой защиты.

Модель рабочей группы (workgroup model) позволяет организовать сеть на основе Windows NT без контроллера домена. Эту модель часто называют одноранговой сетью (peer-to-peer network), так как все ее компьютеры имеют равные права на совместно используемые ресурсы.

Модель рабочей группы не обеспечивает централизованного администрирования учетных записей пользователей и защиты ресурсов. Каждый сконфигурированный как сервер компьютер, работающий под управлением Windows NT Workstation 4.0 или Windows NT Server 4.0, хранит информацию об учетных записях своих пользователей и защите ресурсов в локальной базе данных. В этой модели ресурсы администрируются на всех компьютерах сети; так что, например, при изменении своего пароля пользователь должен поменять его на всех компьютерах, имеющих соответствующую учетную запись.

7.4.3.2. Функции администратора Windows NT

Администрирование Windows NT включает выполнение как специальных операций после установки системы, так и каждодневных действий. Функции администратора Windows NT Workstation и Windows NT Server схожи, но средства администрирования, входящие в состав этих версий, различны.

Администрирование Windows NT включает следующие функции и задачи:

Администрирование учетных записей пользователей и групп: планирование, создание и ведение учетных записей пользователей и групп для обеспечения каждому пользователю возможности регистрации в сети и доступа к необходимым ресурсам.

Администрирование защиты: планирование и реализация стратегии безопасности для защиты данных и общих сетевых ресурсов, включая папки, файлы и принтеры.

Администрирование принтеров: настройка локальных и сетевых принтеров для обеспечения пользователям доступа к ресурсам печати; устранение проблем печати.

Мониторинг событий и ресурсов сети: планирование и реализация стратегии аудита событий в сети с целью обнаружения нарушений защиты; управление ресурсами и контроль их использования.

Резервное копирование и восстановление данных: планирование и выполнение регулярных операций резервного копирования для обеспечения быстрого восстановления данных.

7.4.3.3. Средства администратора Windows NT 4.0

Для реализации названных функций администрирования в Windows NT 4.0 имеются следующие средства**:**

Administrative Wizards (административные мастера) -- инструментальные средства Windows NT Server 4.0, которые позволяют выполнять многие административные функции, например: создание учетной записи пользователя, создание и изменение учетных записей групп, установку прав доступа к папкам и файлам, а также настройку сетевых принтеров**.**

User Manager for Domains (диспетчер пользователей доменов) — инструментальное средство Windows NT Server 4.0, позволяющее создавать, удалять и временно отключать учетные записи пользователей домена. Кроме того, он позволяет задавать стратегию защиты для групп и добавлять к ним учетные записи пользователей

User Manager (диспетчер пользователей) — инструментальное средство Windows NT Workstation 4.0, позволяющее создавать, удалять и временно отключать локальные учетные записи пользователей и групп

Server Manager (диспетчер сервера) — инструментальное средство Windows NT Server 4.0 для отслеживания компьютеров и доменов и управления ими.

Event Viewer (средство просмотра событий) — инструментальное средство обеспечивающее уведомление администратора о любом значимом событии в системе или программе.

Windows NT Diagnostics — средства диагностики, которые предназначены для просмотра и печати информации о конфигурации системы (сведения о памяти, дисках, установленных сервисах и т.д.)

Backup — средства архивирования данных, которые предназначены для резервного копирования информации на локальный накопитель на магнитной ленте**.**

Средства администрирования Windows NT 4.0 имеют следующие недостатки:

задачи по управлению системой выполняются посредствам автономных и несовместимых друг с другом административных утилит;

ограничена возможность удаленного администрирования системы;

отсутствует возможность расширения задач администрирования;

отсутствует возможность простой передачи инструментов администрирования от одного администратора к другому; отсутствует возможность администрирования корпоративной сети с другой платформы или через Интернет.

Названные недостатки устранены в сетевых продуктах последующих версий компании Microsoft.

7.4.4. Технология и средства администрирования Windows 2000

7.4.4.1. Консоль управления Microsoft MMC

Технология и средства администрирования в Windows 2000 кардинально изменены. В Windows 2000 используется единая среда управления, получившая название консоль управления Microsoft (Microsoft Management Console — MMC). Эта общая консоль управления предназначена для запуска программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие программные модули называются оснастками (snap-ins).

Консоль MMC представляет собой общую расширяемую рабочую среду для управления и контролирования ресурсов компьютера, дисковой подсистемы, учетных записей, и т.д. Сама по себе консоль управления не обеспечивает никаких управляющих функций, а лишь является средой для оснасток (snap-ins).

Оснастка — это управляющий компонент. Одна оснастка обеспечивает единицу управления, а набор оснасток составляет управляющий инструмент. Оснастки позволяют администраторам расширять и настраивать консоль для решения своих задач. Оснастка, может вызывать другие, поддерживаемые в системе элементы управления, и динамические библиотеки. Оснастки могут работать в самостоятельном режиме и режиме расширения. В самостоятельном режиме они, обладая полной функциональностью, необходимой для выполнения какой-либо задачи, не могут использовать другие оснастки. В режиме расширения оснастки обеспечивают функциональность только при вызове их родительской оснасткой. Многие оснастки могут работать в обоих режимах

Оснастки, включенные в пользовательский интерфейс при инсталляции Windows 2000 (стандартные инструменты MMC, установленные на компьютере; см. рис. 7.2) можно вызывать непосредственно из меню **Пуск** (Start > Programs > Administrative Tools) или из группы **Администрирование** на панели управления (My Computer > Control Panel > Administrative Tools).

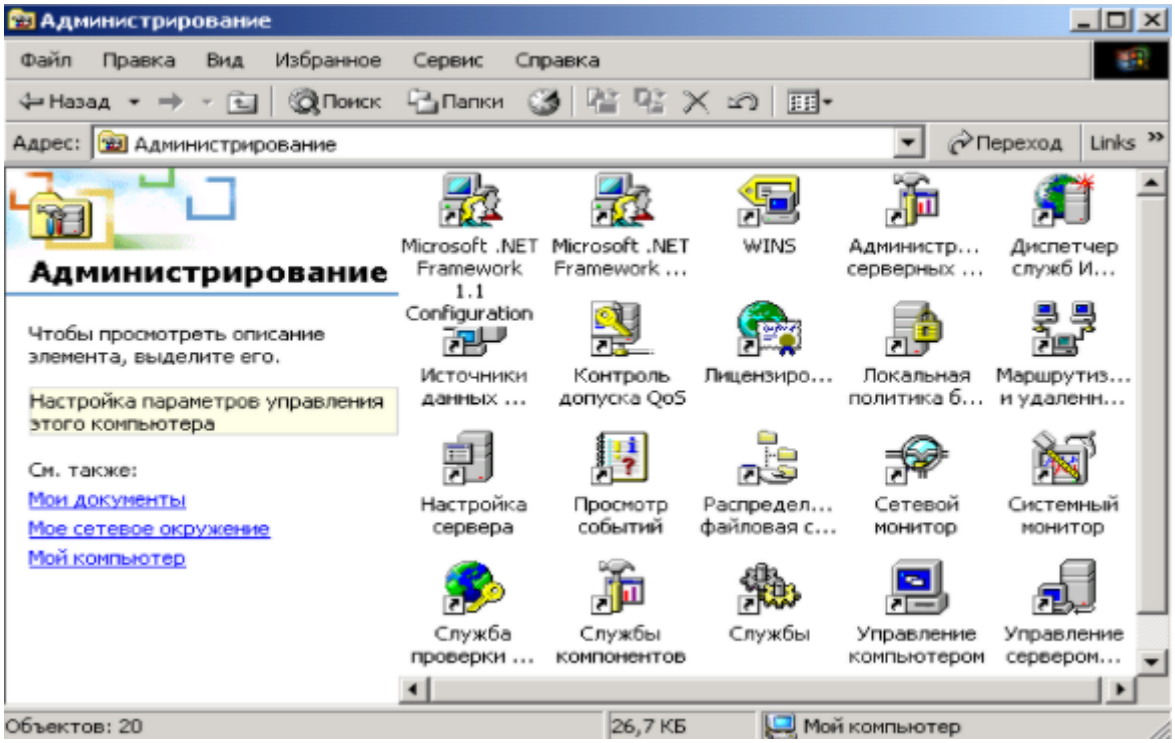

Рис. 7.2. Стандартные инструменты MMC

Консоль MMC обладает такими достоинствами, как возможность индивидуальной настройки и передача полномочий, интеграция и унификация, гибкость в выборе инструментов и продуктов. Эти достоинства позволяют существенно сократить издержки на администрирование. Консоль MMC предоставляет возможность полностью индивидуальной настройки, что позволяет администраторам создавать консоли управления, включающие только необходимые инструменты. Настройка консоли также позволяет администраторам передавать определенную часть полномочий менее опытным сотрудникам. С помощью MMC можно создать консоль, которая будет содержать объекты, необходимые для выполнения только определенных функций

7.4.4.2. Основные оснастки Windows 2000

В табл. 7.3 приведены основные оснастки Windows 2000 Professional. Оснастки, включенные в пользовательский интерфейс при инсталляции системы, отмечены звездочкой (*). Оснастки, работающие только на контроллере домена под управлением Windows 2000 Server, отмечены буквой "D".

Таблица 7.3. Оснастки Windows 2000 Professional

Оснастка	Назначение
Анализ и настройка безопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности

Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
Дефрагментация диска (Disk Defragmented)	Служит для анализа и дефрагментации дисковых томов
Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
Локальные пользователи и группы (Local Users and Groups)	Служит для управления локальными учетными записями пользователей и групп
Оснастка	Назначение
Общие папки (Shared Folders)	Отображает совместно используемые папки, текущие сеансы и открытые файлы
Оповещения и журналы производительности (Performance Logs and Alerts)	Конфигурирует журналы данных о работе системы и службу оповещений
Папка (Folder)	Служит для добавления новой папки в дерево
Просмотр событий (Event Viewer)*	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Сведения о системе (System Information)	Отображает информацию о системе
Сертификаты (Certificates)	Служит для управления сертификатами
Системный монитор (Performance)*	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и т.д.
Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
Служба компонентов (Component Services)*	Конфигурирует и управляет службами компонентов COM+
Службы (Services)*	Запускает, останавливает и конфигурирует службы (сервисы) Windows
Ссылка на Web-ресурс (Link to Web Address)	Служит для подключения Web -страниц (html, asp, xml)
Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т. д.

Управление компьютером (Computer Management)*	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Управление политикой безопасности IP (IP Security Policy Management)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами
Управление службой факсов (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
Управление съемными носителями (Removable Storage Management)	Служит для управления сменными носителями информации
Управляющий элемент (WMI Control)	Служит для конфигурирования средств Windows Management Instrumentation и управления ими
Шаблоны безопасности (Security Templates)	Обеспечивает возможность редактирования файлов-шаблонов безопасности
Элемент ActiveX (ActiveX Control)	Подключение к дереву консоли различных элементов управления ActiveX

7.4.4.3. Дополнительные оснастки Windows 2000

Дополнительные оснастки Windows 2000 Server приведены в табл. 7.4 .

Таблица 7.4. Дополнительные оснастки Windows 2000 Server

Оснастка	Назначение
*Active Directory - домены и доверие (Active Directory Domains and Trusts) **(D)**	Служит для управления доменами и доверительными отношениями
*Active Directory - пользователи и компьютеры (Active Directory Users and Computers) **(D)**	Управляет пользователями, группами, организационными единицами и другими объектами AD
*Active Directory - сайты и службы (Active Directory Sites and Services) **(D)**	Определяет топологию и расписание репликации AD. Обеспечивает изменение служб корпоративного уровня Windows 2000
Маршрутизация и удаленный доступ (Routing and Remote Access)	Служит для управления маршрутизацией и удаленным доступом
Политика безопасности домена (Domain Security Policy) **(D)**	Служит для управления политиками для всего домена. Фактически, представляет собой оснастку Групповая

	политика, настроенную на работу с конкретным доменом
Политика безопасности контроллера домена (Domain Controller Security Policy) **(D)**	Служит для управления политиками безопасности на отдельных контроллерах домена. Фактически, представляет собой оснастку Групповая политика, настроенную на работу с конкретным контроллером домена
Распределенная файловая система DPS (Distributed file system)	Создает и управляет распределенными файловыми системами, объединяющими совместно используемые папки на различных компьютерах
Телефония (Telephony)	Служит для конфигурирования служб телефонии

Кроме оснасток, перечисленных в табл.7.3 и табл.7.4, после инсталляции дополнительных служб (сетевых служб, Интернет-служб, служб терминалов), в системе появляется множество других оснасток. Такие оснастки использующихся для администрирования этих служб.

7.4.4.4. Создание учетных записей пользователей и групп

Создание учетных записей пользователей и групп занимает важное место в обеспечении безопасности Windows 2000. В процессе установки Windows 2000 Professional или Windows 2000 Server автоматически создаются две встроенные учетные записи пользователей — Администратор (Administrator) и Гость (Guest).

Учетная запись **Администратор** используется при установке и настройке рабочей станции или сервера. Она не может быть уничтожена, блокирована или удалена из группы Администраторы (Administrators), ее можно только переименовать.

Учетная запись **Гость** применяется для регистрации на компьютере без использования специально созданной учетной записи и предназначена для доступа к ресурсам компьютера случайных пользователей. Учетная запись Гость не требует ввода пароля и по умолчанию блокирована. Ей можно предоставить права доступа к ресурсам системы точно так же, как и при создании любой другой учетной записи с помощью оснастки Локальные пользователи и группы.

Группа представляет сбой набор учетных записей пользователей с похожими служебными обязанностями или потребностями в ресурсах. В процессе установки Windows 2000 автоматически создаются шесть встроенных групп (см. рис. 7.3):

Администраторы (Administrators) — ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав.

Операторы архива (Backup Operators) — члены этой группы могут архивировать и восстанавливать файлы независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему

и завершать ее работу, но они не имеют права изменять настройки безопасности.

Гости (Guests) — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Гость и получить ограниченные права на доступ к ресурсам системы.

Опытные пользователи (Power Users) — члены этой группы могут создавать учетные записи пользователей и модифицировать настройки безопасности для созданных ими учетных записей. Они могут создавать локальные группы и модифицировать состав членов групп. Члены группы Опытные пользователи не могут модифицировать членство в группах Администраторы и Операторы архива. Они не могут архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий.

Репликатор (Replicator) — членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи.

Пользователи (Users) — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они не могут получить доступ к общему каталогу или создать локальный принтер.

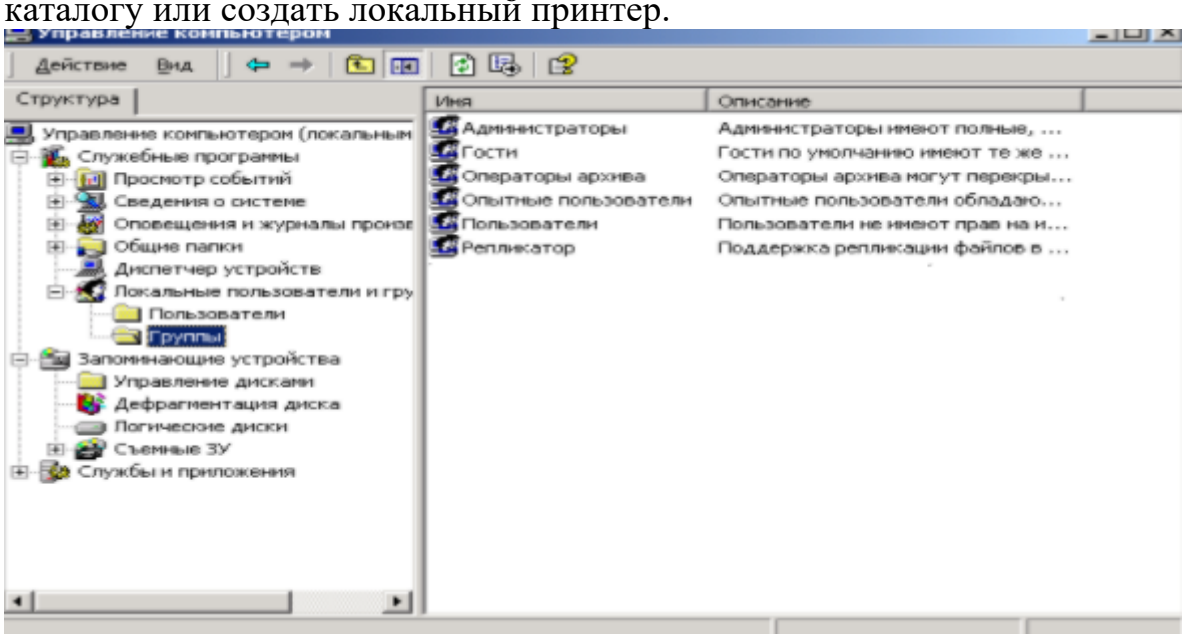

Рис. 7.3. Группы пользователей Windows 2000.

Создание учетных записей пользователей и групп в Windows 2000 осуществляется с использованием оснастки **Локальные пользователи и группы** (Local Users and Groups), которая является инструментом MMC и позволяет выполнять управление локальными учетными записями пользователей и групп. Имя пользователя должно быть уникальным для компьютера и может содержать до 20 символов верхнего и нижнего регистра.

При этом в имени пользователя недопустимо применение следующих символов:
" / \ I]:; I =, + *?<>.

7.4.4.5. Управление рабочей средой пользователя

Рабочая среда пользователя состоит из настроек рабочего стола, настроек процесса обмена информацией по сети и с устройством печати, настроек переменных среды, параметров реестра и набора доступных приложений.

Для управления средой пользователя предназначены следующие средства Windows 2000:

Сценарий входа в сеть (сценарий регистрации) представляет собой командный файл, имеющий расширение bat, или исполняемый файл с расширением exe, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

Профили пользователей. В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает пользователь. Это могут быть настройки рабочего стола, панели управления, панели задач и т.д.

Сервер сценариев Windows (Windows Scripting Host — WSH), включающий как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или на консоли команд.

Локальный профиль каждого пользователя создаются автоматически в процессе его первой регистрации на компьютере Windows 2000. Профиль пользователя хранит настройки конфигурации и параметры, индивидуально назначаемые каждому пользователю и полностью определяющие его рабочую среду. Объекты и параметры настройки профиля пользователя приведены в табл.7.5.

Таблица 7.5. Настройки профиля пользователя

Объект	Соответствующие ему параметры
Windows NT Explorer	Все настройки, определяемые самим пользователем, касающиеся программы Проводник (Windows NT Explorer)
Панель задач	Все персональные группы программ и их свойства, все программные объекты и их свойства, все настройки панели задач
Объект	Соответствующие ему параметры
Панель управления	Все настройки, определенные самим пользователем, касающиеся панели управления
Настройки принтера	Сетевые соединения принтера

Стандартные	Настройки всех стандартных приложений, запускаемых для конкретного пользователя
Приложения, работающие в операционной системе Windows 2000	Любое приложение, специально созданное для работы в среде Windows 2000, может обладать средствами отслеживания своих настроек относительно каждого пользователя. Если такая информация существует, она хранится в профиле пользователя
Электронная подсказка	Любые закладки, установленные в справочной системе Windows 2000
Консоль управления Microsoft	Индивидуальный файл конфигурации и текущего состояния консоли управления

Администратор может создать несколько типов профилей, каждый из которых ориентирован на решение определенной группы задач; назначить общие групповые настройки всем пользователям и обязательные профили, настройки которых пользователи изменять не смогут. Профили пользователей можно сохранять на сервере; при этом пользователь получит возможность работать со своим профилем при регистрации на любом компьютере сети. Такие профили называются перемещаемыми (roaming profile), при этом не все настройки локального профиля пользователя копируются в его перемещаемый профиль.

При создании профиля пользователя используется профиль, назначаемый по умолчанию, находящийся в папке Default User. Папка Default User, папки профилей индивидуальных пользователей, а также папка All Users (в которой находятся общие, используемые в профиле пользователя программные группы, а также содержатся настройки рабочего стола и меню Пуск), находятся в папке Documents and Settings корневого каталога. В папке Default User находятся файл NTuser.dat (в котором содержатся настройки конфигурации, хранящиеся в реестре Windows 2000) и список ссылок на объекты рабочего стола. Содержание папки локального профиля пользователя приведено в табл. 7.6.

Таблица 7.6. Содержимое папки локального профиля пользователя

Подпапка	Содержимое
Application Data	Данные, относящиеся к конкретным приложениям.
Cookies	Служебные файлы, получаемые с просматриваемых Web-серверов
Подпапка	Содержимое
Local Settings	Данные о локальных настройках, влияющих на работу программного обеспечения компьютера
NetHood	Ярлыки объектов сетевого окружения
PrintHood	Ярлыки объектов папки принтера
Recent	Ярлыки недавно используемых объектов
SendTo	Ярлыки объектов, куда могут посылаться документы
Главное меню	Ярлыки программ

(Start Menu)	
Избранное (Favorites)	Ярлыки часто используемых программ и папок
Мои документы (My Documents)	Данные о документах и графических файлах, используемых пользователем
Рабочий стол (Desktop)	Объекты рабочего стола, включая файлы и ярлыки
Шаблоны (Template)	Ярлыки шаблонов

Настройки, находящиеся в папке All Users, не копируются в папки профиля пользователя, но используются для его создания. Платформы Windows NT поддерживают два типа программных групп: общие программные группы и персональные программные группы. Общие программные группы всегда доступны на компьютере, независимо от того, кто зарегистрирован на нем в данный момент. Добавлять объекты к этим группам, удалять или модифицировать их может только администратор. Персональные программные группы доступны только создавшему их пользователю.

Локальный профиль пользователя хранится на компьютере в папке профиля пользователя, имя которой совпадает с именем данного пользователя и находится в папке Documents and Settings. В папке профиля пользователя содержатся подпапки, приведенные в табл. 7, а также файл NTuser.dat и файл журнала транзакций с именем NTuser.dat.log, который позволяет Windows 2000 восстанавливать данный профиль пользователя в случае сбоя при модификации содержимого файла NTuser.dat.

Если для данного пользователя не существует сконфигурированный перемещаемый (находящийся на сервере) профиль, то при первой регистрации пользователя в компьютере для него создается индивидуальный профиль. Содержимое папки Default User копируется в папку нового профиля пользователя. Информация профиля, вместе с содержимым папки All Users используется при конфигурации рабочей среды пользователя. По завершении пользователем работы на компьютере все сделанные им изменения настроек рабочей среды, выбираемых по умолчанию, записываются в его профиль, при этом содержимое папки Default User остается неизменным. Если пользователь имеет отдельную учетную запись на локальном компьютере и в домене, то для каждой из них создается свой профиль пользователя, так как регистрация на компьютере происходит с помощью различных учетных записей.

7.4.4.6. Настройка рабочей среды пользователя

Сценарии входа выполняются автоматически в процессе каждой регистрации пользователя на компьютере с операционной системой Windows 2000. Сценарий входа представляет собой командный файл с расширением bat или cmd; может быть использован также и исполняемый файл (*.exe). Они могут применяться для настройки рабочей среды пользователя, создания сетевых соединений или запуска приложений. Сценарии входа очень удобны, если необходимо изменить некоторые параметры рабочей среды пользователя без выполнения ее полной настройки.

Для создания сценариев входа можно использовать обыкновенный текстовый редактор. Созданный сценарий входа, с помощью оснастки Локальные пользователи и группы (Local Users and Groups), назначаются соответствующему пользователю; при этом один сценарий может быть назначен нескольким пользователям. В табл.7.7 приведено описание параметров, значения которых можно устанавливать с помощью сценария входа.

Таблица 7.7. Параметры, устанавливаемые с помощью сценария входа

Параметр	Описание
%HOMEDRIVE%	Имя устройства локального компьютера, связанного с домашним каталогом пользователя
%HOMEPATH%	Полный путь к домашнему каталогу пользователя
%HOMESHARE%	Имя общего ресурса, где находится домашний каталог пользователя
Параметр	Описание
%OS%	Операционная система компьютера пользователя
% PROCESSOR_ARCHITECTURE%	Тип процессора компьютера пользователя
%PROCESSOR_LEVEL%	Уровень процессора компьютера пользователя
%USERDOMAIN%	Домен, в котором находится учетная запись пользователя
%USERNAME%	Имя пользователя

Данные поля Сценарий входа определяют только имя файла и, возможно, относительный путь к нему, но не содержат сам сценарий входа, который можно поместить с определенным именем в локальный каталог компьютера пользователя. Но подобный подход, как правило, применяется только при администрировании учетных записей, на локальном компьютере, а не в домене (в последнем случае следует поместить файл сценария с указанием локального пути к сценариям входа в компьютер).

7.4.4.7. Установка и настройка аудита локальной системы

Аудит — это процесс, позволяющий фиксировать события, происходящие в операционной системе. Являясь одним из средств защиты Windows 2000, аудит (аудит безопасности) обеспечивает отображение различных событий, связанных с ее безопасностью.

Настройка аудита локального компьютера является одним из элементов локальной политики безопасности (последняя включает также политику паролей, политику учетных записей, политику безопасности IP и др.).

Локальная политика безопасности доступна только на компьютерах, не являющихся контроллерами домена.

Аудит представляет собой многошаговый процесс. По умолчанию аудит безопасности отключен, поскольку он снижает производительность системы. Он активизируется с помощью оснастки **Групповая политика** (Group Policy). После включения аудита необходимо определить набор отслеживаемых событий. Это могут быть, например, вход и выход из системы, попытки получить доступ к объектам файловой системы и т. д. Затем следует указать, какие конкретно объекты необходимо подвергнуть аудиту и включить его с помощью Редактора списков управления доступом.

После включения аудита Windows 2000 начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки **Просмотр событий** (Event Viewer) в журнале безопасности. Каждая запись журнала хранит данные о типе выполненного действия, пользователе, выполнившем его, а также о дате и моменте времени выполнения данного действия. Аудит позволяет отслеживать как успешные, так и неудачные попытки выполнения определенного действия.

7.4.5. Технологии Microsoft Windows Server 2008

7.4.5.1. Основные преимущества семейства Windows Server 2008

Server 2008 реализован на ядре Vista **(**Vista же — на ядре Server 2003)**.** Server 2008 обеспечивает усиленную безопасность и предъявляет более высокие требования к аппаратным средствам. Server 2008 поддерживает технологии аппаратной виртуализации, позволяющие практически без потери производительности запускать гостевые операционные системы; содержит доработку командной строки, позволяющую выполнять 99% операций с удаленной машины (без физического доступа к серверу); содержит улучшенные механизмы мониторинга, диагностики ошибок и восстановления системы после падений.

В операционной системе Server 2008 появился режим Server Core, позволяющий устанавливать операционную систему без графической оболочки, управляя сервером через командную строку или удаленно через **Microsoft Management Console**.

Основные преимущества семейства Windows Server 2008**:**

Надежность серверной платформы. (Windows 2008 поддерживает широкий спектр стандартов; обеспечивает безопасность, управляе-мость, совместимость, быстрое время отклика);

Возможность быстрого развертывания приложений;

Низкие затраты на поддержку IT-инфраструктуры;

Улучшенные сетевые функции, расширенные возможности для конечных пользователей;

Богатые и гибкие интерфейсные возможности платформы прикладных решений;

Надежная и безопасная IT- инфраструктура для решения бизнес-задач.

7.4.5.2. Основные понятия Windows Server 2008

К основным понятиям Windows Server 2008 относятся: классификация сервера (workload), роль (role), ролевые сервисы (role services) и дополнительные функции (features).

Классификация сервера характеризует основное назначение сервера или группы серверов в организации. К классификационным признакам относятся: поддержка сетевых функций, терминальные сервисы, сервисы баз данных, хранения, кластеризации, виртуализация, защита данных, веб-сервисы, сервер приложений, управление доступом и т, п.

Роль описывает основную функциональность сервера. Имеется возможность либо выделения всего сервера для выполнения ролевых функций, либо установки нескольких серверных ролей на одном компьютере.

Ролевые сервисы являются подмножеством роли. Каждая роль может включать один или несколько ролевых сервисов используемых для поддержки функциональности той или иной роли.

Дополнительные функции обычно не относятся к основной функциональности сервера и используются для реализации дополнительных возможностей сервера.

7.4.5.3. Описание основных ролей Windows Server 2008

Сервер может выполнять следующие роли:

- Active Directory Domain Services,
- Active Directory Federation Services,
- Active Directory Certificate Server,
- Application Server,
- DNS Server,
- File Server,
- Print Server,
- UDDI Services,
- Web Server (IIS),
- Windows Media Services,
- Active Directory Lightweight Directory Services,
- Active Directory Rights Management Services,
- Network Access Services,
- DHCP Server,

- Fax Server,
- Media Server,
- Terminal Services,
- Virtual Server,
- Windows Deployment Services,
- Windows SharePoint Services,

Описание ролей.

Active Directory Certificate Services (AD CS) — позволяет создавать и управлять цифровыми сертификатами для пользователей, компьютеров и организаций, представляя собой часть инфраструктуры поддержки публичных ключей (public key).

Active Directory Domain Services (AD DS) — хранит информацию о сетевых объектах и делает эту информацию доступной пользователям и сетевым администраторам. Для своей работы AD DS использует контролеры доменов для предоставления сетевым пользователям ресурсов в любой точке сети.

Active Directory Federation Services (AD FS) — обеспечивает упрощенный, зашифрованный способ передачи идентификационной информации и поддержку единого доступа к ресурсам (Web single sign-on, SSO).

Active Directory Lightweight Directory Services (AD LDS) — предоставляет хранилище для данных, требуемых определенным классом приложений.

Active Directory Rights Management Services (AD RMS) — может использоваться для защиты информации от несанкционированного доступа. Active Directory Rights Management Services — это технология защиты информации, которая используется соответствующим классом приложений.

Dynamic Host Configuration Protocol (DHCP) Server — обеспечивает централизованную конфигурацию и управление временными IP-адресами и соответствующей информацией для клиентских компьютеров.

Domain Name System (DNS) Server — транслирует доменные и компьютерные DNS-имена в IP-адреса. Такой сервер более прост в управлении, если он установлен на том же сервере, что и доменные сервисы Active Directory Domain Services.

Fax Server — отсылает и принимает факсовые сообщения и позволяет управлять ресурсами факса — задачами, настройками, отчетами, а также локальными и сетевыми факсовыми устройствами.

File Server — предоставляет технологии для управления хранилищами, репликации файлов, распределенного управления пространством, быстрого поиска файлов и клиентского доступа к файловой системе сервера.

Terminal Services — предоставляет технологии, обеспечивающие доступ к серверу, выполняющему Windows-приложения или полной среде Windows. Пользователи соединяются с терминальным сервером для запуска приложений, сохранения файлов и использования сетевых ресурсов сервера.

Network Access Services — поддерживает роутинг сетевого трафика через LAN и WAN, создание и применение правил сетевого доступа(network access policies) и доступ к сетевым ресурсам через VPN-соединения и dial-up.

Print Services — управляет сетевыми принтерами и драйверами, предоставляя соответствующие сервисы.

Web Server — надежная, управляемая, масштабируемая инфраструктура для выполнения веб-приложений и сервисов.

Windows Deployment Services (WDS) — позволяет быстро и безопасно развернуть на компьютерах системы на базе операционной системы Windows, используя сетевые установки без необходимости привлечения администратора для установки системы на каждом компьютере или установки компонентов Windows с CD или DVD.

Windows Media Services — поставляет непрерывный поток цифро- аудио- и видеоинформации для клиентов внутри сети.

Windows SharePoint Services — облегчает создание сайтов, на которых пользователи могут совместно работать над документами, задачами, событиями, обмениваться контактной и другой информацией.

7.4.5.4. Описание дополнительных **функции, доступных в Server 2008**

Дополнительные функции, доступные в windows server 2008:

- Windows Activation Services (WAS),
- BitLocker Drive Encryption,
- Failover Clustering,
- Internet Storage Naming Server,
- Microsoft Message Queuing (MSMQ) Services,
- Removable Storage Manager,
- Simple Mail Transfer Protocol (SMTP) Server,
- Storage Manager for Storage Area Networks (SANs),
- Subsystem for UNIX-based application,
- Telnet Server,
- Windows Internal Database Server,
- Windows Network Load Balancing,
- Windows Foundation Components for WinFX,
- SQL Server Embedded Edition ,
- Background Intelligent Transfer Service (BITS) Server Extensions,
- Desktop Experience,
- Windows Server Backup,
- Line Print Remote (LPR) Port Monitor

- Remote Assistance,
- RPC over HTTP Proxy,
- SNMP Service,
- Simple TCP/IP Services,
- Telnet Client,
- TFTP Client,
- Windows Internal Naming Service (WINS),
- Windows System Resource Manager (WSRM) Wireless LAN Service.

Описание дополнительных функций

- **Background Intelligent Transfer Service (BITS) Server Extensions** — позволяет BITS-сервер получать загруженные клиентами файлы. Этот компонент не требуется для предоставления клиентам возможности загрузки файлов с BITS-сервера.
- **Windows BltLocker Drive Encryption** — аппаратная система обеспечения безопасности, позволяющие реализовать шифрование на уровне томов.
- **Desktop Experience** — включает ряд функций Windows Vista, темы для рабочего стола и управление фотографиями.
- **Internet Storage Naming Server (iSNS)** — обрабатывает запросы на регистрацию, отмену регистрации и запросы к iSCSI-устройствам.
- **Line Printer Remote (IPR) Port Monitor** — позволяет выводить информацию на устройства печати, присоединенные к компьютерам, работающим под управлением операционной системы UNIX.
- **Message Queuing** (также называется MSMQ) позволяет приложениям общаться между собой через гетерогенные сети и системы, которые могут временно находиться в режиме offline. MSMQ обеспечивает гарантированную доставку сообщений, эффективное перенаправление сообщений, безопасность и пересылку сообщений на основе приоритетов.
- **Multipath I/O** — обеспечивает поддержку использования различных механизмов адресации для устройств хранения.
- **Removable Storage Manager** — управляет сменными носителями и устройствами, поддерживающими такие носители.
- **Remote Assistance** — позволяет удаленным пользователям подсоединяться к данному компьютеру для непосредственного решения возникших на компьютере проблем.
- **Remote Procedure Call (RPC) over HTTP Proxy** — перенаправляет RPC-трафик от клиентских приложений

через HTTP на сервер в качестве альтернативы для клиентов, обращающихся к серверу через VPN-соединение.

- **Simple Mail Transfer Protocol (SMTP) Server** — обеспечивает поддержку передачи электронной почты между серверами.
- **Storage Manager for Storage Area Networks (SAN)** — поддерживает сети класса SAN, соответствующие требованиям VDS.
- **Subsystem for UNIX-based Applications (SUA)** — позволяет выполнять UNIX-приложения и выполнять администрирование системы непосредственно из командной сроки UNIX.
- **Telnet Client** — использует протокол Telnet для соединения с удаленным Telnet-сервером и выполнения приложений на этом сервере.
- **Telnet Server** — позволяет удаленным пользователям выполнять пакетное администрирование и выполнять приложения, используя клиент Telnet, включая клиентов, выполняемых на UNIX-системах.
- **Trivial File Transfer Protocol (TFTP) Client** — позволяет передавать файлы через сервер TFTP.
- **Windows Activation Service (WAS)** — обеспечивает поддержку среды для .NET-процессов и конфигурационных функций.
- **Failover Clustering** — обеспечивает высокую доступность различных серверных ролей и приложений, которые имеют сохраняемые состояния — таких как файловые сервисы, SQL Server и т. п. за счет использования отказоустойчивых кластеров на основе разделяемых дисков.
- **Windows Foundation Components for WinFX** — поддерживает приложения, созданные с использованием компонентов .NET Framework 3-0.
- **Windows Internal Database** — использует SQL Server 2005 Embedded Edition (Windows) в качестве реляционного хранилища данных для ролей Windows, включая Windows SharePoint Services, Active Directory Rights Management Services. Services .
- **Windows Internet Name Service (WINS)** — позволяет компьютерам, работающим под управлением Windows, обнаруживать в подсетях другие компьютеры, использующие NetBIOS.
- **Wireless Networking** — конфигурирует беспроводные соединения и соответствующие профили беспроводных сетей.
- **Windows Network Load Balancing (WNLB)** — распределяет приходящие прикладные запросы

среди групп серверов, на которых находятся экземпляры приложения.

- **Windows Server Backup** — позволяет восстанавливать состояние операционной системы, файлов, папок и данных приложений за счет периодического создания «снимков» полного сервера или выбранных томов.

7.4.5.5. Server Manager Windows 2008

Для управления ролями, ролевыми сервисами и дополнительны функциями в Windows Server 2008 используется **Server Manager**; по существу это замена утилитам (Manage Your Server, Configure Your Server и Add or Remove Windows Components), входящим в состав Windows Server 2003.

Server Manager позволяет:

устанавливать и удалять роли и дополнительные функции,
добавлять ролевые сервисы,
запускать и останавливать сервисы,
управлять учетными записями,
анализировать протокол событий
и т. п.

Server Manager содержит набор «мастеров» для добавления ролей, ролевых сервисов, дополнительной функциональности, а также удаления соответствующих компонентов (Add Roles Wizard, Add Role Services Wizard, Add Features Wizard, Remove Roles Wizard, Remove Role Services Wizard и Remove Features Wizard).

7.4.5.6. Server Core

Server Core (минимальная установка; называется **ядром сервера**) обеспечивает среду для функционирования следующих ключевых серверных ролей:

Dynamic Host Configuration Protocol (DHCP) Server,
Domain Name System (DNS) Server,
File Server,
Domain Controller.

ОС Windows Server 2008 первая операционная система семейства Windows обеспечивающая возможность минимального набора функциональности. Такая возможность, сокращая набор ролей, доступных на сервере, существенно повышает безопасность и упрощает управление серве. Однако в Server Core отличие от Linux графическая подсистема и API-функции продолжают работать, пожирая системные ресурсы.

7.4.5.7. Сетевой стек Windows Server 2008

В Microsoft Windows Server 2008 появился полностью переписанный сетевой стек TCP/IP (Next Generation TCP/IP Stack). Изменения представляет собой обновление функциональных возможностей Windows TCP/IP, а также соответствующих служб и интерфейсов прикладного программирования, отвечающих требованиям современных сетевых сред и технологий.

К названным изменениям и улучшениям относятся:

- новая архитектура стека TCP/IP для универсальной поддержки IPv4 и IPv6;
- интеллектуальные алгоритмы автоматической настройки и оптимизации сети;
- безопасность сетевых узлов и улучшения IPsec;
- интегрированная поддержка аппаратной разгрузки сети;
- упрощенное управление и сетевая диагностика;
- набор интерфейсов прикладного программирования, обеспечивающих возможности расширения.

Архитектура драйвера стека TCP/IP Server 2008, реализованного в файле tcpip.sys, состоит из следующих уровней:

Транспортный уровень (содержит реализации протоколов TCP и UDP, а также механизм для отсылки базовых IP-пакетов, которым не требуется наличие TCP или UDP-заголовков);

Сетевой уровень (содержит реализации протоколов IPv4 и IPv6 в виде уровня Dual IP layer);

Уровень доступа к сети (содержит модули для IPv4 и IPv6; модули для интерфейсов IEEE 802.3, IEEE 802.11 и PPP и др.)

7.4.5.7. Усовершенствованная версия Windows Server 2008

Усовершенствованная версия Windows Server 2008: **Windows Server 2008 R2** (октябрь 2009 г.) использует ядро Windows NT 6.1 (как и Windows 7); содержит новые и усовершенствованные средства и возможности включая виртуализацию клиентских и серверных систем с помощью **Hyper-V,** а также виртуализацию представлений с помощью служб удаленных рабочих столов.

Новая версия Hyper-V обеспечивает:

- усовершенствование управления виртуальными центрами обработки данных;
- снижение трудоемкости ежедневно выполняемых задач по администрированию Hyper-V путем использования консоли управления Hyper-V.

- повышение эффективности использования средств командной строки и автоматизированного управления для администрирования Hyper-V благодаря применению командлетов PowerShell;
- повышение эффективности управления несколькими серверами Hyper-V в среде виртуального центра обработки данных путем использования диспетчера виртуальных машин System Center 2008.

В Windows Server 2008 R2 роль служб терминалов переименована в роль служб удаленных рабочих столов; последняя предоставляет пользователям, с использованием протокола RDP (Remote Desktop Protocol), возможность доступа к рабочим столам виртуальных машин сервера Windows 2008 R2. Роль служб удаленных рабочих столов включает: узел сеансов удаленных рабочих столов, веб-доступ к удаленным рабочим столам, лицензирование удаленных рабочих столов, шлюз удаленных рабочих столов, узел виртуализации удаленных рабочих столов.

ОС Windows Server 2008 R2 в сравнение с предыдущими версиями Windows Server, облегчает планирование, развертывание и управление корпоративными сетями. Внедрение Windows 2008 R2 позволяет сократить расходы и повысить эффективность управления и контроля ресурсов предприятия.

Тема 8. Сетевая безопасность

8.1. Проблемы сетевой безопасности

Защита компьютерной сети является одним из наиболее важных и сложных аспектов сетевой технологии. Причем наибольшую сложность составляют вопросы обеспечения Internet-безопасности современных корпоративных сетей. Проблема безопасности в Internet усугубляется тем, что Internet разрабатывалась как открытая система, при этом вопросам безопасности стека протоколов TCP/IP уделялось очень мало внимания. И все это происходит на фоне, с одной стороны, всевозрастающего количества различных вредоносных программ (вирусы, черви, троянские кони и др.) и технологий, а с другой, — увеличивающейся стоимости и значимости корпоративной информации.

Особенностью обеспечения технологии сетевой безопасности организации (предприятия, фирмы), в плане профессиональной подготовки, являются высокие требования к специалистам по информационной безопасности (к специалистам отдела информационной безопасности, а в небольших организациях — к системному администратору). Специалист по информационной безопасности должен обладать не только глубокими специальными знаниями, должен не только регулярно отслеживать состояние в области безопасности (http://www.bezpeka.com/, http://www.bugtraq.ru/), но и уметь руководствоваться здравым смыслом. В некоторых литературных источниках приводят такое соотношение: 98% здравого смысла и 2% технологии. Очевидно, что специалистов, отвечающих таким требованиям не так много, при этом разрыв между спросом и предложением на этих высокооплачиваемых специалистов велик и постоянно растет.

Под информационной безопасностью понимают защищенность информации от случайных или преднамеренных воздействий (угроз) естественного или искусственного характера, связанных с нанесением ущерба информационной системе.

Обеспечение информационной безопасности корпоративной сети является комплексной проблемой, разрешение которой требует системного подхода предполагающего анализ и структурирование возможных нарушений с последующей разработкой и внедрением необходимых средств обеспечения информационной безопасности.

Для уяснения сложности и многоплановости анализа возможных нарушений информационной безопасности обратимся к результатам исследований, выполненных компанией InfoWatch в области корпоративной защиты информации от внутренних угроз («Внутренние ИТ-угрозы в России 2005»), и опубликованных на сайте http://www.infowatch.ru. Здесь же можно получить «свежую» аналитическую информацию.

На рис. 8.1 приведена статистика наиболее опасных ИТ-угроз, а на рис. 8.2 - самых опасных внутренних ИТ-угроз (взяты из названного источника).

Рис. 8.1. Наиболее опасные ИТ-угрозы**.**

Рис. 8.2. Самые опасные внутренние ИТ-угрозы

Заметим, что на этих рисунках приведены лишь наиболее опасные угрозы, при этом каждая из приведенных видов угроз, как правило, включает подвиды. Так, например, кража включает:

кражу технических средств (винчестеров, системных блоков, ноутбуков и т.д.);

кражу носителей информации (магнитных, оптических и др.);

кражу информации (несанкционированное копирование и др.);

кражу средств доступа (ключи, пароли и т.д.).

Далее, например, срез «вредоносные программы» включает: вирусы, черви, троянские кони, бомбы, салями и т.д.

На рис. 8.3 приведена информация по каналам утечки данных.

Рис. 8.3 Каналы утечки данных

Обеспечение информационной безопасности предполагает использование определенных средств безопасности, см. рис. 8.4

Рис. 8.4. Популярные средства ИТ-безопасности.

Однако системного подхода требуют не только анализ возможных нарушений и разработка технологических средств информационной безопасности, но и сам процесс внедрения этих средств. Препятствия, связанные с внедрением средств ИТ-безопасности отражены на рис. **8.5.**

Рис. 8.5. Препятствия, связанные с внедрением средств ИТ-безопасности.

Закончим этот пункт известным постулатом: абсолютную (100%) защиту обеспечить нельзя. Однако сбалансированный комплексный подход к созданию системы защиты информации, начинающийся с проработки технического задания и заканчивающийся оценкой эффективности и качества системы защиты, позволит при фиксированных затратах обеспечить максимальный процент защиты. При таком подходе система защиты информации приобретает интегративные (эмерджентные) свойства, которые не присущие ни одной из ее составных частей.

8.2. Основные этапы создания системы защиты информации

Система защиты информации является сложной системой, поэтому процесс ее создания, как и всякой другой сложной системы, представляет собой поэтапный последовательно-циклический процесс. Наиболее полно обсуждаемый процесс описан в различных регламентирующих документах и стандартах, например, в ISO 17779, ISO 27001 RFC 2196 и др. Кроме названных стандартов, которые относятся к уровню менеджмента, существует и множество других международных стандартов по информационной безопасности (стандарты на криптосистемы, стандарты защищенной передачи данных и т.д.).

Понятийный же базис в области информационной безопасности был заложен в так называемой "Оранжевой книге": стандарт Министерства обороны США (Department of Defense Trusted Computer System Evaliation Criteria, 1985 г.). Позднее была выпущена "Радужная серия", наиболее

значимым документ которой: "Интерпретация "Оранжевой книги" для сетевых конфигураций" (Trusted Network Interpretation; 1987 г.). Этот документ содержит важнейшие концептуальные понятия (включая криптографические аспекты), и описание сервисов безопасности в области сетевых конфигураций.

Одной из наиболее удачных технологий создания современных систем безопасности считается разработанная компания Cisco Systems стратегия безопасности, получившая название **SAFE,** которая включает следующие этапы:

1. Политика безопасности.
2. Средства обеспечения политики безопасности.
3. Мониторинг.
4. Тестирование
5. Управление и улучшение.

Разработка политики безопасности организации (компании) предполагает создание документа, регламентирующего принципы информационной безопасности, которыми должен руководствоваться каждый сотрудник организации. На данном этапе целесообразно использовать стандарты ISO 17799 RFC ISO 27001 RFC 2196.

На втором этапе согласно разработанной политике безопасности проектируется система комплексного обеспечения безопасности. Используются межсетевые экраны, системы обнаружения атак, устройства шифрования и другое необходимое оборудование, а также реализуются организационные и физические методы обеспечения безопасности.

Третий этап предполагает внедрение систем постоянного мониторинга и анализа активности в сети компании на базе информации, полученной от систем обнаружения атак, серверов SNMP, а также различных систем регистрации.

Четвертый этап связан с вопросами тестирования существующей сети на предмет ее уязвимости путем использования специализированных сетевых сканнеров, которые позволяют обнаружить слабые места и элементы в системе защиты, и выдают некоторые рекомендации по их устранению.

На пятом, завершающем, этапе реализуется управление всеми устройствами обеспечения безопасности, а также оптимизация параметров элементов защиты в существующей системе. В последующем можно проводить и модернизацию существующей системы безопасности.

8.3. Политика информационной безопасности

Политика информационной безопасности представляет собой изложение целей, задач и решений которые должны быть достигнуты при внедрении системы защиты информации. В политике информационной безопасности должны быть отражены:

Предмет политики (предметная область, терминология, цель и причины разработки политики).

Позиция руководства организации (решение руководства по данной политике, разрешения и запреты по использованию ресурсов).

Применимость политики (где, как, когда, кем и к чему применяется данная политика).

Роли и обязанности должностных лиц (ответственные лица и их обязанности в плане разработки и внедрения политики безопасности).

Реализация политики (регламент, нарушения и наказание).

Справочная информация и консультанты по безопасности.

8.4. Основные уровни и средства защиты сети

Защита сети охватывает следующие уровни**:**

Физическая защита.

Контроль действий пользователей.

Программная защита.

Физическая защита предполагает ограничение доступа пользователей к серверам, маршрутизаторам, брандмауэрам и другой сетевой аппаратуре путем ограничение доступа в помещение, в котором расположена аппаратура, или/и посредством идентификационных карт, карточек-ключей и т. п.

Контроль действий пользователей предполагает аутентификацию, аудит и управление рабочей средой пользователей. Неправильно сформированная в этой части политика безопасности или ее несоблюдение(записанный на бумажке пароль или незаблокированная администратором консоль) может свести на нет все усилия по обеспечению физической или программной защиты сети.

Программная защита предполагает анализ уязвимости программной среды, идентификацию и устранение потенциальных точек воздействия, закрытие дыр, черных ходов (back doors) и защиту от атак. В сети, требующей высокого уровня защиты, значительная часть работы связана с отслеживанием новых эксплойтов (документированных способов проникновения в систему) и осуществлением превентивных мер, направленных на устранение возможности их применения в сети.

Технология защиты сети базируется на использовании определенного комплекса средств обеспечения безопасности. К основным средствам обеспечения безопасности относятся: антивирусные программы, антишпионские программы , анализаторы сетевых протоколов, брандмауэры, сканеры сетевой безопасности.

Несмотря на сложность и многоплановость самой проблематики защиты сети потеря работоспособности сети во многих случаях обусловлена тривиальными причинами. Так по данным Международного общества компьютерной безопасности ICSA (International Computer Security Association), более 90% времени, стоимости и усилий, направленных на нейтрализацию последствий потери данных или служб в сетях, затрачиваются вследствие таких банальных причин, как вирусы, нарушение энергопотребления и злонамеренные действия персонала организаций. При

этом в 70% проникновение в сети и системы осуществляется самими сотрудниками организаций.

Сложность проблематики информационной безопасности трудно переоценить. Эта сложность обусловлена не только спецификой сетевых технологий и конфликтным характером атакующей и противоборствующей сторон, но и факторами организационного, мотивационного, психологического, финансового и другого характера. При этом здесь очень важна правильная позиции высшего руководства организации и высокая оплата специалистов, обеспечивающих безопасность системы.

Более детальному знакомству со спецификой сетевой безопасности, основными положениями и литературой в данной области, а также практическому освоению технологии диагностики и борьбы с нарушением сетевой защиты посвящены 4, 5, 7 и 8 практические занятия по данному курсу.