

КУЗИН А.В., ДЕМИН В.М.

КОМПЬЮТЕРНЫЕ СЕТИ

МОСКВА

2004

Оглавление

Введение

Глава 1. Основные понятия о компьютерных сетях

- 1.1. Классификация информационно-вычислительных сетей (ИВС).
Локальные, городские и глобальные сети.....
- 1.2. Основные характеристики и классификация ЭВМ
- 1.3. Программные и аппаратные средства ИВС
- 1.4. Сети одноранговые и "клиент/сервер"
- 1.5. Способы коммутации, топология ИВС
- 1.6. Сетевые компоненты
- 1.7. Многоуровневые ИВС
- 1.8. Эталонная модель взаимосвязи открытых систем

Контрольные вопросы к главе 1

Глава 2. Основные технические характеристики и качество компьютерных сетей и телекоммуникационных каналов

- 2.1. Показатели качества информационно-вычислительных сетей
- 2.2. Классификация каналов связи
- 2.3. Типы цифровых каналов

Контрольные вопросы к главе 2

Глава 3. Линии связи сетей ЭВМ

- 3.1. Типы линий связи
- 3.2. Характеристики линий связи
- 3.3. Беспроводные каналы связи
- 3.4. Системы мобильной связи

Контрольные вопросы к главе 3

Глава 4. Локальные вычислительные сети

- 4.1. Характеристики локальных сетей
- 4.2. Методы доступа к среде передачи данных

4.2.1. Множественный доступ с контролем несущей и обнаружением конфликтов	
4.2.2. Приоритетный доступ.....	
4.2.3. Маркерные методы доступа.....	
4.3. Локальные сети на основе маркерной шины	
4.4. Сети на основе маркерного кольца	
4.5. Сети Ethernet.....	
4.6. Сети FDDI.....	
4.7. Высокоскоростные локальные сети.....	
4.8. Структурированные кабельные системы	
4.9. Общие подходы к выбору топологии сети.....	
Контрольные вопросы к главе 4	
Глава 5. Организация корпоративных сетей.....	
5.1. Общие сведения	
5.2. Алгоритмы маршрутизации.....	
5.3. Уровни и протоколы.....	
5.3.1. Спецификация интерфейса сетевых устройств	
5.3.2. Протоколы	
5.4. Адресация компьютеров в Интернет	
5.5. Службы обмена данными.....	
5.5.1. Сети X.25.....	
5.5.2. Уровень передачи данных ATM.....	
5.5.3. Сети SDH	
Контрольные вопросы к главе 5	
Глава 6. Сетевые операционные системы	
6.1. Классификация операционных систем	
6.2. Обобщенная структура операционных систем.....	
6.3. Модель клиент-сервер и модель ОС на базе микроядра.....	
6.3.1. Модель клиент-сервер	

6.3.2. Режим пользователя.....	
6.3.3. Режим ядра.....	
6.3.4. Взаимодействие подсистем с исполнительной системой.....	
6.4. Топологии распределенных вычислений	
6.5. Администрирование сети.....	
6.5.1. Модели администрирования и регистрации в сети	
6.5.2. Основные правила конфигурирования компьютеров, подключенных к сети	
6.5.3. Общие сведения об администрировании пользователей и рабочих групп.....	
Контрольные вопросы к главе 6	
Глава 7. Структура и информационные услуги	
территориальных сетей	
7.1. Структура территориальных сетей	
7.2. Протоколы файлового обмена, электронной почты, дистанционного управления	
7.3. Виды конференц-связи	
7.4. Web-технологии	
7.5. Языки и средства создания Web-приложений	
Контрольные вопросы к главе 7	
Приложение. Пример подхода к разработке ЛВС предприятия, выбору типа сервера с возможностью расширения сети	
СПИСОК ЛИТЕРАТУРЫ	

Введение

Компьютерные информационно-вычислительные сети и телекоммуникации - сравнительно новая стремительно развивающаяся область науки и техники. Работы по проектированию и созданию ИВС и телекоммуникаций ведутся одновременно во многих передовых странах мира.

Для изучения принципов организации и функционирования информационно-вычислительных сетей (ИВС) и телекоммуникаций необходимо обладать знаниями в достаточно широкой области, включающей основы электротехники и электроники, информатики и вычислительной техники, и дополнить их знаниями сетевых технологий, техники электрической связи и других.

Учитывая специфику среднего профессионального обучения, материал предлагаемого учебника излагается последовательно, вначале с рассмотрения общих вопросов построения ИВС, а затем с углубленным описанием основных компонентов сетей и телекоммуникаций.

Основой книги послужили тексты лекций и практических занятий, проводимых авторами в Красногорском оптико-электронном колледже, а также на факультете Информационных систем и защиты информации Московского государственного социального университета.

Глава 1. Основные понятия о компьютерных сетях

1.1. Классификация информационно-вычислительных сетей (ИВС). Локальные, городские и глобальные сети

Коммуникационная сеть - система, состоящая из объектов, называемых пунктами (узлами) сети и осуществляющих функции генерации, преобразования, хранения и потребления некоторого продукта, а также линий передачи (связей, коммуникаций, соединений), осуществляющих передачу продукта между пунктами. В качестве продукта могут фигурировать информация, энергия, масса. Соответственно различают группы сетей информационных, энергетических, вещественных. В группах сетей возможно разделение на подгруппы. Так, среди вещественных сетей могут быть выделены сети транспортные, водопроводные, производственные и др.

Информационно-вычислительная сеть - коммуникационная сеть, в которой продуктом генерирования, переработки, хранения и использования является информация, а узлами сети является вычислительное оборудование. Компонентами ИВС могут быть ЭВМ и периферийные устройства, являющиеся источниками и приемниками данных, передаваемых по сети. Эти компоненты составляют оконечное оборудование данных. В качестве оконечного оборудования данных могут выступать ЭВМ, принтеры, плоттеры и другое вычислительное, измерительное и исполнительное оборудование автоматических и автоматизированных систем. Собственно пересылка данных происходит с помощью сред и средств, объединяемых под названием среда передачи данных.

Классификация сетей.

ИВС классифицируются по ряду признаков. В зависимости от расстояний между связываемыми узлами различают вычислительные сети:

территориальные - охватывающие значительное географическое пространство. Среди территориальных сетей можно выделить сети **региональные** и **глобальные**, имеющие соответственно региональные или глобальные масштабы; региональные сети иногда называют сетями MAN (Metropolitan Area Network), а общее англоязычное название для территориальных сетей - WAN (Wide Area Network).

локальные вычислительные сети (ЛВС) - охватывающие ограниченную территорию (обычно в пределах удаленности станций не более чем на несколько десятков или сотен метров друг от друга, реже на 1...2 км). Локальные сети обозначают LAN (Local Area Network).

корпоративные сети (масштаба предприятия) - совокупность связанных между собой ЛВС, охватывающих территорию, на которой размещено одно предприятие или учреждение в одном или нескольких близко расположенных зданиях.

Среди глобальных сетей следует выделить единственную в своем роде глобальную сеть Internet и реализованную в ней информационную службу World Wide Web (WWW) (переводится на русский язык как всемирная паутина).

Различают интегрированные сети, неинтегрированные сети и подсети. **Интегрированная вычислительная сеть (интерсеть)** представляет собой взаимосвязанную совокупность многих вычислительных сетей, которые в интерсети называются подсетями. Обычно интерсети приспособлены для различных видов связи:

телефонии, электронной почты, передачи видеoinформации, цифровых данных и т.п. В этом случае они называются **сетями интегрального обслуживания**.

В зависимости от топологии соединений узлов различают **сети шинной (магистральной), кольцевой, звездной, ячеистой, комбинированной, произвольной структуры**.

В зависимости от способа управления различают сети:

"клиент/сервер" или сети с выделенным сервером. В них выделяется один или несколько узлов (их название - серверы), выполняющих в сети управляющие или специальные обслуживающие функции, а остальные узлы (клиенты) являются терминальными, в них работают пользователи. Сети клиент/сервер различаются по характеру распределения функций между серверами, другими словами по типам серверов (например, файл-серверы, серверы баз данных). При специализации серверов по определенным приложениям получается **сеть распределенных вычислений**.

одноранговые - в них все узлы равноправны. Поскольку в общем случае под клиентом понимается объект (устройство или программа), запрашивающий некоторые услуги, а под сервером - объект, предоставляющий эти услуги, поэтому каждый узел в одноранговых сетях может выполнять функции и клиента, и сервера.

В зависимости от того, одинаковые или неодинаковые ЭВМ применяют в сети, различают сети однотипных ЭВМ, называемые **однородными**, и разнотипных ЭВМ - **неоднородные** (гетерогенные).

В зависимости от прав собственности на сети последние могут быть **сетями общего пользования** (public) или **частными** (private).

Среди сетей общего пользования выделяют телефонные сети и сети передачи данных

Сети также различают в зависимости от используемых в них протоколов и по способам коммутации.

Протоколы - это набор семантических и синтаксических правил, определяющий поведение функциональных блоков сети при передаче данных. Другими словами, протокол - это совокупность соглашений относительно способа представления данных, обеспечивающего их передачу в нужных направлениях и правильную интерпретацию данных всеми участниками процесса информационного обмена.

Поскольку информационный обмен - процесс многофункциональный, то протоколы делятся на уровни. К каждому уровню относится группа родственных функций. Для правильного взаимодействия узлов различных вычислительных сетей их архитектура должна быть открытой. Этим целям служат унификация и стандартизация в области телекоммуникаций и вычислительных сетей.

Унификация и стандартизация протоколов выполняются рядом международных организаций, что наряду с разнообразием типов сетей породило большое число различных протоколов. Наиболее широко распространенными являются протоколы, разработанные и применяемые в глобальной сети Internet, протоколы открытых систем Международной организации по стандартизации (ISO - International Standard Organization), протоколы Международного телекоммуникационного союза (International Telecommunication Union - ITU, ранее называвшегося CCITT) и протоколы Института инженеров по электротехнике и электронике (IEEE - Institute of Electrical and Electronics Engineers).

Протоколы сети Internet объединяют под названием TCP/IP. Протоколы ISO являются семиуровневыми и известны как протоколы **базовой эталонной модели взаимосвязи открытых систем**.

1.2. Основные характеристики и классификация ЭВМ

ЭВМ являются центральными элементами обработки данных в информационно-вычислительных сетях, параметры которых играют определяющую роль в эффективности функционирования сети. **Эффективность** - это свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством.

Вычислительные машины могут быть классифицированы по размерам и по признаку вычислительной мощности, другое название которой - **производительность**, измеряется в МИПС (MIPS от Mega Instruction Per Second) - миллионах операций в секунду над числами с фиксированной запятой (точкой). Для операций над числами, представленными в форме с плавающей точкой, единица измерения производительности МФлоПС (MFLoPS - Mega FLoating point Operation Per Second). Поскольку компьютеры выполняют самые разные задачи, оценки производительности в МИПС и МФлоПС получаются не достаточно точными, поэтому для персональных компьютеров вместо производительности указывают **тактовую частоту**, более объективно определяющую быстродействие машины. Например, тактовый генератор с частотой 100 МГц обеспечивает выполнение 20 млн коротких простейших машинных операций (сложение, вычитание, пересылка информации) в секунду, с частотой 1000 МГц - 200 млн операций в секунду.

По этим двум признакам ЭВМ разбиты на классы: микроЭВМ, малые ЭВМ, большие ЭВМ и суперЭВМ. Основные характеристики классов современных ЭВМ приведены в табл. 1.1.

Таблица 1.1. Основные параметры классов современных компьютеров

Параметры	Класс компьютера			
	Супер-компьютеры	Большие компьютеры	Малые компьютеры	Микрокомпьютеры
Производительность, MIPS	1000 - 1000000	100 - 10000	10 - 1000	10 - 100
Емкость оперативной памяти, Гбайт	2000 - 100000	512 - 100000	128- 2048	32 - 512
Емкость накопителя на магнитных дисках, Гбайт	500 - 500000	100- 10000	20 - 500	10 - 50
Разрядность, бит	64 - 256	64 - 126	32 - 128	32 - 128

МикроЭВМ многочисленны и разнообразны. Многопользовательские микрокомпьютеры оборудованы несколькими видеотерминалами и работают в режиме разделения времени, что позволяет эффективно работать на них одновременно нескольким пользователям (многопользовательский режим, режим с разделением времени).

Персональные компьютеры (ПК)- однопользовательские, удовлетворяющие требованиям общедоступности и универсальности применения.

Рабочие станции (work station) представляют собой однопользовательские микрокомпьютеры, часто специализированные для определенного вида работ - графических, инженерных, издательских и т. п. **Специализированные ЭВМ**, в отличие от универсальных, призваны решать определенный достаточно узкий круг задач с меньшими затратами оборудования и потому более простой архитектуры и низкой стоимости.

Серверы (от server) - многопользовательские мощные микрокомпьютеры в вычислительных сетях, выделенные для обработки запросов от всех рабочих станций сети.

Сетевые компьютеры (network computer) - упрощенные микрокомпьютеры, обеспечивающие работу в сети и доступ к сетевым ресурсам, часто специализированные на выполнение определенного вида работ, таких, как организация просмотра сетевых ресурсов, электронной почты, защита сети от несанкционированного доступа и т. д.

Персональные компьютеры универсальны и общедоступны ввиду их малой стоимости, автономности эксплуатации без специальных требований к условиям окружающей среды, обеспечивают адаптируемость архитектуры к разнообразным применениям в сфере управления, науки, образования, в быту. Обладают высокими показателями ожидаемой надежности работы - более 5000 часов наработки на отказ.

Широко известны компьютеры американской фирмы IBM (International Business Machine Corporation):

- IBM PC XT (Personal Computer eXtended Technology);
- IBM PC AT (Personal Computer Advanced Technology) на микропроцессорах (МП) 80286 (16-ти разрядные, то есть длина разрядной сетки, длина машинного слова равна 16-ти битам);

- IBM PS/2 8030 - PS/2 8080 (Personal System, все, кроме PS/2 8080 - 16-ти разрядные, PS/2 8080 - 32-х разрядная);
- IBM PC на МП 80386 и 80486 (32-х разрядные);
- IBM PC на МП Pentium - Pentium 4 (64-х разрядные).

Персональные компьютеры выпускаются и другими фирмами: американскими - Apple (Macintosh), Compaq Computer, Hewlett Packard, Dell, DEC (Digital Equipment Corporation), а также фирмами Великобритании - Spectrum, Amstard, Франции - Micral, Италии - Olivetty, Японии - Toshiba, Panasonic, Partner. В настоящее время широкое распространение (более 80%) получили появившиеся в 1981 году ПК фирмы IBM и их аналоги. Второе место занимают ПК фирмы Apple (Macintosh). Из всего мирового парка компьютеров количество ПК составляет более 90%.

Промышленность стран СНГ выпускала ПК Apple - совместимые (диалоговые вычислительные комплексы ДВК-1 - ДВК-4 на основе "Электроники МС-1201", "Электроники 85", "Электроники 32" и т.п.) а также IBM PC - совместимые (ЕС 1840 - ЕС 1842, ЕС 1845, ЕС 1849, ЕС 1861, Искра 1030", "Истра 4816", "Нейрон И9.66" и т.д.).

Малые ЭВМ (другое название мини-ЭВМ) - надежные, недорогие и удобные в эксплуатации. Применяются в качестве управляющих вычислительных комплексов для управления технологическими процессами, для вычислений в многопользовательских вычислительных системах, в системах автоматизированного проектирования, в системах моделирования несложных объектов. в системах искусственного интеллекта.

Характеристики современных мини-компьютеров и наиболее мощных из них - супер-мини-компьютеров таковы:

производительность - до 1000 MIPS;

емкость основной памяти (оперативной и кэш-памяти) - до 8000 Мбайт;

емкость дисковой памяти - до 1000Гбайт;

разрядность - 32, 64 и 128;

число поддерживаемых пользователей - 16 - 1024.

Первыми микрокомпьютерами являлись компьютеры PDP 11 фирмы DEC (США), ставшие прототипами отечественных мини-ЭВМ - Системы Малых ЭВМ (СМ ЭВМ): СМ 1, 2, 3, 4, 1400, 1700 и других. Семейство мини-компьютеров PDP-11 объединяет модели от VAX-11 до VAX-3600; мощные модели мини-компьютеров класса 8000(VAX-8250, 8820); супер-мини-компьютеры класса 9000 (VAX-9410, 9430) и другие. Характеристики моделей VAX:

производительность 10 - 1000 MIPS;

количество процессоров 1 - 32;

емкость основной памяти - 512 Мбайт - 2 Гбайт;

емкость дисковой памяти - 50 - 500 Гбайт;

число каналов ввода-вывода - до 64.

К большим ЭВМ относятся компьютеры, имеющие следующие основные характеристики:

производительность - не менее 100 MIPS;

емкость основной памяти - 512 - 10000 Мбайт;

емкость дисковой памяти - не менее 100 Гбайт;

число поддерживаемых пользователей - 16 - 1000.

Большие ЭВМ иначе называются *мэйнфреймами* (main - главный, основной; frame - стойка, корпус), поскольку они выполняют роль главной ЭВМ вычислительного центра. Применяются большие ЭВМ для решения научно-технических задач, в ВС с пакетной обработкой информации, для работы с большими базами данных, для управления вычислительными сетями

и их ресурсами а также в качестве больших серверов ВС, так называемых серверов - мэйнфреймов. Первыми появились машины фирмы IBM. Архитектура и программное обеспечение моделей IBM 360 и IBM 370 стали прототипами отечественной Единой Системы больших машин ЕС ЭВМ. С 1990 года выпускаются 18 моделей компьютеров семейства IBM ES/9000 (ES - Enterprise System - система предприятий). Младшая модель ES/9221 model 120 имеет оперативную память емкостью 256 Мбайт, производительность десятки MIPS и 12 каналов ввода-вывода. Старшая модель ES/9221 model 900 имеет 6 векторных процессоров, оперативную память емкостью 9 Гбайт, производительность тысячи MIPS и 256 каналов ввода-вывода, использующих волоконно-оптический кабели.

С 1997 года большие компьютеры трансформировались в малогабаритные мэйнфреймы семейства S/390, включающее 14 моделей машин с объемом оперативной памяти до 16 Гбайт, с быстродействием от 50 MIPS до 500 MIPS у 10-процессорной машины. Семейство S/390 получило широкое распространение в мире, а также в России. Кроме того, на отечественных предприятиях выполняется сборка моделей семейства S/390.

Также распространены и большие ЭВМ семейства M 1800 корпорации Fujitsu (Япония) и Millennium 400 и 500 предприятия Amdahl, являющегося дочерним фирмы Fujitsu. Семейство состоит из 5-ти моделей: Model-20, 30, 45, 65, 85. Модели 45, 65 и 85 - многопроцессорные компьютеры с 4-мя, 6-тью и 8-ю процессорами соответственно; модель 85 имеет основную память емкостью 2 Гбайт и 256 каналов ввода-вывода. Фирма Amdahl с 1999 года выпускает 12-ти процессорные модели Millennium 700 и 800 производительностью 685 и 1000 MIPS соответственно.

СуперЭВМ - мощные многопроцессорные компьютеры с производительностью сотни миллионов - десятки миллиардов операций в секунду. Характеристики типового суперкомпьютера 2001 года: высокопараллельная многопроцессорная вычислительная система с производительностью порядка 100 000 MFLoPS, с емкостью оперативной памяти 10 Гбайт, дисковой памяти 1 -10 Тбайт (1 Тбайт = 1000 Гбайт), с разрядностью 64 - 128 бит. Для сбалансированности ресурсов ЭВМ необходимо, чтобы на каждый MFLoPS производительности процессора приходилось не менее 1 Мбайт оперативной памяти.

Фирма IBM недавно объявила о разработке новой суперЭВМ, которая будет содержать более миллиона микропроцессоров Pentium III и обладать быстродействием 10^{15} операций /с.

Архитектура всех этих высокопроизводительных ЭВМ отлична от традиционной однопроцессорной фон-Неймановской архитектуры с одиночным потоком команд и одиночным потоком данных (ОКОД или *скалярные* процессоры, рис 1.1 а) и называется **архитектурой массового параллелизма**. СуперЭВМ создаются в виде высокопараллельных многопроцессорных вычислительных систем, имеющих по принятой классификации три разновидности структур:

1. **Магистральные** (другое название *конвейерные*), у которых процессор одновременно выполняет разные операции над последовательным потоком обрабатываемых данных. Это системы с многократным потоком команд и однократным потоком данных (МКОД или MISD - Multiple Instruction Single Data - рис. 1.1. б). Например, отечественные суперЭВМ "Эльбрус 3,4", имеют модифицированную параллельно-конвейерную структуру MMISD.

2. **Векторные**, у которых все процессоры одновременно выполняют одну команду над различными данными - однократный поток команд с многократным потоком данных (ОКМД или SIMD - Single Instruction Multiple Data - рис. 1.1 в).

3. **Матричные**, у которых микропроцессор одновременно выполняет разные операции над последовательными потоками обрабатываемых данных - многократный поток команд с многократным потоком данных (МКМД или MIMD - Multiple Instruction Multiple Data - рис. 1.1 г).

В периодически обновляемой таблице TOP500 (www.top500.org) сведены показатели суперкомпьютеров различных производителей. Суммарная мощность этих 500 наиболее производительных компьютеров составляет менее 0,1% от суммарной вычислительной мощности всех компьютеров мира.

1.3. Программные и аппаратные средства ИВС

Вычислительная сеть - это сложный комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов, основными элементами которого являются:

- компьютеры;
- коммуникационное оборудование;
- операционные системы;
- сетевые приложения.

В основе любой сети лежит стандартизованная аппаратная платформа. В настоящее время в сетях широко и успешно применяются компьютеры различных классов - от персональных компьютеров до мэйнфреймов и суперЭВМ. Набор компьютеров в

сети должен соответствовать набору разнообразных задач, решаемых сетью.

Второй элемент - это коммуникационное оборудование. Хотя компьютеры и являются центральными элементами обработки данных в сетях, в последнее время не менее важную роль стали играть коммуникационные устройства. Кабельные системы, повторители, мосты, коммутаторы, маршрутизаторы и модульные концентраторы из вспомогательных компонентов сети превратились в основные наряду с компьютерами и системным программным обеспечением как по влиянию на характеристики сети, так и по стоимости. Сегодня коммуникационное устройство может представлять собой сложный специализированный мультипроцессор, который нужно конфигурировать, оптимизировать и администрировать. Изучение принципов работы коммуникационного оборудования требует знакомства с большим количеством протоколов, используемых как в локальных, так и глобальных сетях.

Третьей составляющей, образующей программную платформу сети, являются операционные системы (ОС). От того, какие концепции управления локальными и распределенными ресурсами положены в основу сетевой ОС, зависит эффективность работы всей сети. При проектировании сети важно учитывать, насколько просто данная операционная система может взаимодействовать с другими ОС сети, насколько она обеспечивает безопасность и защищенность данных, до какой степени она позволяет наращивать число пользователей, можно ли перенести ее на компьютер другого типа и многие другие соображения.

Последней составляющей сетевых средств являются различные сетевые приложения, такие как сетевые базы данных,

почтовые системы, средства архивирования данных, системы автоматизации коллективной работы и др. Очень важно представлять диапазон возможностей, предоставляемых приложениями для различных областей применения, а также знать, насколько они совместимы с другими сетевыми приложениями и операционными системами.

1.4. Сети одноранговые и "клиент/сервер"

Локальные, глобальные и территориальные сети могут быть одноранговыми сетями, сетями типа "клиент/сервер" (они также называются сетями с выделенным сервером) или смешанными сетями (в которых используются как одноранговые технологии, так и технологии с выделенным сервером).

Компьютеры в **одноранговых сетях** могут выступать как в роли клиентов, так и в роли серверов. Так как все компьютеры в этом типе сетей равноправны, одноранговые сети не имеют централизованного управления разделением ресурсов. Любой из компьютеров может разделять свои ресурсы с любым компьютером в той же сети. Одноранговые взаимоотношения также означают, что ни один компьютер не имеет ни высшего приоритета на доступ, ни повышенной ответственности за предоставление ресурсов в совместное пользование.

Каждый пользователь в одноранговой сети является одновременно сетевым администратором. Это означает, что каждый пользователь в сети управляет доступом к ресурсам, расположенным на его компьютере. Он может дать всем остальным неограниченный доступ к локальным ресурсам, дать ограниченный доступ, а может не дать вообще никакого доступа другим пользователям. Каждый

пользователь также решает, дать другим пользователям доступ просто по их запросу или защитить эти ресурсы паролем.

Основной проблемой в одноранговых сетях является безопасность, т.к. отсутствуют средства обеспечения безопасности в масштабе сети. При этом отдельные ресурсы отдельных компьютеров могут быть защищены системой паролей, и только те пользователи, которые знают пароль, могут получить доступ к ресурсам.

Этот тип сети может быть работоспособным в малых сетях, но также требует, чтобы пользователи знали и помнили различные пароли для каждого разделенного ресурса в сети. С ростом количества пользователей и ресурсов одноранговая сеть становится неработоспособной. Это происходит не потому, что сеть не может функционировать правильно, а потому, что пользователи не в состоянии справиться со сложностью сети.

К тому же большинство одноранговых сетей состоит из набора типичных персональных компьютеров, связанных общим сетевым носителем. Эти типы компьютеров не были разработаны для работы в качестве сетевых серверов, поэтому производительность сети может упасть, когда много пользователей попытаются одновременно получить доступ к ресурсам какого-то одного компьютера. Кроме того, пользователь, к чьей машине происходит доступ по сети, сталкивается с падением производительности в то время, когда компьютер выполняет затребованные сетевые службы. Например, если к компьютеру пользователя подключен принтер, к которому осуществляется доступ по сети, компьютер будет замедлять свою работу каждый раз, когда пользователи посылают задание на этот принтер. Это может раздражать того, кто работает на данной машине.

В одноранговой сети также трудно организовывать хранение и учет данных. Когда каждый сетевой компьютер может служить сервером, пользователям трудно отслеживать, на какой машине лежит интересующая их информация. Децентрализованная природа такого типа сети делает поиск ресурсов чрезвычайно сложным с ростом числа узлов, на которых должна происходить проверка. Децентрализация также затрудняет процедуру резервного копирования данных - вместо копирования централизованного хранилища данных требуется осуществлять резервное копирование на каждом сетевом компьютере, чтобы защитить разделенные данные.

Однако одноранговые сети имеют серьезные преимущества перед сетями с выделенным сервером, особенно для малых организаций и сетей. Одноранговые сети являются наиболее легким и дешевым типом сетей для установки. Большинство одноранговых сетей требует наличия на компьютерах, кроме сетевой карты и сетевого носителя (кабеля), только операционной системы. Как только компьютеры соединены, пользователи немедленно могут начинать предоставление ресурсов и информации в совместное пользование.

Преимущества одноранговых сетей:

- легкость в установке и настройке;
- независимость отдельных машин от выделенного сервера;
- возможность пользователем контролировать свои собственные ресурсы;
- сравнительная дешевизна в приобретении и эксплуатации;
- отсутствие необходимости в дополнительном программном обеспечении, кроме операционной системы;

отсутствие необходимости иметь отдельного человека в качестве выделенного администратора сети.

Недостатки одноранговых сетей:

необходимость помнить столько паролей, сколько имеется разделенных ресурсов;

необходимость производить резервное копирование отдельно на каждом компьютере, чтобы защитить все совместные данные;

падение производительности при доступе к разделенному ресурсу, на компьютере, где этот ресурс расположен;

отсутствие централизованной организационной схемы для поиска и управления доступом к данным.

Сети с выделенным сервером или сети типа "клиент/сервер" опираются на специализированные компьютеры, называемые серверами, представляющими собой централизованные хранилища сетевых ресурсов и объединяющими централизованное обеспечение безопасности и управления доступом. В отличие от сетей с выделенным сервером, одноранговые сети не имеют централизованного обеспечения безопасности и управления. Сервер представляет собой сочетание специализированного программного обеспечения и оборудования, которое предоставляет службы в сети для остальных клиентских компьютеров (рабочих станций) или других процессов.

Имеется несколько причин для реализации сети с выделенным сервером, включающих централизованное управление сетевыми ресурсами путем использования сетевой безопасности и управление посредством установки и настройки сервера. С точки зрения оборудования, серверные компьютеры обычно имеют более быстрый центральный процессор, больше памяти, большие жесткие диски и дополнительные периферийные устройства, например

накопители на магнитной ленте и приводы компакт-дисков, по сравнению с клиентскими машинами. Серверы также ориентированы на то, чтобы обрабатывать многочисленные запросы на разделяемые ресурсы быстро и эффективно. Серверы обычно выделены для обслуживания сетевых запросов клиентов. В дополнение, физическая безопасность - доступ к самой машине - является ключевым компонентом сетевой безопасности. Поэтому важно, чтобы серверы располагались в специальном помещении с контролируемым доступом, отделенном от помещений с общим доступом.

Сети с выделенным сервером также предоставляют централизованную проверку учетных записей пользователей и паролей. Например, Windows NT использует доменную концепцию для управления пользователями, группами и машинами и для контроля над доступом к сетевым ресурсам. Прежде чем пользователь сможет получить доступ к сетевым ресурсам, он должен сообщить свое регистрационное имя и пароль контроллеру домена - серверу, который проверяет имена учетных записей и пароли в базе данных с такой информацией. Контроллер домена позволит доступ к определенным ресурсам только в случае допустимой комбинации регистрационного имени и пароля. Изменять связанную с безопасностью информацию в базе данных контроллера домена может только сетевой администратор. Этот подход обеспечивает централизованную безопасность и позволяет управлять ресурсами с изменяющейся степенью контроля в зависимости от их важности и расположения.

В отличие от одноранговой модели, сеть с выделенным сервером обычно требует только один пароль для доступа к самой сети, что уменьшает количество паролей, которые пользователь

должен помнить. Кроме того, сетевые ресурсы типа файлов и принтеров легче найти, потому что они расположены на определенном сервере, а не на чьей-то машине в сети. Концентрация сетевых ресурсов на небольшом количестве серверов также упрощает резервное копирование и поддержку данных.

Сети с выделенным сервером лучше масштабируются - в сравнении с одноранговыми сетями. С ростом размера одноранговые сети сильно замедляют свою работу и становятся неуправляемыми. Сети с выделенным сервером, наоборот, могут обслуживать от единичных пользователей до десятков тысяч пользователей и географически распределенных ресурсов. Другими словами, сеть с выделенным сервером может расти с ростом использующей ее организации.

Подобно одноранговой модели, сеть с выделенным сервером также имеет недостатки. Первой в этом списке стоят необходимость дополнительных расходов на такие сети. Сеть с выделенным сервером требует наличия одного или нескольких более мощных - и, соответственно, более дорогих - компьютеров для запуска специального (и тоже дорогого) серверного программного обеспечения. Вдобавок серверное программное обеспечение требует квалифицированного персонала для его обслуживания. Подготовка персонала для овладения необходимыми для обслуживания сети с выделенным сервером навыками или наем на работу подготовленных сетевых администраторов также увеличивают стоимость такой сети.

Есть и другие негативные аспекты сетей с выделенным сервером. Централизация ресурсов и управления упрощает доступ, контроль и объединение ресурсов, но при этом приводит к появлению точки, которая может привести к неполадкам во всей

сети. Если сервер вышел из строя, - не работает вся сеть. В сетях с несколькими серверами потеря одного сервера означает потерю всех ресурсов, связанных с этим сервером. Также, если неисправный сервер является единственным источником информации о правах доступа определенной части пользователей, эти пользователи не смогут получить доступ к сети.

Преимущества сетей с выделенным сервером:

обеспечение централизованного управления учетными записями пользователей, безопасностью и доступом, что упрощает сетевое администрирование;

использование более мощного серверного оборудования означает и более эффективный доступ к сетевым ресурсам;

пользователям для входа в сеть нужно помнить только один пароль, что позволяет им получить доступ ко всем ресурсам, к которым имеют права;

Недостатки сетей с выделенным сервером:

неисправность сервера может сделать сеть неработоспособной; что в лучшем случае означает потерю сетевых ресурсов;

сети требуют квалифицированного персонала для сопровождения сложного специализированного программного обеспечения, что увеличивает общую стоимость сети;

стоимость также увеличивается благодаря потребности в выделенном оборудовании и специализированном программном обеспечении.

1.5. Способы коммутации, топология ИВС

Под **коммутацией данных** понимается их передача, при которой канал передачи данных может использоваться попеременно

для обмена информацией между различными пунктами информационной сети в отличие от связи через некоммутируемые каналы, обычно закрепленные за определенными абонентами.

Различают следующие способы коммутации данных:

- **коммутация каналов** - осуществляется соединением двух или более станций данных и обеспечивается монопольное использование канала передачи данных до тех пор, пока соединение не будет разомкнуто;

- **коммутация сообщений** - характеризуется тем, что создание физического канала между оконечными узлами необязательно и пересылка сообщений происходит без нарушения их целостности; вместо физического канала имеется виртуальный канал, состоящий из физических участков, и между участками возможна буферизация сообщения;

- **коммутация пакетов** - сообщение передается по виртуальному каналу, но оно разделяется на пакеты, при этом канал передачи данных занят только во время передачи пакета (без нарушения его целостности) и по ее завершении освобождается для передачи других пакетов.

Коммутация каналов может быть пространственной и временной.

Пространственный коммутатор размера $N \times M$ представляет собой сетку (матрицу), в которой N входов подключены к горизонтальным шинам, а M выходов - к вертикальным (рис. 1.2).

В узлах сетки имеются коммутирующие элементы, причем в каждом столбце сетки может быть открыто не более чем по одному элементу. Если $N < M$, то коммутатор может обеспечить соединение каждого входа с не менее чем одним выходом; в противном случае коммутатор называется блокирующим, т.е. не обеспечивающим

соединения любого входа с одним из выходов. Обычно применяются коммутаторы с равным числом входов и выходов $N \times N$.

Недостаток рассмотренной схемы - большое число коммутирующих элементов в квадратной матрице, равное N^2 . Для устранения этого недостатка применяют многоступенчатые коммутаторы.

Временной коммутатор строится на основе буферной памяти, запись производится в ее ячейки последовательным опросом входов, а коммутация осуществляется благодаря считыванию данных на выходы из нужных ячеек памяти. При этом происходит задержка на время одного цикла "запись-чтение". В настоящее время преимущественно используются временная или смешанная коммутация.

Во многих случаях наиболее эффективной оказывается коммутация пакетов. Во-первых, ускоряется передача данных в сетях сложной конфигурации за счет того, что возможна параллельная передача пакетов одного сообщения на разных участках сети; во-вторых, при появлении ошибки требуется повторная передача короткого пакета, а не всего длинного сообщения. Кроме того, ограничение сверху на размер пакета позволяет обойтись меньшим объемом буферной памяти в промежуточных узлах на маршрутах передачи данных в сети.

Под топологией сети понимается описание ее физического расположения, а именно, как компьютеры соединены друг с другом в сети, и с помощью каких устройств входят в физическую топологию. Существуют четыре основных топологии: шина (Bus), кольцо (Ring), звезда (Star) и ячеистая топология (Mesh). Другие топологии обычно являются комбинацией двух и более главных типов. Выбор типа физической топологии для сети является одним

из первых шагов планирования сети. Выбор топологии основывается на множестве факторов, в число которых входят цена, расстояния, вопросы безопасности, предполагаемая сетевая операционная система, а также будет ли новая сеть использовать существующее оборудование, проводку и т. п.

Физическая топология **"шина"** (Bus), именуемая также линейной шиной (Linear Bus), состоит из единственного кабеля, к которому присоединены все компьютеры сегмента (рис. 1.3). Сообщения посылаются по линии всем подключенным станциям вне зависимости от того, кто является получателем. Каждый компьютер проверяет каждый пакет в проводе, чтобы определить получателя пакета. Если пакет предназначен для другой станции, компьютер отвергнет его. Соответственно, компьютер получит и обработает любой пакет на шине, адресованный ему.

Главный кабель шины, известный как магистраль (backbone), имеет на обоих концах заглушки (terminator) для предотвращения отражения сигнала. Без правильно установленных заглушек работа шины будет ненадежной или вообще невозможной.

Шинная топология представляет собой быстрее и простейший способ установки сети. Она требует меньше оборудования и кабелей, чем другие топологии, и ее легче настраивать. Это хороший способ быстрого построения временной сети. Это обычно лучший выбор для малых сетей (не более 10 компьютеров).

Имеется несколько недостатков, о которых надо знать при решении вопроса об использовании шинной топологии для сети. Неполадки станции или другого компонента сети трудно изолировать. Кроме того, неполадки в магистральном кабеле могут привести к выходу из строя всей сети.

Топология **"кольцо"** (Ring) обычно используется в сетях Token Ring и FDDI (волоконно-оптических). В физической топологии Ring линия передачи данных фактически образует логическое кольцо, к которому подключены все компьютеры сети (рис. 1.4). В отличие от шинной топологии, которая использует конкурентную схему, чтобы позволить станциям получать доступ к сетевому носителю, доступ к носителю в кольце осуществляется посредством логических знаков - "маркеров" (token), которые пускаются по кругу от станции, к станции, давая им возможность переслать пакет, если это нужно. Это дает каждому компьютеру в сети равную возможность получить доступ к носителю и, следовательно, переслать по нему данные. Компьютер может посылать данные только тогда, когда владеет маркером.

Так как каждый компьютер при этой топологии является частью кольца, он имеет возможность пересылать любые полученные им пакеты данных, адресованные другой станции. Получающаяся регенерация делает сигнал сильным и позволяет избежать необходимости в применении повторителей. Так как кольцо формирует бесконечный цикл, заглушки не требуются. Кольцевая топология относительно легка для установки и настройки, требуя минимального аппаратного обеспечения.

Топология физического кольца имеет несколько недостатков. Как и в случае линейной шины, неполадки на одной станции могут привести к отказу всей сети. Поддерживать логическое кольцо трудно, особенно в больших сетях. Кроме того, в случае необходимости настройки и переконфигурации любой части сети придется временно отключить всю сеть.

Кольцевая топология даст всем компьютерам равные возможности доступа к сетевому носителю.

В топологии "звезда" (Star) все компьютеры в сети соединены друг с другом с помощью центрального концентратора (рис. 1.5). Все данные, которые посылает станция, направляются прямо на концентратор, который затем пересылает пакет в направлении получателя. Как и при шинной топологии, компьютер в сети типа "звезда" может пытаться послать данные в любой момент. Однако на деле только один компьютер может в конкретный момент времени производить посылку. Если две станции посылают сигналы на концентратор точно в одно время, обе посылки окажутся неудачными и каждому компьютеру придется подождать случайный период времени, прежде чем снова пытаться получить доступ к носителю. Сети с топологией Star обычно лучше масштабируются, чем другие типы.

Главное преимущество внедрения топологии "звезда" заключается в том, что в отличие от линейной шины неполадки на одной станции не выведут из строя всю сеть. В сетях с этой топологией проще находить обрывы кабеля и прочие неисправности. Это облегчает обнаружение обрыва кабеля и других неполадок. Кроме того, наличие центрального концентратора в топологии "звезда" облегчает добавление нового компьютера и реконфигурацию сети.

Топологии "звезда" присущи несколько недостатков. Во-первых, этот тип конфигурации требует больше кабеля, чем большинство других сетей, вследствие наличия отдельных линий, соединяющих каждый компьютер с концентратором. Кроме того, центральный концентратор выполняет большинство функций сети, так что выход из строя одного этого устройства отключит всю сеть.

Ячеистая топология (Mesh) соединяет все компьютеры попарно (рис. 1.6). Сети ячеистой топологии используют

значительно большее количество кабеля, чем любая другая топология, что делает их дороже. Кроме того, такие сети значительно сложнее устанавливать, чем другие топологии. Однако ячеистая топология устойчива к сбоям (fault tolerance). Устойчивость к сбоям заключается в способности работать при наличии повреждений. В сети с поврежденным сегментом это означает обход сегмента. Каждый компьютер имеет множество возможных путей соединения с другим компьютером по сети, так что отдельный обрыв кабеля не приведет к потере соединения между любыми двумя компьютерами.

Многие организации используют комбинации главных сетевых топологий, называемые смешанные сети

Смешанная топология **звезда на шине** (Star Bus), показанная на рис.1.7 объединяет топологии "шина" и "звезда". Преимущество этой топологии заключается в том, что никакие неполадки на отдельном компьютере или в сегменте не могут вывести из строя всю сеть. Также в случае неисправности отдельного концентратора не смогут взаимодействовать по сети только те компьютеры, которые присоединены к этому концентратору, а остальные компьютеры эта проблема не затронет.

Топология " звезда на кольце" (Star Ring) известна также под названием Star-wired Ring, поскольку сам концентратор выполнен как кольцо. Сеть " звезда на кольце" внешне идентична топологии "звезда", но на самом деле концентратор соединен проводами как логическое кольцо (рис. 1.8). Эта топология популярна для сетей Token Ring, поскольку легче в реализации, чем физическое кольцо, но дает возможность посылать "токены" внутри концентратора так же, как и в случае физического кольца. Почти так же, как при топологии "кольцо", компьютеры имеют равный доступ к сетевому

носителю за счет посылки "токенов". Повреждение отдельного компьютера не может привести к остановке всей сети, но если выходит из строя концентратор, кольцо, которым управляет концентратор, тоже отключается.

Реализация настоящей ячеистой топологии в крупных сетях может быть дорогой, требующей времени и непростой. Сеть **"гибридной ячеистой топологии"** (Hybrid Mesh) может предоставить некоторые из существенных преимуществ настоящей сети ячеистой топологии без необходимости использовать большого количества кабеля. В большинстве крупных организаций критически важные данные хранятся не на всех компьютерах сети. Вместо этого они хранятся на сетевых серверах. Компании, которые хотят обеспечить защиту от сбоев для своих сетей на уровне кабелей, могут ограничить только компьютерами с критически важными данными. Это означает, что ячеистая топология существует только на части сети (рис. 1.9). Этот тип ячеистой топологии по-прежнему обеспечивает защиту от сбоев для серверов с важной информацией, но не добавляет защиты для отдельных клиентов сети. Гибридная ячеистая топология должна стоить меньше, чем сеть, полностью построенная на ячеистой топологии, но будет не столь защищенной от сбоев.

1.6. Сетевые компоненты

Существует множество сетевых устройств, которые возможно использовать для создания, сегментирования и усовершенствования сети. Основными из них являются сетевые адаптеры, повторители, усилители, мосты, маршрутизаторы и шлюзы.

Сетевые адаптеры (карты), или NIC (Network Interface Card), являются теми устройствами, которые физически соединяет

компьютер с сетью. Прежде чем выполнить такое соединение, надо правильно установить и настроить сетевой адаптер. Простота или сложность этой установки и настройки зависит от типа сетевого адаптера, который предполагается использовать. Для некоторых конфигураций достаточно просто вставить адаптер в подходящий слот материнской платы компьютера. Автоматически конфигурирующиеся адаптеры, а также адаптеры, отвечающие стандарту Plug and Play (Вставь и работай), автоматически производят свою настройку. Если сетевой адаптер не отвечает стандарту Plug and Play, требуется настроить его запрос на прерывание IRQ (Interrupt Request) и адрес ввода/вывода (Input/Output address). IRQ представляет собой логическую коммуникационную линию, которую устройство использует для связи с процессором. Адрес ввода/вывода - это трехзначное шестнадцатеричное число, которое идентифицирует коммуникационный канал между аппаратными устройствами и центральным процессором. Чтобы сетевой адаптер функционировал правильно, должны быть правильно настроены как IRQ, так и адрес ввода/вывода.

Повторители и усилители.

Сигнал при перемещении по сети ослабевает. Чтобы противодействовать этому ослаблению, можно использовать повторители и/или усилители, которые усиливают сигналы, проходящие через них по сети.

Повторители (repeater) используются в сетях с цифровым сигналом для борьбы с ослаблением сигнала. Повторители обеспечивают надежную передачу данных на большие расстояния, нежели обычно позволяет тип носителя. Когда повторитель получает ослабленный входящий сигнал, он очищает сигнал,

увеличивает его мощность и посылает этот сигнал следующему сегменту,

Усилители (amplifier), хоть и имеют сходное назначение, используются для увеличения дальности передачи в сетях, использующих аналоговый сигнал. Аналоговые сигналы могут переносить как голос, так и данные одновременно - носитель делится на несколько каналов, так что разные частоты могут передаваться параллельно.

Концентратор (hub) представляет собой сетевое устройство, служащее в качестве центральной точки соединения в сетевой конфигурации “звезда” (star). Концентратор также может быть использован для соединения сетевых сегментов. Существуют три основных типа концентраторов: пассивные (passive), активные (active) и интеллектуальные (intelligent). Пассивные концентраторы, не требующие электроэнергии, действуют просто как физическая точка соединения, ничего не добавляя к проходящему сигналу. Активные концентраторы требуют энергии, которую они используют для восстановления и усиления сигнала, проходящего через них. Интеллектуальные концентраторы могут предоставлять такие сервисы, как переключение пакетов (packet switching) и перенаправление трафика (traffic routing).

Мост (bridge) представляет собой другое устройство, используемое для соединения сетевых сегментов. Мост функционирует в первую очередь как повторитель, он может получать данные из любого сегмента, однако он более разборчив в передаче этих сигналов, чем повторитель. Если получатель пакета находится в том же физическом сегменте, что и мост, то мост знает, что этот пакет достиг цели и, таким образом, больше не нужен. Однако, если получатель пакета находится в другом физическом

сегменте, мост знает, что его надо переслать. Эта обработка помогает уменьшить загрузку сети. Например, сегмент не получает сообщений, не относящихся к нему.

Мосты могут соединять сегменты, которые используют разные типы носителей (кабелей). Они могут соединять сети с разными схемами доступа к носителю - например, сеть Ethernet и сеть Token Ring. Примером таких устройств являются мосты-трансляторы (translating bridge), которые осуществляют преобразование между различными методами доступа к носителю, позволяя связывать сети разных типов. Другой специальный тип моста, прозрачный, (transparent bridge) или интеллектуальный мост (learning bridge), периодически “изучает”, куда направлять получаемые им пакеты. Он делает это посредством непрерывного построения специальных таблиц, добавляя в них по мере необходимости новые элементы.

Возможным недостатком мостов является то, что они передают данные дольше, чем повторители, так как проверяют адрес сетевой карты получателя для каждого пакета. Они также сложнее в управлении и дороже, нежели повторители.

Маршрутизатор (router) представляет собой сетевое коммуникационное устройство, которое может связывать два и более сетевых сегментов (или подсетей). Маршрутизатор функционирует подобно мосту, но для фильтрации трафика он использует не адрес сетевой карты компьютера, а информацию о сетевом адресе, передаваемую в относящейся к сетевому уровню части пакета. После получения этой информации об адресе маршрутизатор использует таблицу маршрутизации (routing table), содержащую сетевые адреса, чтобы определить, куда направить пакет. Он делает это посредством сравнения сетевого адреса в пакете с элементами в таблице маршрутизации - если совпадение

найден, пакет направляется по указанному маршруту. Если же совпадение не найдено, обычно пакет отбрасывается.

Существуют два типа маршрутизирующих устройств: статические и динамические. Статические маршрутизаторы (static router) используют таблицы маршрутизации, которые должен создать и вручную обновлять сетевой администратор. С другой стороны, динамические маршрутизаторы (dynamic router) создают и обновляют свои собственные таблицы маршрутизации. Они используют информацию, как найденную на своих собственных сегментах, так и полученную от других динамических маршрутизаторов. Динамические маршрутизаторы всегда содержат свежую информацию о возможных маршрутах по сети, а также информацию об узких местах и задержках в прохождении пакетов. Эта информация позволяет им определить наиболее эффективный путь, доступный в данный момент, для перенаправления пакетов данных к их получателям.

Поскольку маршрутизаторы могут осуществлять интеллектуальный выбор пути и отфильтровывать пакеты, которые им не нужно получать, - они помогают уменьшить загрузку сети, сохранить ресурсы и увеличить пропускную способность. Кроме того, они повышают надежность доставки данных, поскольку маршрутизаторы могут выбрать для пакетов альтернативный путь, если маршрут по умолчанию недоступен.

Термин “маршрутизатор” (router) может обозначать элемент электронной аппаратуры, сконструированной специально для маршрутизации. Он также может означать компьютер (обеспеченный таблицей маршрутизации), подключенный к другим сегментам сети с помощью нескольких сетевых карт и,

следовательно, способный выполнять функции маршрутизации между связанными сегментами.

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных по сети. И в отличие от мостов для них можно отключить пересылку широковещательных сообщений, что уменьшает сетевой широковещательный трафик.

Другое важное преимущество маршрутизатора как соединительного устройства заключается в том, что, поскольку он работает на сетевом уровне, он может соединять сети, использующие различную сетевую архитектуру, методы доступа к устройствам или протоколы. Например, маршрутизатор может соединять подсеть Ethernet и сегмент Token Ring. Он может связывать несколько небольших сетей, использующих различные протоколы, если используемые протоколы поддерживают маршрутизацию.

Маршрутизаторы по сравнению с повторителями дороже и сложнее в управлении. У них меньшая пропускная способность, чем у мостов, поскольку они должны производить дополнительную обработку пакетов данных. Кроме того, динамические маршрутизаторы могут добавлять излишний трафик в сети, поскольку для обновления таблиц маршрутизации постоянно обмениваются сообщениями.

Английский термин “Brouter” (**мост-маршрутизатор**) представляет собой комбинацию слов “bridge” (мост) и “router” (маршрутизатор). Из этого можно сделать вывод, что мост-маршрутизатор сочетает функции моста и маршрутизатора. Когда мост-маршрутизатор получает пакет данных, он проверяет, послан пакет с использованием маршрутизируемого протокола или нет. Если это пакет маршрутизируемого протокола, мост-маршрутизатор

выполняет функции маршрутизатора, посылая при необходимости пакет получателю вне локального сегмента.

Если же пакет содержит немаршрутизируемый протокол, мост-маршрутизатор выполняет функции моста, используя адрес сетевой карты для поиска получателя на локальном сегменте. Для выполнения этих двух функций мост-маршрутизатор может поддерживать как таблицы маршрутизации, так и таблицы мостов.

Шлюз (gateway) представляет собой метод осуществления связи между двумя или несколькими сетевыми сегментами. В качестве шлюза обычно выступает выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать несходным системам в сети. Например, при использовании шлюза персональные компьютеры на базе Intel-совместимых процессоров на одном сегменте могут связываться и разделять ресурсы с компьютерами Macintosh.

Другой функцией шлюзов является преобразование протоколов. Шлюз может получить сообщение IPX/SPX, направленное клиенту, использующему другой протокол, например TCP/IP, на удаленном сетевом сегменте. После того как шлюз определяет, что получателем сообщения является станция TCP/IP, он действительно преобразует данные-сообщения в протокол TCP/IP. (В этом состоит отличие от моста, который просто пересылает сообщение, используя один протокол внутри формата данных другого протокола, - преобразование при необходимости происходит у получателя.) Почтовые шлюзы производят сходные операции по преобразованию почтовых сообщений и других почтовых передач из родного формата вашего приложения электронной почты в более универсальный почтовый протокол,

например SMTP, который может быть затем использован для направления сообщения в Интернет.

Хотя шлюзы имеют много преимуществ, нужно учитывать несколько факторов, которые должны учитываться при принятии решения об использовании шлюзов в сети. Шлюзы сложны в установке и настройке. Они также дороже других коммуникационных устройств. Вследствие лишнего этапа обработки, связанного с процессом преобразования, шлюзы работают медленнее, чем маршрутизаторы и подобные устройства.

1.7. Многоуровневые ИВС

Основу компьютерной сети составляет соединение различного оборудования, где одной из наиболее острых проблем является проблема совместимости. Без принятия всеми производителями общепринятых правил (стандартов) создания сетевого оборудования построение сетей в целом было бы невозможно. В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов.

Открытой системой может быть названа любая система (компьютер, вычислительная сеть, ОС, программный пакет, другие аппаратные и программные продукты), которая построена в соответствии с открытыми спецификациями.

Под термином «спецификация» (в вычислительной технике) понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с

другими компонентами, условий эксплуатации, ограничений и особых характеристик. Понятно, что не всякая спецификация является стандартом. В свою очередь, под открытыми спецификациями понимаются опубликованные, общедоступные спецификации, соответствующие стандартам и принятые в результате достижения согласия после всестороннего обсуждения всеми заинтересованными сторонами.

Использование при разработке систем открытых спецификаций позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Организация взаимодействия между устройствами в сети является сложной задачей, которая разбивается на несколько более простых задач-модулей. Процедура разбиения (декомпозиции) включает в себя четкое определение функций каждого модуля, решающего отдельную задачу, и интерфейсов между ними. В результате достигается логическое упрощение задачи, а также появляется возможность модификации отдельных модулей без изменения остальной части системы.

При декомпозиции часто используют многоуровневый подход. Он заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, то есть имеются вышележащие и нижележащие уровни (рис. 1.10). Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям

соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функции каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, и возможность их легкой замены.

Средства сетевого взаимодействия также могут быть представлены в виде иерархически организованного множества модулей. При этом модули нижнего уровня могут, например, решать все вопросы, связанные с надежной передачей электрических сигналов между двумя соседними узлами. Модули более высокого уровня организуют транспортировку сообщений в пределах всей сети, пользуясь для этого средствами упомянутого нижележащего уровня. А на верхнем уровне работают модули, предоставляющие пользователям доступ к различным службам - файловой, печати и т. п.

Многоуровневое представление средств сетевого взаимодействия имеет свою специфику, связанную с тем, что для организации обмена сообщениями между двумя компьютерами необходимо принять множество соглашений для всех уровней, начиная от самого низкого уровня передачи битов, и до самого высокого уровня, реализующего сервис для пользователей сети.

Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются **протоколом**.

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в

соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений, которые называются **интерфейсом**. Таким образом, протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы определяют правила взаимодействия модулей соседних уровней в одном узле.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется **стеком коммуникационных протоколов**. Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней - как правило, чисто программными средствами. На эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, в частности, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними.

Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами - концентраторами, мостами, коммутаторами, маршрутизаторами и т. д. Действительно, в общем случае связь компьютеров в сети осуществляется не напрямую, а через различные коммуникационные устройства. В зависимости от типа устройства в нем должны быть встроенные средства, реализующие тот или иной набор протоколов.

1.8. Эталонная модель взаимосвязи открытых систем

В начале 80-х годов ряд международных организаций по стандартизации - ISO, ITU и некоторые другие - разработали модель,

которая сыграла значительную роль в развитии сетей. Эта модель называется **моделью взаимодействия открытых систем** или моделью **OSI (Open System Interconnection)**. Модель OSI определяет различные уровни взаимодействия систем, дает им стандартные имена и указывает, какие функции должен выполнять каждый уровень. Модель OSI была разработана на основании большого опыта, полученного при создании компьютерных сетей, в основном глобальных, в 70-е годы. Полное описание этой модели занимает более 1000 страниц текста.

В модели OSI (рис. 1.11) средства взаимодействия делятся на семь уровней: прикладной, представительный, сеансовый, транспортный, сетевой, канальный и физический. Каждый уровень имеет дело с одним определенным аспектом взаимодействия сетевых устройств.

Физический уровень (Physical layer) имеет дело с передачей битов по физическим каналам связи, таким, например, как коаксиальный кабель, витая пара, оптоволоконный кабель или цифровой территориальный канал. К этому уровню имеют отношение характеристики физических сред передачи данных, такие как полоса пропускания, помехозащищенность, волновое сопротивление и другие. На этом же уровне определяются характеристики электрических сигналов, передающих дискретную информацию, например, крутизна фронтов импульсов, уровни напряжения или тока передаваемого сигнала, тип кодирования, скорость передачи сигналов. Кроме этого, здесь стандартизуются типы разъемов и назначение каждого контакта.

Функции физического уровня реализуются во всех устройствах, подключенных к сети. Со стороны компьютера

функции физического уровня выполняются сетевым адаптером или последовательным портом.

В некоторых сетях линии связи используются (разделяются) попеременно несколькими парами взаимодействующих компьютеров, и физическая среда передачи может быть занята. Поэтому одной из задач **канального уровня** (Data Link layer) является проверка доступности среды передачи. Другой задачей канального уровня является реализация механизмов обнаружения и коррекции ошибок. Для этого на канальном уровне биты группируются в наборы, называемые **кадрами**. Канальный уровень обеспечивает корректность передачи каждого кадра, помещая специальную последовательность бит в начало и конец каждого кадра, для его выделения, а также вычисляет контрольную сумму, обрабатывая все байты кадра определенным способом и добавляя контрольную сумму к кадру. Когда кадр приходит по сети, получатель снова вычисляет контрольную сумму полученных данных и сравнивает результат с контрольной суммой из кадра. Если они совпадают, кадр считается правильным и принимается. Если же контрольные суммы не совпадают, то фиксируется ошибка. Канальный уровень может не только обнаруживать ошибки, но и исправлять их за счет повторной передачи поврежденных кадров. Необходимо отметить, что функция исправления ошибок не является обязательной для канального уровня, поэтому в некоторых протоколах этого уровня она отсутствует.

К типовым топологиям, поддерживаемым протоколами канального уровня локальных сетей, относятся общая шина, кольцо и звезда, а также структуры, полученные из них с помощью мостов и коммутаторов. Примерами протоколов канального уровня являются протоколы Ethernet, Token Ring, FDDI.

В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи.

Для обеспечения качественной транспортировки сообщений в сетях любых топологий и технологий функций канального уровня оказывается недостаточно, поэтому в модели OSI решение этой задачи возлагается на два следующих уровня - сетевой и транспортный.

Сетевой уровень (Network layer) служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и обладать произвольной структурой связей.

На сетевом уровне сам термин **сеть** наделяют специфическим значением. В данном случае под сетью понимается совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий и использующих для передачи данных один из протоколов канального уровня, определенный для этой топологии.

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения

даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня. Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами. Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет.

Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

Сообщения сетевого уровня принято называть **пакетами** (packets). При организации доставки пакетов на сетевом уровне используется понятие «номер сети». В этом случае адрес получателя состоит из старшей части - номера сети и младшей - номера узла в этой сети. Все узлы одной сети должны иметь одну и ту же старшую часть адреса, поэтому термину «сеть» на сетевом уровне можно дать и другое, более формальное определение: сеть - это совокупность узлов, сетевой адрес которых содержит один и тот же номер сети.

Транспортный уровень (Transport layer) обеспечивает приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется. Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств

мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное - способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Сеансовый уровень (Session layer) обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. На практике немногие приложения используют сеансовый уровень, и он редко реализуется в виде отдельных протоколов, хотя функции этого уровня часто объединяют с функциями прикладного уровня и реализуют в одном протоколе.

Представительный уровень (Presentation layer) имеет дело с формой представления передаваемой по сети информации, не меняя при этом ее содержания. За счет уровня представления информация, передаваемая прикладным уровнем одной системы, всегда понятна прикладному уровню другой системы. С помощью средств данного уровня протоколы прикладных уровней могут преодолеть синтаксические различия в представлении данных или же различия в кодах символов, например кодов ASCII и EBCDIC. На этом уровне может выполняться шифрование и дешифрование данных, благодаря которому секретность обмена данными обеспечивается сразу для всех прикладных служб. Примером такого протокола является протокол SSL (Secure Socket Layer), который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Прикладной уровень (Application layer) - это набор разнообразных протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры или гипертекстовые Web-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Единица данных, которой оперирует прикладной уровень, обычно называется **сообщением** (message).

Сетезависимые и сетезависимые уровни

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп: либо к функциям, зависящим от конкретной технической реализации сети, либо к функциям, ориентированным на работу с приложениями.

Три нижних уровня - физический, канальный и сетевой - являются сетезависимыми, то есть протоколы этих уровней тесно связаны с технической реализацией сети и используемым коммуникационным оборудованием. Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровней во всех узлах сети.

Три верхних уровня - прикладной, представительный и сеансовый - ориентированы на приложения и мало зависят от технических особенностей построения сети. На протоколы этих уровней не влияют какие бы то ни было изменения в топологии сети, замена оборудования или переход на другую сетевую технологию. Так, переход от Ethernet на высокоскоростную технологию 100VG-AnyLAN не потребует никаких изменений в программных средствах, реализующих функции прикладного, представительного и сеансового уровней.

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это

позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений. Компьютер с установленной на нем сетевой ОС взаимодействует с другим компьютером с помощью протоколов всех семи уровней. Это взаимодействие компьютеры осуществляют опосредовано через различные коммуникационные устройства: концентраторы, модемы, мосты, коммутаторы, маршрутизаторы, мультиплексоры. В зависимости от типа коммуникационное устройство может работать либо только на физическом уровне (повторитель), либо на физическом и канальном (мост), либо на физическом, канальном и сетевом, иногда захватывая и транспортный уровень (маршрутизатор).

В модели OSI различаются два основных типа протоколов. В протоколах с **установлением соединения** (connection-oriented) перед обменом данными отправитель и получатель должны сначала установить соединение и, возможно, выбрать некоторые параметры протокола, которые они будут использовать при обмене данными. После завершения диалога они должны разорвать это соединение.

Вторая группа протоколов - протоколы **без предварительного установления соединения** (connectionless). Отправитель просто передает сообщение, когда оно готово. При взаимодействии компьютеров используются протоколы обоих типов.

Модель OSI касается только открытости средств взаимодействия устройств, связанных в вычислительную сеть. Здесь под открытой системой понимается сетевое устройство, готовое взаимодействовать с другими сетевыми устройствами с использованием стандартных правил, определяющих формат, содержание и значение принимаемых и отправляемых сообщений.

Это дает следующие преимущества:

- возможность построения сети из аппаратных и программных средств различных производителей, придерживающихся одного и того же стандарта;

- возможность безболезненной замены отдельных компонентов сети другими, более совершенными, что позволяет сети развиваться с минимальными затратами;

- возможность легкого сопряжения одной сети с другой;

- простота освоения и обслуживания сети.

Примером открытой системы является международная сеть Internet. Эта сеть развивалась в полном соответствии с требованиями, предъявляемыми к открытым системам. В разработке ее стандартов принимали участие тысячи специалистов-пользователей этой сети из различных университетов, научных организаций и фирм-производителей вычислительной аппаратуры и программного обеспечения, работающих в разных странах.

Стандартные стеки коммуникационных протоколов

Важнейшим направлением стандартизации в области вычислительных сетей является стандартизация коммуникационных протоколов. В настоящее время в сетях используется большое количество стеков коммуникационных протоколов. Наиболее популярными являются стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA и OSI. Все эти стеки, кроме SNA на нижних уровнях - физическом и канальном, - используют одни и те же хорошо стандартизованные протоколы Ethernet, Token Ring, FDDI и некоторые другие, которые позволяют использовать во всех сетях одну и ту же аппаратуру. Зато на верхних уровнях все стеки работают по своим собственным протоколам. Эти протоколы часто не соответствуют рекомендуемому моделью OSI разбиению на уровни. В частности, функции сеансового и представительного

уровня, как правило, объединены с прикладным уровнем. Такое несоответствие связано с тем, что модель OSI появилась как результат обобщения уже существующих и реально используемых стеков, а не наоборот.

Следует четко различать модель OSI и стек OSI. В то время как модель OSI является концептуальной схемой взаимодействия открытых систем, стек OSI представляет собой набор вполне конкретных спецификаций протоколов. В отличие от других стеков протоколов стек OSI полностью соответствует модели OSI, он включает спецификации протоколов для всех семи уровней взаимодействия, определенных в этой модели. На нижних уровнях стек OSI поддерживает Ethernet, Token Ring, FDDI, протоколы глобальных сетей, X.25 и ISDN, - то есть использует разработанные вне стека протоколы нижних уровней, как и все другие стеки. Протоколы сетевого, транспортного и сеансового уровней стека OSI специфицированы и реализованы различными производителями, но распространены пока мало. Наиболее популярными протоколами стека OSI являются прикладные протоколы. К ним относятся: протокол передачи файлов FTAM, протокол эмуляции терминала VTP, протоколы справочной службы X.500, электронной почты X.400 и ряд других.

Стек OSI - международный, независимый от производителей стандарт. Его поддерживает правительство США в своей программе GOSIP, в соответствии с которой 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 TCP/IP был разработан по инициативе Министерства обороны США более 20 лет назад для связи экспериментальной сети

ARPAnet с другими сетями как набор общих протоколов для разнородной вычислительной среды. Сегодня этот стек используется для связи компьютеров всемирной информационной сети Internet, а также в огромном числе корпоративных сетей.

Стек TCP/IP на нижнем уровне поддерживает все популярные стандарты физического и канального уровней: для локальных сетей - это Ethernet, Token Ring, FDDI, для глобальных - протоколы работы на аналоговых коммутируемых и выделенных линиях SLIP, PPP, протоколы территориальных сетей X.25 и ISDN.

Основными протоколами стека, давшими ему название, являются протоколы IP и TCP. Эти протоколы в терминологии модели OSI относятся к сетевому и транспортному уровням соответственно. IP обеспечивает продвижение пакета по составной сети, а TCP гарантирует надежность его доставки.

За долгие годы использования в сетях различных стран и организаций стек TCP/IP вобрал в себя большое количество протоколов прикладного уровня. К ним относятся такие популярные протоколы, как протокол пересылки файлов FTP, протокол эмуляции терминала Telnet, почтовый протокол SMTP, используемый в электронной почте сети Internet, гипертекстовые сервисы службы WWW и многие другие.

Контрольные вопросы к главе 1

1. Дайте определение сети.
2. В чем сходство и различие между локальными и глобальными телекоммуникационными сетями?
3. Сформулируйте достоинства и недостатки одноранговых сетей.

4. Сформулируйте достоинства и недостатки сетей с выделенным сервером.
5. Охарактеризуйте сетевую модель OSI.
6. Какие способы коммутации вы знаете? Охарактеризуйте их.
7. Какие топологии сетей вы знаете? Охарактеризуйте их.
8. Какие основные сетевые устройства вы знаете? Охарактеризуйте их.
9. Охарактеризуйте назначение сетевых карт (адаптеров).
10. Охарактеризуйте назначение и случаи применения повторителей и усилителей.
11. Охарактеризуйте назначение и случаи применения концентраторов.
12. Охарактеризуйте назначение и случаи применения мостов.
13. Охарактеризуйте назначение и случаи применения маршрутизаторов.
14. Охарактеризуйте назначение и случаи применения шлюзов.
15. Сформулируйте достоинства и недостатки беспроводных сетевых технологий.

Глава 2. Основные технические характеристики и качество компьютерных сетей и телекоммуникационных каналов

2.1. Показатели качества информационно-вычислительных сетей

Согласно Серии Международных Стандартов ISO 9000 **качество** - это совокупность свойств системы, позволяющих удовлетворять потребностям и ожиданиям потребителя. Рассмотрим основные показатели качества информационно-вычислительных сетей.

1. **Полнота выполняемых функций.** Сеть должна обеспечивать выполнение всех предусмотренных для нее функций по доступу ко всем ресурсам, по совместной работе узлов и по реализации всех протоколов и стандартов работы.

2. **Производительность** - среднее количество запросов пользователей сети, исполняемых за единицу времени.

3. **Пропускная способность** - важная характеристика производительности сети, определяется объемом данных, передаваемых через сеть (или ее звено - сегмент) за единицу времени. Часто используется другое название - **скорость передачи данных**.

4. **Надежность** сети - важная ее техническая характеристика, чаще всего характеризующаяся средним временем наработки на отказ.

5. **Достоверность** результатной информации - важная потребительская характеристика сети.

6. **Безопасность информации** в сети является важнейшим ее параметром, поскольку современные сети имеют дело с конфиденциальной информацией. Способность сети защитить

информацию от несанкционированного доступа и определяет степень ее безопасности.

7. **Прозрачность сети** - еще одна ее потребительская характеристика, означающая невидимость особенностей внутренней архитектуры сети для пользователя, он должен иметь возможность обращаться к ресурсам сети как к локальным ресурсам своего собственного компьютера.

8. **Масштабируемость** - это возможность расширения сети без заметного снижения ее производительности.

9. **Универсальность сети** - возможность подключения к ней разнообразного технического оборудования программного обеспечения от разных производителей.

В состав этих показателей качества сети входят важные технические характеристики, которые могут быть оценены и выражены количественными значениями измеряемых или вычисляемых величин: производительность, пропускная способность, надежность, достоверность результатной информации, безопасность информации.

Производительность ИВС, иначе называемая **вычислительной мощностью**, определяется тремя характеристиками:

- **временем реакции** сети на запрос пользователя;
- **пропускной способностью** сети;
- **задержкой передачи**.

Время реакции системы определяется как интервал времени между возникновением запроса пользователя (ЗП) к какой-либо сетевой службе и получением ответа на этот запрос и складывается из следующих составляющих:

- времени подготовки запроса на компьютере пользователя;

- времени передачи запроса через сегменты сети и промежуточное телекоммуникационное оборудование от пользователя к узлу сети, ответственному за его исполнение;
- времени выполнения (обработки) запроса в этом узле;
- времени передачи пользователю ответа на запрос;
- времени обработки полученного от сервера ответа на компьютере пользователя.

Значение времени реакции зависит от типа службы, к которой обращается пользователь, от того, какой пользователь и к какому узлу обращается, а также от состояния элементов сети на данный момент, а именно от загруженности сервера и сегментов, коммутаторов и маршрутизаторов, через которые проходит запрос и др. Поэтому на практике используется оценка времени реакции сети усредненная по пользователям, серверам, времени дня, от которого зависит загрузка сети. Эти сетевые составляющие времени реакции дают возможность оценить производительность отдельных элементов сети и выявить "узкие" места с целью модернизации сети для повышения общей производительности.

Значительную часть времени реакции составляет ***время передачи*** информации по телекоммуникациям сети, от длительности которого и зависит величина пропускной способности. Пропускная способность определяет скорость выполнения внутренних операций сети по передаче пакетов данных между узлами сети через коммутационные устройства и характеризует качество выполнения одной из основных функций сети - транспортировки сообщений. По этой причине при анализе производительности сети эта характеристика чаще используется, чем время реакции.

Пропускная способность, называемая в некоторых литературных источниках ***скоростью передачи данных***, измеряется

в Бодах (названных в честь французского ученого Э.Бодо), равных 1 бит/с, либо в пакетах в секунду и характеризует эффективность передачи данных.

Например, скорость передачи данных по кабельным линиям связи ЛВС от 10 Мбит/с, по телефонным каналам связи глобальных сетей - всего 1200 бит/с. Используются три понятия пропускной способности - средняя, мгновенная и максимальная. ***Средняя пропускная способность*** вычисляется делением объема переданных данных на время их передачи за длительный интервал времени (час, день, неделя). ***Мгновенная пропускная способность*** - средняя пропускная способность за очень маленький интервал: 10 мс или 1 с. ***Максимальная пропускная способность*** - это наибольшая мгновенная пропускная способность, зафиксированная за время наблюдения.

Пропускная способность может измеряться между двумя узлами или точками сети, например, между компьютером пользователя и сервера, между входным и выходным портами маршрутизатора. Общая пропускная способность любого составного пути сети будет равна ***минимальной*** из пропускных способностей составляющих элементов маршрута, поскольку пакеты передаются различными элементами сети последовательно. ***Общая пропускная способность сети*** характеризует качество сети в целом и определяется как среднее количество информации, переданной между всеми узлами сети в единицу времени.

Задержка передачи - это задержка между моментом поступления пакета на вход какого-нибудь сетевого устройства или части сети и моментом появления его на выходе этого устройства. Эта характеристика производительности отличается от времени реакции сети тем, что включает в себя только время этапов сетевой

обработки данных, без учета задержек обработки данных компьютерами сети. Практически величина задержки не превышает сотен миллисекунд, реже нескольких секунд и не влияет на качество файловой службы, служб электронной почты и печати с точки зрения пользователя. Однако такие задержки пакетов, переносящих изображение или речь, приводят к снижению качества предоставляемой пользователю информации из-за возникновения дрожания изображения, эффекта "эха", неразборчивости слов и т.п.

Задержка передачи и пропускная способность являются независимыми характеристиками, поэтому, не смотря на высокую пропускную способность, сеть может вносить значительные задержки при передаче каждого пакета.

2.2. Классификация каналов связи

Данные, изначально имеющие *аналоговую*, непрерывную форму, такие, как речь, фото и телевизионные изображения, телеметрическая информация, в последнее время все чаще передаются по каналам связи в дискретном виде, то есть в виде последовательности "нулей" и "единиц". Для преобразования непрерывного сигнала в дискретную форму производится *дискретная модуляция*, называемая также *кодированием*.

Применяются два типа кодирования данных. Первый - на основе непрерывного синусоидального несущего сигнала - называется *аналоговой модуляцией*, или просто модуляцией. Кодирование осуществляется за счет изменения параметров аналогового сигнала. Второй тип кодирования называется *цифровым кодированием* и осуществляется на основе последовательности прямоугольных импульсов. Эти способы

кодирования различаются шириной спектра передаваемого сигнала и сложностью аппаратуры для их реализации.

В зависимости от типа промежуточной аппаратуры все линии связи делятся на аналоговые и цифровые. Промежуточная аппаратура используется на линиях большой протяженности и решает две задачи - улучшение качества сигнала и создание составного канала связи между двумя абонентами. В *аналоговых* линиях промежуточная аппаратура предназначена для усиления аналоговых сигналов, то есть сигналов, которые имеют непрерывный диапазон значений. Такие линии традиционно применялись в телефонных сетях с узкой полосой частот, представителем которых является канал *тональной частоты*. Аналоговые линии используются для связи между собой телефонных станций, для создания высокоскоростных каналов, которые мультиплексируют несколько низкоскоростных аналоговых абонентских каналов. При аналоговом подходе для уплотнения низкоскоростных каналов абонентов в общий высокоскоростной канал обычно используется техника *разделения частот* или частотного мультиплексирования - FDM (Frequency Division Multiplexing). FDM - разбиение средств передачи на два и более каналов путем разделения полосы частот канала на узкие "подполосы", образующие каждая отдельный канал в одной и той же физической среде.

Современные телекоммуникационные системы и сети явились синтезом развития двух исходно независимых сетей - сетей электросвязи (телефонной, телеграфной, телетайпной и радиосвязи) и вычислительных сетей. Логика развития систем связи требовала применения цифровых систем передачи данных, а также применения вычислительных средств для решения задач

маршрутизации, управления трафиком, сигнализации; в свою очередь, логика развития вычислительной техники требовала все большего применения средств связи между периферийными устройствами и отдельными ЭВМ. Достигнутое в результате этих двух встречных движений совмещение техники связи с вычислительной техникой позволило усовершенствовать технологию обслуживания телефонной клиентуры и повысить эффективность отрасли связи, а также полнее использовать ресурсы вычислительных центров, вычислительных систем и сетей путем перераспределения их ресурсов и распараллеливания между ними задач и информационных потоков.

Многие сети общего пользования традиционных операторов являются в основном аналоговыми. Сети связи, создаваемые новыми операторами - цифровые, что обеспечивает внедрение современных служб и гарантирует перспективность этих сетей. В то же время существующие аналоговые сети активно используются для передачи информации как в аналоговой форме (телефония, радиотелефония, радиовещание и телевидение), так и для передачи дискретных (цифровых) данных. Носителем информации в телекоммуникационных каналах являются электрические сигналы (непрерывные, называемые аналоговыми, и дискретные или цифровые) и электромагнитные колебания - волны.

Линия связи (ЛС) - это физическая среда, по которой передаются информационные сигналы. В одной линии связи может быть организовано несколько **каналов связи** (КС) путем временного, частотного кодового и других видов разделения, тогда говорят о **логических (виртуальных)** каналах. Когда канал монополизирован линией связи, то он может называться физическим каналом и в этом случае совпадает с линией связи. Канал связи может быть

аналоговым или цифровым; в линии, как в физической среде, могут быть образованы каналы связи разного типа.

2.3. Типы цифровых каналов

Для передачи по цифровым каналам аналогового сообщения в виде непрерывной последовательности (телеметрические, метеорологические данные, данные систем контроля и управления) она предварительно оцифровывается. Частота оцифровки обычно равна порядка 8 кГц, через каждые 125 мкс значение величины аналогового сигнала отображается 8-разрядным двоичным кодом. Таким образом, скорость передачи данных составляет 64 кбит/с. Объединение нескольких таких базовых цифровых каналов в один (*мультиплексирование*) позволяет создавать более скоростные каналы: простейший мультиплексированный канал обеспечивает скорость передачи 128 кбит/с, более сложные каналы, например, мультиплексирующие 32 базовых канала, обеспечивают пропускную способность 2048 Мбит/с. С помощью цифровых каналов подключаются к магистралям также и офисные цифровые АТС.

Цифровые абонентские каналы в режиме коммутации каналов используются в наиболее распространенной цифровой сети с интеграцией услуг ISDN. По популярности сеть ISDN уступает лишь аналоговой телефонной сети. Адресация в ISDN организована так же, как и в телефонной сети, так как сеть создавалась для объединения существующих телефонных сетей с появляющимися сетями передачи данных. Поэтому сети ISDN позволяют объединять разнообразные виды связи (видео-, аудиопередачу данных, тексты, компьютерные данные и т.п.) со скоростями 64 кбит/с, 128 кбит/с, 2 Мбит/с и 155 Мбит/с на широкополосных каналах связи.

Заметим, что названием "ISDN" принято именовать и сеть, использующую технологию ISDN, и протокол, применяющий эту технологию.

Активно развиваются и другие типы цифровых систем, из которых следует отметить модификации технологии цифровых абонентских линий DSL (Digital Subscriber Line). HDSL (High Bit Rate DSL)- высокоскоростной вариант абонентской линии ISDN.

Конкуренцию ISDN и HDSL могут составить цифровые магистрали с синхронно-цифровой иерархией SDN (Synchronous Digital Hierarchy). В системе SDN имеется иерархия скоростей передачи данных. В магистралях SDN применяются оптоволоконные линии связи и частично радиолинии.

Контрольные вопросы к главе 2

1. Какими характеристиками определяется производительность ИВС?
2. Из каких составляющих состоит время реакции на запрос в вычислительной сети?
3. В каких единицах измеряется пропускная способность ИВС?
4. Чем различаются пропускные способности сети средняя, максимальная и мгновенная?
5. Чем отличаются задержка передачи информации в сети от времени реакции сети?
6. Назовите причины перехода от аналоговых каналов к цифровым.
7. Поясните, как проводится оцифровка дискретизированного непрерывного сигнала и из каких соображений выбирается частота дискретизации непрерывной временной последовательности.

8. Назовите, чем отличается цифровое кодирование информации от аналоговой модуляции.

9. Назовите преимущества цифровых методов связи по сравнению с методами аналоговой модуляции.

Глава 3. Линии связи сетей ЭВМ

3.1. Типы линий связи

Линия связи состоит в общем случае из физической среды, по которой передаются электрические информационные сигналы, аппаратуры передачи данных и промежуточной аппаратуры (рис. 3.1).

Физическая среда передачи данных может представлять собой кабель, то есть набор проводов, изоляционных и защитных оболочек и соединительных разъемов, а также земную атмосферу или космическое пространство, через которые распространяются электромагнитные волны.

В зависимости от среды передачи данных линии связи разделяются на следующие:

- проводные (воздушные);
- кабельные (медные и волоконно-оптические);
- радиоканалы наземной и спутниковой связи.

Проводные (воздушные) линии связи представляют собой провода без каких-либо изолирующих или экранирующих оплеток, проложенные между столбами и висящие в воздухе. По таким линиям связи традиционно передаются телефонные или телеграфные сигналы, но при отсутствии других возможностей эти линии используются и для передачи компьютерных данных. Скоростные качества и помехозащищенность этих линий оставляют желать много лучшего. Сегодня проводные линии связи быстро вытесняются кабельными.

Кабельные линии состоят из проводников, заключенных в несколько слоев изоляции: электрической, электромагнитной,

механической. Кроме того, кабель может быть оснащен разъемами, позволяющими быстро выполнять присоединение к нему различного оборудования. В компьютерных сетях применяются три основных типа кабеля: кабели на основе скрученных пар медных проводов, коаксиальные кабели с медной жилой, а также волоконно-оптические кабели.

Скрученная пара проводов называется **витой парой**. Витая пара существует в экранированном варианте, когда пара медных проводов обертывается в изоляционный экран, и неэкранированном, когда изоляционная обертка отсутствует. Скручивание проводов снижает влияние внешних помех на полезные сигналы, передаваемые по кабелю.

Коаксиальный кабель имеет несимметричную конструкцию и состоит из внутренней медной жилы и оплетки, отделенной от жилы слоем изоляции. Существует несколько типов коаксиального кабеля, отличающихся характеристиками и областями применения - для локальных сетей, для глобальных сетей, для кабельного телевидения и т. п.

Волоконно-оптический кабель состоит из тонких (5-60 микрон) волокон, по которым распространяются световые сигналы. Это наиболее качественный тип кабеля - он обеспечивает передачу данных с очень высокой скоростью (до 10 Гбит/с и выше) и к тому же лучше других типов передающей среды обеспечивает защиту данных от внешних помех.

Радиоканалы наземной и спутниковой связи образуются с помощью передатчика и приемника радиоволн. Существует большое количество различных типов радиоканалов, отличающихся как используемым частотным диапазоном, так и дальностью канала. Диапазоны коротких, средних и длинных волн (КВ, СВ и ДВ),

называемые также диапазонами амплитудной модуляции (Amplitude Modulation, AM) по типу используемого в них метода модуляции сигнала, обеспечивают дальнюю связь, но при невысокой скорости передачи данных. Более скоростными являются каналы, работающие на диапазонах ультракоротких волн (УКВ), для которых характерна частотная модуляция (Frequency Modulation, FM), а также диапазонах сверхвысоких частот (СВЧ или microwaves). В диапазоне СВЧ (свыше 4 ГГц) сигналы уже не отражаются ионосферой Земли, и для устойчивой связи требуется наличие прямой видимости между передатчиком и приемником. Поэтому такие частоты используют либо спутниковые каналы, либо радиорелейные каналы, где это условие выполняется.

В компьютерных сетях сегодня применяются практически все описанные типы физических сред передачи данных, но наиболее перспективными являются волоконно-оптические. На них сегодня строятся как магистрали крупных территориальных сетей, так и высокоскоростные линии связи локальных сетей. Популярной средой является также витая пара, которая характеризуется отличным соотношением качества к стоимости, а также простотой монтажа. С помощью витой пары обычно подключают конечных абонентов сетей на расстояниях до 100 метров от концентратора. Спутниковые каналы и радиосвязь используются чаще всего в тех случаях, когда кабельные связи применить нельзя - например, при прохождении канала через малонаселенную местность или же для связи с мобильным пользователем сети.

3.2. Характеристики линий связи

К основным характеристикам линий связи относятся:

амплитудно-частотная характеристика;

полоса пропускания;
затухание;
помехоустойчивость;
перекрестные наводки на ближнем конце линии;
пропускная способность;
достоверность передачи данных;
удельная стоимость.

В первую очередь разработчика вычислительной сети интересуют пропускная способность и достоверность передачи данных, поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети.

Амплитудно-частотная характеристика (рис. 3.2) показывает, как затухает амплитуда синусоиды на выходе линии связи по сравнению с амплитудой на ее входе для всех возможных частот передаваемого сигнала.

Знание амплитудно-частотной характеристики реальной линии позволяет определить форму выходного сигнала практически для любого входного сигнала. Для этого необходимо найти спектр входного сигнала, преобразовать амплитуду составляющих его гармоник в соответствии с амплитудно-частотной характеристикой, а затем найти форму выходного сигнала, сложив преобразованные гармоники.

На практике вместо амплитудно-частотной характеристики применяются другие, упрощенные характеристики, например, полоса пропускания и затухание.

Полоса пропускания (bandwidth) - это непрерывный диапазон частот, для которого отношение амплитуды выходного сигнала к входному превышает некоторый заранее заданный предел, обычно 0,5 (рис. 3.2). То есть, полоса пропускания определяет диапазон

частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений.

Затухание (attenuation) определяется как относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты. Таким образом, затухание представляет собой одну точку из амплитудно-частотной характеристики линии.

Затухание A обычно измеряется в децибелах (дБ, decibel - dB) и вычисляется по следующей формуле:

$$A = 10 \log_{10} P_{\text{вых}} / P_{\text{вх}},$$

где $P_{\text{вых}}$ - мощность сигнала на выходе линии, $P_{\text{вх}}$ - мощность сигнала на входе линии.

Так как мощность выходного сигнала кабеля без промежуточных усилителей всегда меньше, чем мощность входного сигнала, затухание кабеля всегда является отрицательной величиной.

Полоса пропускания зависит от типа линии и ее протяженности.

Пропускная способность (throughput) линии характеризует максимально возможную скорость передачи данных по линии связи. Пропускная способность измеряется в битах в секунду - бит/с, а также в производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д.

Связь между полосой пропускания линии и ее максимально возможной пропускной способностью выражается формулой Шеннона:

$$C = F \log_2 (1 + P_c / P_{\text{ш}}),$$

где C - максимальная пропускная способность линии в битах в секунду, F - ширина полосы пропускания линии в герцах, P_c - мощность сигнала, $P_{ш}$ - мощность шума.

Помехоустойчивость линии определяет ее способность уменьшать уровень помех, создаваемых во внешней среде, на внутренних проводниках. Помехоустойчивость линии зависит от типа используемой физической среды, а также от экранирующих и подавляющих помехи средств самой линии. Наименее помехоустойчивыми являются радиолинии, хорошей устойчивостью обладают кабельные линии и отличной - волоконно-оптические линии, малочувствительные к внешнему электромагнитному излучению. Обычно для уменьшения помех, появляющихся из-за внешних электромагнитных полей, проводники экранируют и/или скручивают.

Перекрестные наводки на ближнем конце (Near End Cross Talk - NEXT) определяют помехоустойчивость кабеля к внутренним источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре проводников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель перекрестных наводок NEXT, выраженный в децибелах, представляется формулой

$$NEXT = 10 \log P_{\text{вых}} / P_{\text{нав}},$$

где $P_{\text{вых}}$ - мощность выходного сигнала, $P_{\text{нав}}$ - мощность наведенного сигнала.

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Величина этого показателя для каналов связи без дополнительных средств защиты

от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило, 10^{-4} - 10^{-6} , в оптоволоконных линиях связи - 10^{-9} . Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10000 бит искажается значение одного бита.

Искажения бит происходят как из-за наличия помех на линии, так и по причине искажений формы сигнала ограниченной полосой пропускания линии. Поэтому для повышения достоверности передаваемых данных нужно повышать степень помехозащищенности линии, снижать уровень перекрестных наводок в кабеле, а также использовать более широкополосные линии связи.

Стандарты кабелей

В компьютерных сетях применяются кабели, удовлетворяющие определенным стандартам, что позволяет строить кабельную систему сети из кабелей и соединительных устройств разных производителей.

Кабели на основе неэкранированной витой пары (Unshielded Twisted Pair - UTP)

Стандартом определено пять категорий UTP. Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки (рис. 3.3). Обычно две пары предназначены для передачи данных, а две - для передачи голоса.

Таблица 3.1 Категории кабелей на основе неэкранированной витой пары

Категория	Характеристики
1	Телефонный кабель для передачи аналоговых сигналов
2	Кабель из 4 витых пар, способный передавать данные со скоростью 4 Мбит/с

3	Кабель из 4 витых пар, способный передавать данные со скоростью 10 Мбит/с
4	Кабель из 4 витых пар, способный передавать данные со скоростью 16 Мбит/с
5	Кабель из 4 витых пар, способный передавать данные со скоростью 100 Мбит/с

Наиболее важные электромагнитные характеристики кабеля категории 5 имеют следующие значения:

полное волновое сопротивление в диапазоне частот до 100 МГц равно 100 Ом (стандарт ISO 11801 допускает также кабель с волновым сопротивлением 120 Ом, волновое сопротивление – сопротивление переменному току);

величина перекрестных наводок NEXT в зависимости от частоты сигнала должна принимать значения не менее 74 дБ на частоте 150 кГц и не менее 32 дБ на частоте 100 МГц;

затухание имеет предельные значения от 0,8 дБ (на частоте 64 кГц) до 22 дБ (на частоте 100 МГц);

активное сопротивление не должно превышать 9,4 Ом на 100 м;

емкость кабеля не должна превышать 5,6 нФ на 100 м.

Для соединения кабелей с оборудованием используются вилки и розетки RJ-45, представляющие 8-контактные разъемы, похожие на обычные телефонные разъемы RJ-11 (рис. 3.4).

Кабели на основе экранированной витой пары (Shielded Twisted Pair - STP)

Экранированная витая пара STP хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления.

Экранированный кабель применяется только для передачи данных, голос по нему не передают.

Основным стандартом, определяющим параметры экранированной витой пары, является фирменный стандарт IBM. В этом стандарте кабели делятся не на категории, а на типы: Type I, Type 2,..., Type 9.

Основным типом экранированного кабеля является кабель Type 1 стандарта IBM. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5, однако волновое сопротивление кабеля Type 1 равно 150 Ом.

Для присоединения экранированных кабелей к оборудованию используются разъемы конструкции IBM.

Коаксиальные кабели

Существует большое количество типов коаксиальных кабелей, используемых в сетях различного типа - телефонных, телевизионных и компьютерных.

Для организации компьютерных сетей используются два типа коаксиальных кабелей (рис. 3.5):

- тонкий коаксиальный кабель;
- толстый коаксиальный кабель.

Тонкий коаксиальный кабель – гибкий кабель диаметром примерно 0,5см. Он способен передавать сигнал на расстояние до 185 м без его заметного искажения, вызванного затуханием. Волновое сопротивление кабеля составляет 50 Ом.

Таблица 3.2. Таблица кодировки тонких коаксиальных кабелей

Кабель	Характеристики кабеля
RG58 /U	Сплошная медная жила

RG58 A/U	Переплетенные провода
RG58 C/U	Военный стандарт для RG58 A/U
PK50	Отечественный аналог

Для подключения кабеля используются специальные разъемы типа BNC (Bayonet Naval Connector) (рис. 3.6).

Кабель RG58 позволяет реализовать топологии шина и кольцо и был до последнего времени самым распространенным при построении сетей.

Толстый коаксиальный кабель – относительно жесткий кабель диаметром около 1 см. Медная жила кабеля толще, чем у тонкого коаксиального кабеля и, следовательно, сопротивление меньше. Поэтому толстый коаксиальный кабель передает сигналы дальше, чем тонкий, до 500 м.

Для подключения к толстому коаксиальному кабелю применяют специальное устройство – трансивер. Трансивер снабжен специальным коннектором, который “прокусывает” изоляционный слой и осуществляет контакт с проводящей жилой.

Волоконно-оптические кабели

Волоконно-оптические линии предназначены для перемещения больших объемов данных на высоких скоростях. Оптоволоконный кабель состоит из центрального стеклянного или пластикового проводника, окруженного другим слоем стеклянного или пластикового покрытия, и внешней защитной оболочки (рис. 3.7).

Данные передаются по кабелю с помощью лазерного (laser transmitter) или светодиодного (LED, light-emitting diode transmitter) передатчика, который посылает однонаправленные световые импульсы через центральное стеклянное волокно. Стеклянное покрытие помогает поддерживать фокусировку света во внутреннем

проводнике. Сигнал принимается на другом конце фотодиодным приемником (photodiode receiver), преобразующим световые импульсы в электрический сигнал, который сможет использовать получающий компьютер.

Конструкций световодов и оптических волокон очень много, но основных типов два:

многомодовый;

одномодовый.

Диаметр сердцевины у многомодовых волокон в десятки раз превышает длину волны передаваемого излучения, из-за чего по волокну распространяется несколько типов волн (мод). Стандартные диаметры сердцевины многомодовых волокон – 50 и 62,5 мкм.

У одномодового волокна диаметр сердцевины находится обычно в пределах 5–10 мкм. Диаметр кварцевой оболочки световода тоже стандартизован и составляет 125 мкм.

Скорость передачи данных для оптоволоконных сетей находится в диапазоне от 100 Мбит/с до 2 Гбит/с, а данные могут быть надежно переданы на расстояние до 2 километров без повторителя. Оптоволоконный кабель может поддерживать передачу видео и голосовой информации так же, как и передачу данных. Поскольку световые импульсы полностью закрыты в пределах внешней оболочки, оптоволоконный носитель фактически невосприимчив к внешней интерференции и подслушиванию. Эти качества делают оптоволоконный кабель привлекательным выбором для защищенных сетей или сетей, которые требуют очень быстрой передачи на большие расстояния.

Поскольку световые импульсы могут двигаться только в одном направлении, системы на базе оптоволоконных кабелей должны иметь входящий кабель и исходящий кабель для каждого

сегмента, который будет посылать и получать данные. Волоконный кабель также жесток и сложен в установке, что делает его самым дорогим типом сетевого носителя. Волоконный носитель требует специальных соединителей - коннекторов и высококвалифицированной установки. Эти факторы в дальнейшем приведут к высокой стоимости внедрения. Одним способом снижения расходов является ограничение использования волоконного кабеля сетевыми магистралями: или теми областями, где имеют значение влияние электромагнитного наложения, возгораемость или другие вопросы окружения.

При проектировании или расширении сетей нужно принимать во внимание факторы, перечисленные в таблице.

Таблица 3.3. Сравнительные характеристики кабелей

Тип кабеля	Скорость передачи, Мбит/с	Длина передачи, м	Простота установки	Подверженность помехам	Стоимость
Неэкранированная витая пара	100	100	Прост в установке	Подвержен помехам	Самый дешевый
Тонкий коаксиальный	10	185	Прост в установке	Хорошая защита от помех	Дороже витой пары
Толстый коаксиальный	10	500	Прост в установке	Хорошая защита от помех	Дороже тонкого коаксиального кабеля
Оптоволоконный	100-2000	2000	Труден в установке	Не подвержен помехам	Самый дорогой

3.3. Беспроводные каналы связи

В дополнение к традиционным физическим носителям, методы беспроводной передачи данных могут являться удобной, а иногда и неизбежной альтернативой кабельным соединениям. Беспроводные технологии различаются по типам сигнала, частоте (большая частота означает большую скорость передачи) и расстоянию передачи. Тремя главными типами беспроводной

передачи данных являются радиосвязь, связь в микроволновом диапазоне и инфракрасная связь.

Радиосвязь

Технологии радиосвязи (Radio Waves) пересылают данные на радиочастотах и практически не имеют ограничений по дальности. Она используется для соединения локальных сетей на больших географических расстояниях. Радиопередача в целом имеет высокую стоимость, подлежит государственному регулированию и крайне чувствительна к электронному и атмосферному наложению. Она также подвержена перехвату, поэтому требует шифрования или другой модификации при передаче, чтобы обеспечить разумный уровень безопасности.

Связь в микроволновом диапазоне

Передача данных в микроволновом диапазоне (Microwaves) использует высокие частоты и применяется как на коротких расстояниях, так и в глобальных коммуникациях. Их главное ограничение заключается в том, что передатчик и приемник должны быть в зоне прямой видимости друг друга. Передача данных в микроволновом диапазоне обычно используется для соединения локальных сетей в отдельных зданиях, где использование физического носителя затруднено или непрактично. Связь в микроволновом диапазоне также широко используется в глобальной передаче с помощью спутников и наземных спутниковых антенн, обеспечивающих выполнение требования прямой видимости (рис. 3.8). Спутники в системах связи могут находиться на геостационарных (высота 36 тысяч км) или низких орбитах. При геостационарных орбитах заметны задержки на прохождение сигналов (туда и обратно около 520 мс). Возможно покрытие поверхности всего земного шара с помощью четырех спутников. В

низкоорбитальных системах обслуживание конкретного пользователя происходит попеременно разными спутниками. Чем ниже орбита, тем меньше площадь покрытия и, следовательно, нужно или больше наземных станций, или требуется межспутниковая связь, что естественно утяжеляет спутник. Число спутников также значительно больше (обычно несколько десятков). Например, глобальная спутниковая сеть Iridium, имеющая и российский сегмент, включает 66 низкоорбитальных спутников, диапазон частот 1610-1626,5 МГц.

Инфракрасная связь

Инфракрасные технологии (infrared transmissions), функционирующие на очень высоких частотах, приближающихся к частотам видимого света, могут быть использованы для установления двусторонней или широковещательной передачи на близких расстояниях. Они обычно используют светодиоды (LED, light-emitting diode) для передачи инфракрасных волн приемнику. Поскольку они могут быть физически заблокированы и испытывать интерференцию с ярким светом, инфракрасная передача ограничена малыми расстояниями в зоне прямой видимости. Инфракрасная передача обычно используется в складских или офисных зданиях, иногда для связи двух зданий. Другим популярным использованием инфракрасной связи является беспроводная передача данных в портативных компьютерах.

3.4. Системы мобильной связи

Системы мобильной связи осуществляют передачу информации между пунктами, один или оба из которых являются подвижными. Характерным признаком систем мобильной связи

является применение радиоканала. К технологиям мобильной связи относятся пейджинг, твейджинг, сотовая телефония.

Пейджинг - система односторонней связи, при которой передаваемое сообщение поступает на пейджер пользователя, извещая его о необходимости предпринять то или действие или просто информируя его о тех или иных текущих событиях. Это наиболее дешевый вид мобильной связи.

Твейджинг - это двухсторонний пейджинг. В отличие от пейджинга возможно подтверждение получения сообщения и даже проведение некоторого подобия диалога.

Сотовые технологии обеспечивают телефонную связь между подвижными абонентами (ячейками). Связь осуществляется через базовые (стационарных) станции, выполняющие коммутирующие функции.

Разработано несколько стандартов мобильной связи.

Одной из наиболее широко распространенных технологий мобильной связи (в том числе и в России) является технология, соответствующая стандарту для цифровых сетей сотовой связи GSM (Global System for Mobile Communications). GSM может поддерживать интенсивный трафик (270 кбит/с), обеспечивает роуминг (т.е. автоматическое отслеживание перехода мобильного пользователя из одной соты в другую), допускает интеграцию речи и данных и связь с сетями общего пользования. Используются разновидности: сотовая связь GSM-900 в частотном диапазоне 900 МГц (более точно 890-960 МГц), и микросотовая связь GSM-1800 в диапазоне 1800 МГц (1710-1880 МГц). Название микросотовая обусловлено большим затуханием и, следовательно, меньшей площадью соты. Однако увеличение числа каналов выгодно при

высокой плотности абонентов. Мощность излучения мобильных телефонов - 1-2 Вт.

Архитектура GSM-системы представлена на рис. 3.9. В каждой соте действует базовая станция BTS (Base Transciever Station), обеспечивающая прием и передачу радиосигналов абонентам. Базовая станция имеет диапазон частот, отличный от диапазонов соседних сот. Мобильная ячейка прослушивает соседние базовые станции и сообщает контроллеру базовых станций (BSC - Base Station Controller) о качестве приема с тем, чтобы контроллер мог своевременно переключить ячейку на нужную станцию. Центр коммутации (MSC - Mobile services Switching Centre) осуществляет коммутацию и маршрутизацию, направляя вызовы нужному абоненту, в том числе во внешние сети общего пользования. В базе данных хранятся сведения о местоположении пользователей, технических характеристиках мобильных станций, данные для идентификации пользователей.

Контрольные вопросы к главе 3

1. Дайте определение линии связи
2. Дайте определение физической среды передачи данных
3. Как классифицируются линии связи?
4. Перечислите основные характеристики линий связи
5. Дайте определение амплитудно-частотной характеристики, полосы пропускания, затухания, пропускной способности линий связи
6. Охарактеризуйте помехоустойчивость, перекрестные наводки, достоверность передачи данных линий связи
7. Перечислите основные типы кабелей

8. Дайте характеристику кабелей на основе неэкранированной витой пары
9. Дайте характеристику кабелей на основе экранированной витой пары
10. Дайте характеристику коаксиальным кабелям
11. Охарактеризуйте волоконно-оптические кабели
12. Дайте характеристику беспроводным каналам связи
13. Каким будет теоретический предел скорости передачи данных в битах в секунду по каналу с шириной полосы пропускания в 10 кГц, если мощность передатчика составляет 0,01 мВт, а мощность шума в канале равна 0,0001 мВт?

Глава 4. Локальные вычислительные сети

4.1. Характеристики локальных сетей

Локальными сетями называют частные сети, размещающиеся в одном здании или на территории какой-либо организации размерами до нескольких километров. Их часто используют для объединения компьютеров и рабочих станций в офисах компании или предприятия для обмена информацией и предоставления совместного доступа к ресурсам сети (принтерам, сканерам и др.).

Локальные вычислительные сети (ЛВС) применяются и при разработке коллективных проектов, например сложных программных комплексов. На базе ЛВС можно создавать системы автоматизированного проектирования. Это позволяет реализовывать новые технологии проектирования изделий машиностроения, радиоэлектроники и вычислительной техники. В условиях развития рыночной экономики появляется возможность создавать конкурентоспособную продукцию, быстро модернизировать ее, обеспечивая реализацию экономической стратегии предприятия. Кроме того, ЛВС позволяют реализовывать новые информационные технологии в системах организационно-экономического управления, а в учебных лабораториях вузов они позволяют повысить качество обучения и внедрять современные интеллектуальные технологии обучения.

Локальные сети характеризуются: размерами, технологией передачи данных и топологией их построения.

Под *размерами* локальных сетей понимают длину сетевого кабеля, соединяющего компьютеры. Они могут находиться в пределах от 10м до 1 км.

По *технологии* организации локальные сети подразделяют на *широковещательные* и сети с передачей от "*точки к точке*" (point-to-point).

Широковещательные сети обладают единым каналом связи, совместно используемым всеми машинами сети. Пакеты, передаваемые одной машиной, получают все компьютеры сети. Пакет имеет поле "адрес", по которому, благодаря дешифратору адреса, только одна машина, которой предназначается сообщение, считывает его, а затем обрабатывает. Остальные машины игнорируют это сообщение. Такие технологии с успехом используются в небольших локальных сетях.

Сети с передачей от "точки к точке" состоят из большого числа соединенных машин и используются, в отличие от предыдущей технологии, в больших корпоративных сетях. Передаваемые пакеты проходят через ряд промежуточных машин по некоему ранее вычисленному алгоритму пути от источника к получателю.

Существует три основные *топологии* сети, рассмотренные в разделе 1.5: *шинная*, *кольцевая* и топология типа "*звезда*", которые, обладают свойством *однородности*, то есть все компьютеры в такой сети имеют равные права в отношении доступа к другим компьютерам. Такая однородность структуры делает простой процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети. Однако, при этом в таких сетях использование типовых структур порождает различные ограничения, важнейшими из которых являются:

ограничения на длину связи между узлами;

ограничения на количество узлов;

ограничения на интенсивность трафика, порождаемого узлами сети.

Для снятия этих ограничений используются специальные *структуризации* сети и специальное *структурообразующее оборудование* - повторители, концентраторы, мосты, коммутаторы, маршрутизаторы.

4.2. Методы доступа к среде передачи данных

Под *доступом к сети* понимают взаимодействие компьютера в сети *со средой передачи данных* для обмена информацией с другими ЭВМ.

В настоящее время наиболее распространенными методами доступа (правами на передачу информации) к локальной сети являются (рис. 4.1):

случайный доступ CSMA/CS (carrier sense multiple access with collision detection) - множественный доступ с контролем несущей и обнаружением конфликтов.

маркерные методы - на основе маркерной шины и маркерного кольца.

Существует две разновидности метода случайного доступа: *CSMA/CS* - множественный доступ с контролем несущей и обнаружением конфликтов и *приоритетный доступ*

4.2.1. Множественный доступ с контролем несущей и обнаружением конфликтов

В сетях, где станции передают пакеты данных в случайные моменты времени, вероятность возникновения конфликтов очень велик. *Конфликты* (столкновения, коллизии) возникают, когда два или более компьютеров "одновременно" пытаются захватить линию. В результате происходит столкновение двух кадров на общем кабеле, что приводит к искажению передаваемой информации.

Если организовать процесс передачи данных таким образом, чтобы станции прослушивали передачу данных другими станциями, то можно значительно увеличить коэффициент использования сети. Этот принцип и называется **контролем несущей CSMA**.

Когда у станции появляются данные для передачи, она сначала прослушивает канал, проверяя, свободен он или занят. Если канал занят, станция ждет, пока он не освободится, а затем начинает передавать данные.

Существует вероятность того, что как только станция начнет передачу, другая станция, также оказавшись готовой к передаче данных, начнет передавать пакет, в результате чего возникнет конфликт. Если происходит столкновение пакетов, станция ждет некоторое время, а затем начинает прослушивать канал и, если он свободен, пытается передать этот пакет еще раз. Чем больше время распространения сигнала, тем выше вероятность столкновений и ниже производительность метода передачи данных.

Обнаружение столкновений - аналоговый процесс. Аппаратура станции должна прослушивать коаксиальный кабель во время передачи. Если принятая информация отличается от переданной, то станция понимает, что произошло столкновение и прекращает передачу.

4.2.2. Приоритетный доступ

При этом способе концентратор, получив одновременно два запроса, отдает предпочтение тому, который имеет более высокий **приоритет**. Эта технология реализуется в виде системы с опросом. Интеллектуальный концентратор, опрашивает подключенные к нему компьютеры, и при наличии у нескольких из них запроса на передачу, разрешает передать пакет данных тому, у которого

приоритет, установленный для него, выше. Одним из примеров такого доступа является технология 100 VG (Voice Grade - голосовой канал) Any Lan, обладающая следующими возможностями:

скорость передачи данных - более 100 Мбит/сек;

поддержка структурированной кабельной системы на основе витой пары и оптоволоконного кабеля.

4.2.3. Маркерные методы доступа

К маркерным методам доступа относятся два наиболее известных типа передачи данных по локальной сети: **маркерная шина** (стандарт IEEE 802.4) и **маркерное кольцо** (стандарт IEEE 802.5)

Маркер - управляющая последовательность бит, передаваемая компьютером по сети. Маркер предназначен для управления доступом к сети компьютеров в маркерных методах доступа.

Маркер включает в себя три поля длиной в один байт каждый (рис.4.2): начальный ограничитель SD (Start Delimiter), представляющий собой уникальную последовательность JK00JK000, которую нельзя спутать ни с одной битовой последовательностью внутри кадра; управление доступом AC (Access Control), состоящее в свою очередь еще из четырех полей: PPP - битов приоритета, бита маркера - Т (при Т = 1 - передаваемый кадр - маркер доступа), бита монитора - М (устанавливается в 1 активным монитором, и в 0 другими станциями сети), RRR - резервные биты; конечный ограничитель ED (End Delimiter), который, как и начальный ограничитель, содержит уникальную последовательность JK1LK1, а также два бита признаков: I (Intermediate), указывающий, является

ли кадр последним в серии кадров или промежуточным ($I=1$), E (Error) - признак ошибки.

Станция, имеющая данные для передачи, получив маркер, изымает его из кольца, тем самым получая право на передачу информации, заменяет его кадром данных установленного формата, содержащего следующие поля: начальный ограничитель SD, управление кадром FC (Frame Control), адрес назначения DA (Destination Address), адрес источника SA (Source Address), данные (INFO), контрольная сумма (INFO), контрольная сумма FCS, конечный ограничитель ED, статус кадра FS (Frame Status).

4.3. Локальные сети на основе маркерной шины

Физически *маркерная шина* представляет собой линейный или древовидный кабель, к которому присоединены станции. Самой распространенной реализацией данного построения являются сети ArcNet. Логически соединение станций организовано в кольцо, в котором каждая станция знает адреса своих соседей "слева" и "справа". При инициализации логического кольца право посылать кадр получает станция с наибольшим номером. Переслав кадр, она передает право пересылки своему ближайшему соседу, посылая ему специальный управляющий кадр, называемый маркером (рис. 4.3).

Маркер перемещается по логическому кольцу, при этом право передачи кадров имеет только держатель маркера. Поскольку в каждый момент времени маркер может находиться только у одной станции, столкновений не происходит.

Физический порядок, в котором станции соединены кабелем, не имеет значения. Поскольку кабель является широковещательной средой, каждая станция получает каждый кадр, игнорируя кадры, адресованные не ей. Передавая маркер, станция посылает

маркерный кадр своему логическому соседу по кольцу, независимо от его физического расположения.

Инициализация кольца осуществляется следующим образом. Когда все станции выключены и одна из них переходит в подключенный режим, она замечает, что в течение определенного периода в сети нет трафика (по сети ничего не передается). Тогда она посылает широковещательный запрос с требованием маркера. Не услышав никаких конкурентов, претендующих на маркер, она сама создает маркер и кольцо, состоящее из одной станции. Периодически она посылает управляющий кадр, предлагающий другим станциям присоединиться к кольцу. Пример передаваемого кадра при маркерной организации сети представлен на рисунке 4.4. Когда новые станции включаются, они отвечают на эти предложения и присоединяются к кольцу. При этом ее соседи «слева» и «справа» запоминают адрес вновь включенной в кольцо машины и провозглашают ее своим соседом.

При выходе из кольца некой станции она посылает своему предшественнику кадр, информирующий его о том, что с этого момента в место нее будет ее преемник. После чего она прекращает передачу.

Если некая станция выходит из строя, то если ее преемник не начал передавать кадры и не передал маркер дальше, маркер посылается еще раз. Если и после этого станция-приемник не ответила, то посылается широковещательный запрос с информацией об адресе преемника и о станции, которая должна быть следующей. Когда некая станция видит этот запрос с адресом своего предшественника - она широковещательным ответом провозглашает преемником себя, и вышедшая из строя станция удаляется из кольца.

Если станция выбывает из кольца вместе с маркером, то происходит инициализация кольца заново.

4.4. Сети на основе маркерного кольца

Локальные сети на основе *маркерного кольца (Token Ring)* строятся на кольцевой архитектуре, что подразумевает индивидуальные соединения "точка-точка". Управляющая станция генерирует специальное сообщение - маркер (token) и последовательно передает его всем компьютерам. Правом передачи данных обладает единственный компьютер, располагающий маркером. Как только маркер достигает станции, которая собирается передавать данные, последняя "присваивает" маркер себе и изменяет его статус на "занято". Затем маркер дополняется всей информацией, которую предполагалось передать, и снова отправляется в сеть. Маркер будет циркулировать в сети до тех пор, пока не достигнет адресата информации. Получающая сторона обрабатывает полученную вместе с маркером информацию и опять передает маркер в сеть. Когда маркер возвращается к исходной станции, он удаляется, после чего генерируется новый маркер. Циркуляция начинается заново (рис 4.5).

Серьезным недостатком такого типа построения сетей является то, что разрыв кабеля в одной точке приводит к полной остановке работоспособности сети.

На основе маркерного кольца строятся локальные сети Token Ring. В настоящее время существует две разновидности этого типа сетей с пропускной способностью 4 Мбит/с и 16 Мбит/с.

Одним из важнейших параметров сети является *время реакции* на запрос пользователя (T_p) – промежуток времени между моментом готовности подать запрос в сеть и моментом получения

ответа на запрос, то есть возвращения отправленного кадра, что является подтверждением в получении этого кадра адресатом и

$$T_p = T_{ож} + T_{обсл}, \quad (4.1)$$

где $T_{ож}$ – максимальное время ожидания подачи кадра, $T_{обсл}$ – время обслуживания запроса.

С учетом того, что

$$T_{ож} = (N_{рс} - 1) T_{об},$$

где $N_{рс}$ – количество рабочих станций, а $T_{об}$ – время в течение которого маркер вместе с кадром совершает полный оборот в моноканале и

$$T_{об} = T_c + T_k + T_{сз}, \quad (4.2)$$

где T_c – время распространения сигнала в передающей среде через весь моноканал, T_k – время передачи кадра через моноканал, $T_{сз}$ – время задержки передаваемого кадра по кольцу в узлах сети и, исходя из того, что

$$T_c = S_k/V_c; T_k = C_k/V_k; T_{сз} = N_{рс} * T_з,$$

где S_k – длина кольцевого моноканала, V_c – скорость распространения сигнала, C_k – длина маркера и кадра, V_k – скорость передачи данных, $T_з$ – время задержки маркера и кадра узлом, получаем

$$T_{об} = S_k/V_c + C_k/V_k + N_{рс} * T_з \quad (4.3)$$

и

$$T_{ож} = (N_{рс} - 1) (S_k/V_c + C_k/V_k + N_{рс} * T_з)$$

Тогда, с учетом формул (4.1) и (4.3) имеем

$$T_p = (N_{рс} - 1) (S_k/V_c + C_k/V_k + N_{рс} * T_з) + T_{обсл} \quad (4.4)$$

Пример 4.1. Определить время реакции на запрос пользователя в локальной сети построенной на топологии «маркерное кольцо» если

известно, что $N_{pc} = 25$, $S_k = 12,5\text{М}$, $V_c = 50000 \text{ км/с}$, $C_k = 512\text{байт}$, $V_k = 4 \text{ Мбит/с}$, $T_3 = 1500\text{мкс}$ – скорость передачи кадра по моноканалу.

Предполагая, что $T_{обсл} = T_{об}$ и воспользовавшись формулами (4.3) и (4.4), получаем

$$T_p = (N_{pc} - 1) (S_k/V_c + C_k/V_k + N_{pc} * T_3) + (S_k/V_c + C_k/V_k + N_{pc} * T_3) = \\ = N_{pc} (S_k/V_c + C_k/V_k + N_{pc} * T_3) = 969350 \text{ мкс}.$$

4.5. Сети Ethernet

Обычный *Ethernet* является одним из самых простых и дешевых в построении из когда-либо разработанных стандартов локальных сетей, созданный на базе экспериментальной сети Ethernet Network, предложенной фирмой Xerox в 1975 году. В сетях Ethernet все компьютеры имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Одновременно все компьютеры имеют возможность немедленно получить данные, которые любой из компьютеров начал передавать на общую шину. Такая простота подключения и передачи информации компьютерами - одна из причин, которые привели стандарт Ethernet к такому успеху. Иногда такое построение сети называют методом коллективного доступа (Multiply Access).

В зависимости от типа физической реализации различают следующие типы Ethernet:

10base-5 (толстый коаксиальный кабель) , называемый по типу используемого в ней носителя - толстого коаксиального кабеля. Недостатками этого типа построения Ethernet являются: неудобный в использовании кабель за счет своей толщины (внешний диаметр составляет около 10мм), высокая стоимость, максимальное допустимое количество станций - не более 100.

Достоинствами данного стандарта является его высокая защищенность от внешних воздействий и сравнительно большая длина сегмента - до 500м. Данный стандарт разработан фирмой Xerox и считается классическим Ethernet.

10base-2 (тонкий коаксиальный кабель) - самая из простых в установке и дешевых типов сети. Тонкий коаксиальный кабель - до 5мм, прокладывается вдоль расположения компьютеров сети. На конце каждого сегмента располагается 50-омный резистор (терминатор), предотвращающий возникновения эффекта отраженной волны. К недостаткам данного типа сети Ethernet относят: выход из строя сети при повреждении кабеля и сравнительно трудоемкое обнаружение отказавшего отрезка кабеля, которое возможно при использовании кабельного тостера, низкая защита от помех, максимальное число компьютеров в сети - не более 1024. Максимальная длина сегмента данного стандарта без использования повторителей составляет 185м.

10base-T (витая пара) - это сети на основе витой пары, на сегодняшний день являются наиболее распространенными за счет того, что они строятся на основе витой пары и используют топологию типа "звезда". За счет этого конфигурировать локальную сеть становится значительно удобнее и рациональнее. Однако эти сети не лишены следующих недостатков: слабая помехозащищенность и восприимчивость к электрическим помехам не дают возможности использовать такие сети в непосредственной близости к источникам электромагнитных излучений.

10base-F (волоконно-оптический канал) - технология, использующая в качестве носителя волоконно-оптический

кабель. По строению аналогичен Ethernet 10Base-T, то есть использует топологию "звезда". Использование волоконно-оптического кабеля приводит к тому, что такое построение ЛВС обеспечивает почти полную помехозащищенность от электромагнитных излучений. Однако этот метод построения Ethernet имеет следующие недостатки:

- волоконно-оптический кабель является самым дорогим из всех видов кабеля;
- волоконно-оптический кабель хрупкий, поэтому монтаж его очень затруднен.

Топология для всех четырех типов практически не отличается. Данные в локальной сети передаются со скоростью до 10 Мбит/с, о чем говорит первая цифра в названии типа сети.

Существует еще одна разновидность технологии Ethernet - Fast Ethernet, способная передавать данные со скоростью до 100 Мбит/сек, которая в свою очередь подразделяется на:

100base-T4 (4 витые пары)

100base-TX (2 витые пары)

100base-FX (волоконно-оптический канал).

4.6. Сети FDDI

FDDI (Fiber Distributed Data Interface - распределенный интерфейс передачи данных по волоконно-оптическим каналам) является высокоскоростной волоконно-оптической системой со скоростью передачи данных - 100 Мбит/с. Сеть поддерживает метод доступа маркерное кольцо, но в отличие от Token Ring, система FDDI использует для передачи данных не одно кольцо, а два, передача информации по которым осуществляется в противоположных направлениях, причем второе кольцо является резервным (рис.4.6 а).

В случае разрыва по каким либо причинам первого кольца, информация считываться со второго, что увеличивает надежность работоспособности сети. Если произошел разрыв сразу обоих колец в одном и том же месте, то есть возможность помощью специальных переключателей объединить два кольца в одно (рис. 4.6 б).

В настоящее время разрабатывается модель сети, предполагающая возможность передавать различную информацию по двум кольцам одновременно, делая оба кольца основными. При этом пропускная способность такой системы увеличивается в два раза, без уменьшения надежности ее работы.

4.7. Высокоскоростные локальные сети

В настоящее время в связи с увеличившимися объемами необходимой для передачи информации получили большое развитие сети с пропускной способностью свыше 100 Мбит/с. К таким сетям относится новое поколение сетей с топологией построения Ethernet – Gigabit Ethernet.

Технология Gigabit Ethernet представляет собой дальнейшее развитие стандартов 802.3 для сетей Ethernet с пропускной способностью 10 и 100Мбит/сек. Она призвана резко повысить скорость передачи данных, сохранив при этом совместимость с существующими сетями Ethernet, использующих метод случайного доступа к ЛВС.

Пример подхода в выбору архитектуры и типа ЛВС приведен в приложении 16.

4.8. Структурированные кабельные системы

В последние годы получил развитие новый вид организации промышленной связи – локальные кабельные системы, основанные

на изготовлении, поставке, монтаже, сертификации полностью комплектных, стыкующихся со всем сетевым оборудованием систем проводки и соединений для зданий и сооружений. За этим видом продукции закрепилось название – ***структурированные кабельные системы***, базирующиеся на специально разработанных в настоящее время для них стандартов и спецификаций.

Структура типичной кабельной системы, представленная на рис. 4.7, представляет собой кабель локальной сети, прокладываемый между рабочими станциями, и коммутируемый между ними с помощью концентраторов и кроссов. Обычно такое соединение заканчивается стандартным разъемом. Внутри многоэтажного здания прокладывают вертикальные и горизонтальные проводки, последние из которых еще делятся с помощью кроссов. Подобные кабельные системы и называются структурированными.

Основным достоинством таких систем является то, что при перемещении служб и персонала внутри здания из одних помещений в другие, изменять структуру проводки не надо. Достаточно аппаратуру из одних помещений перенести в другие и сделать необходимые переключения на кроссировочных панелях, поскольку розетки во всех помещениях однотипные для всех видов сетевого оборудования и телефонии - спецификации RJ-45. Такие системы не требуют каждый раз прокладывать новую проводку и ставить новые розетки, а позволяют использовать при любых переустройствах или перестановках ту сеть, которая капитально смонтирована в здании.

В основу одного соединения в структурированной системе входит стандартный кабель с четырьмя неэкранированными витыми парами, обеспечивающими соединения для компьютеров, телефонии, охранных сигнализаций и др. и позволяющими

передавать голос, данные, видео, мультимедиа и графики.

Структурированная кабельная система состоит из следующих подсистем (рис. 4.7): рабочего места, предназначенного для подключения компьютеров, терминалов, принтеров, телефонов(факсов) и др.; горизонтальной, предназначенной для организации соединений сетевого оборудования в горизонтальной плоскости (на одном этаже) с помощью витых пар или оптических волокон; управления, состоящая преимущественно из концентраторов и кроссировочного оборудования и предназначенной для объединения и переключения соединительных цепей; вертикальной, обеспечивающей соединение подсистем управления, расположенных на разных этажах; аппаратной, предназначенной для организации связи центральной серверной с локальной или корпоративной сетью; внешней, служащей для соединения между собой сетей, расположенных в различных территориально удаленных зданиях и базирующиеся как правило на оптоволоконных соединениях.

В основе построения структурированных систем лежит стандарт TIA/EIA-568 (Commercial building telecommunication wiring standard), разработанный в 1991 году.

Данный стандарт устанавливает следующие требования к горизонтальной проводке:

- длина горизонтальных кабелей не должна превышать 90 м независимо от его типа;
- допускается применение четырех типов кабелей: четырехпарный из неэкранированных витых пар, двухпарный из экранированных витых пар; коаксиальный, оптический с волокнами размером 62,5/125 мкм;
- типы соединений: модульный восьмиконтактный RJ-45,

специальный IBM (IEEE 802.5), коаксиальный BNC, оптический соединитель;

- на каждом рабочем месте должно быть установлено не менее двух соединительных разъемов (один – модульный восьмиконтактный RJ-45, и второй – любой из перечисленных в предыдущем пункте;

- топология сети – «звезда».

4.9. Общие подходы к выбору топологии сети

В настоящее время наиболее распространенными являются локальные сети Ethernet с электрической средой обмена (10, 100-base-T). В таких сетях, на сегментах с максимальной стандартной длиной, критичной по быстродействию и помехозащищенности является сама среда обмена. Поэтому увеличение быстродействия и улучшения помехозащищенности этих сетей становится возможным при переходе от электрической среды обмена к оптической.

В высокоскоростных сетях со средой обмена на волоконной оптике критичным по быстродействию является среда обработки сигналов (оборудование узлов). Увеличение быстродействия таких сетей становится возможным при переходе к следующему поколению элементной базы.

Однако, в случайных методах доступа при большом количестве пользователей наблюдается резкое снижение пропускной способности сети при их попытке одновременно передать сообщения по сети. Устойчивый же доступ к среде обмена при любом количестве пользователей обеспечивают маркерные методы. Поэтому, при планировании сети, необходимо придерживаться следующих принципов:

- Если сеть состоит из небольших сегментов и небольшого количества пользователей, то максимальное быстродействие обеспечит сеть Ethernet с электрической средой передачи данных.

- Если сеть состоит из большого количества пользователей и сравнительно небольших сегментов, то устойчивый доступ к сети обеспечат маркерные методы доступа.

- Если сеть состоит из сегментов большой длины, то максимальное быстродействие обеспечат сети с оптической средой передачи.

Контрольные вопросы к главе 4

1. Какие сети называют локальными и чем они характеризуются?
2. Что понимают под размерами локальных сетей?
3. В чем основное отличие широковещательной топологии локальной сети от сети с передачей "от точки к точке"?
4. В чем особенности шинной, кольцевой и звездообразной топологии сети?
5. Что понимают под свойством однородности?
6. Дайте определение понятию доступа к сети.
7. Перечислите наиболее распространенные методы доступа к сети.
8. Какие Вы знаете разновидности метода случайного доступа?
9. Что понимают под конфликтом в локальной сети?
10. Перечислите маркерные методы доступа и объясните их основные принципы построения.
10. Для чего используется маркер?
11. Какие разновидности сетей Ethernet Вы знаете?
12. В чем особенность организации высокоскоростных локальных сетей?

Глава 5. Организация корпоративных сетей

5.1. Общие сведения

В настоящее время все большее число компаний испытывают необходимость в организации современных мощных **корпоративных сетей**. Растут требования как к скорости передачи информации (уменьшению времени доступа к сетевым ресурсам, находящимся в различных географических поясах), так и к надежности и защите передаваемых данных. Модульность построения аппаратно-программного обеспечения, новейшие технологии в развитии сетевых технологий и решают эти задачи.

Корпоративной сетью называется сеть, охватывающая большое количество компьютеров и располагающаяся в пределах одного предприятия. Корпоративная сеть соответствует английскому термину «enterprise-wide networks».

В связи с тем, что современные предприятия и их филиалы могут территориально охватывать разные города, страны и даже континенты, их корпоративные сети состоят из десятков и сотен локальных сетей, включающих в себя десятки тысяч компьютеров и сотни серверов, для объединения которых используются глобальные сети, по средствам организации связи с помощью телефонии, спутниковых и радиоканалов. Пример построения корпоративной сети представлен на рисунке 5.1

Для управления доступом к ресурсам таких сетей обычно используют единые базы учетных записей пользователей, которые позволяют получать доступ к ресурсам всей сети из разных частей предприятия и избавляют администраторов сети от дополнительной необходимости дублировать одно и то же пользовательское имя на

нескольких серверах локальных сетей.

Одной из важнейших характеристик корпоративных сетей является их *гетерогенность*, то есть способность обеспечивать обмен информацией компьютеров, имеющих различную коммуникационную и аппаратную конфигурацию, а также программное обеспечение.

Кроме того, оптимальность выбора маршрута от отправителя к получателю влияет на скорость передачи информации, что является "узким" местом в современных сетях, за счет своей низкой скорости передачи информации и качества сетей. Чтобы передаваемому кадру добраться до пункта назначения, ему может потребоваться преодолеть несколько транзитных участков между маршрутизаторами. Для решения этой задачи транспортный уровень располагает информацией о топологии сети.

Как уже указывалось в разделе 1.8, существует два варианта организации работы сетевого уровня: с использованием *соединений*, а другой – *без соединений*. В контексте внутреннего устройства подсети соединение обычно называют *виртуальным каналом*. Независимые пакеты в системе без установления соединений называются *дейтаграммами*.

Виртуальные каналы организованы таким образом, что для каждого посылаемого пакета не нужно выбирать маршрут заново. Этот маршрут используется для всех данных, передаваемых за время соединения. При разрыве соединения или выходе из строя маршрутизатора виртуальный канал перестает существовать. Таким образом, передаваемые пакеты всегда перемещаются по одному и тому же маршруту. При передаче пакетов указывается номер виртуального канала. Каждый маршрутизатор при такой организации сетевого уровня должен помнить, куда направлять

пакеты для каждого из открытых в данный момент виртуальных каналов, для чего, кроме системной информации маршрутизаторы хранят таблицу виртуальных каналов, проходящих через них.

При организации сетевого уровня без установления соединения, в отличие от виртуальной организации, маршрут для каждой передачи пакета выбирается заново. Перед передачей пакета необходимо рассчитать маршрут пересылки, что приводит к некоторой задержке, особенно в больших корпоративных сетях. Однако, в отличие от виртуального канала, данный способ организации более гибкий и позволяет легче приспосабливаться к неисправностям и заторам передачи данных. При передаче данных используются адреса получателя, которые при увеличении сетей становятся довольно длинными, до нескольких байтов. Маршрутизаторы при такой организации сети хранят номера входных и выходных линий для пунктов назначения пакетов.

5.2. Алгоритмы маршрутизации

Алгоритм маршрутизации - совокупность действий, которая выполняется активными компонентами сети, для того чтобы обеспечить возможность корректной доставки данных абонентам данной сети.

В сложных сетях всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя станциями. Под *маршрутом* будем понимать последовательность маршрутизаторов, которую должен пройти пакет от станции отправителя до станции получателя.

При выполнении алгоритма маршрутизации узел должен получать информацию от соседних узлов, выполняющих такой же алгоритм маршрутизации, о сетях, которые могут быть достижимы

при передаче данных через каждый соседний узел (рис. 5.2). Концентрируя такую информацию в так называемых таблицах маршрутизации, каждый узел может определить направление - маршрут передачи данных для каждой из доступных сетей. В том случае, если таких маршрутов оказалось несколько, алгоритм маршрутизации предусматривает возможность использования специального критерия для выбора оптимального маршрута - например, задержка прохождения маршрута отдельным пакетом, количество пройденных промежуточных маршрутизаторов и др. Чтобы по адресу назначения в сети можно было выбрать маршрут движения пакета, каждая станция анализирует таблицу маршрутизации.

Таблица маршрутизации представляет собой некую базу данных составных элементов сети (сетевых адресов маршрутизаторов, сетей, расстояние до сети назначения, флаг канала и др.) (Рис. 5.2 и таблица 5.1). Флаг U свидетельствует о том, что маршрут в настоящее время занят.

Таблица маршрутизации строится и для станций сети, передающих и принимающих пакеты и для самих маршрутизаторов, отвечающих за пересылку пакетов между различными сетями.

Когда на маршрутизатор поступает новый пакет, из него извлекается адрес сети, который сравнивается с адресами сети в таблице маршрутизации. Строка с совпавшим адресом указывает, на какой ближайший маршрутизатор следует направить пакет.

С увеличением количества маршрутизаторов, а, следовательно, и числа подсетей в больших корпоративных сетях, число записей в таблице маршрутизации также увеличивается. Это приводит к возрастанию времени поиска в ней нужной информации, что в свою очередь уменьшает скорость передачи данных и

приводит к снижению пропускной способности сети в целом. Рациональным решением данной проблемы является следующий принцип построения таблицы: в нее вносятся только адреса маршрутизаторов, связывающих данную сеть с "соседними" сетями, а все остальные сети идентифицируются в таблице специальной записью - "маршрутизатор по умолчанию", через который пролегает путь ко всем остальным сетям. Пример построения таблицы маршрутизации для сети 1 (рис.5.2) представлен в таблице 5.1

Таблица 5.1. Пример построения таблицы маршрутизации

Наименование сети - получателя пакета	Адрес маршрутизатора	Расстояние до сети получателя	Флаг состояния канала
Сеть 2	1	1	U
По умолчанию	3	-	

В зависимости от способа, который используется для обеспечения обмена информацией о маршрутах в сети между узлами при выполнении алгоритма маршрутизации, различают два типа протоколов маршрутизации:

протоколы ***distant vector***, предусматривающие передачу информации о маршрутах периодически, через установленные интервалы времени. Одним из примеров реализации такой технологии является протокол маршрутизации RIP (Routing Information Protocol), применяемый в сетях небольшого размера;

протоколы ***link state***, предусматривающие передачу информации о маршрутах в момент первоначального включения или возникновения изменений в структуре информационных каналов.

Прежде чем пакет будет передан через сеть, необходимо установить ***виртуальное соединение*** между абонентами сети. Существует два типа виртуальных соединений - коммутируемый

виртуальный канал Switched Virtual Circuit, SVC) и постоянный виртуальный канал (Permanent Virtual Circuit, PVC). При создании коммутируемого виртуального канала коммутаторы сети настраиваются на передачу пакетов динамически, по запросу абонента, а создание постоянного виртуального канала происходит заранее.

Необходимость создания виртуальных каналов заключается в том, что маршрутизация пакетов между коммутаторами сети на основании таблиц коммутации происходит только один раз - при создании виртуального канала. После создания виртуального канала передача пакетов коммутации происходит на основании идентификаторов виртуальных каналов.

5.3. Уровни и протоколы

Диспетчер ввода/вывода, через который осуществляется доступ к сетевой среде, включает в себя большинство сетевых компонентов. Они организованы в несколько уровней (рис.5.3):

Драйверы плат сетевого адаптера, совместимые со спецификацией интерфейса сетевых устройств (Network Device Interface Specification, **NDIS**), используя соответствующие сетевые платы и протоколы, соединяют компьютеры под управлением СОС.

Протоколы организуют надежную передачу данных между компьютерами в сети.

Драйверы файловой системы предоставляют приложениям доступ к локальным и удаленным файловым ресурсам, например, сетевым принтерам.

Драйвер - это программа, непосредственно взаимодействующая с сетевым адаптером. *Модуль* - это программа, взаимодействующая с драйвером, сетевыми прикладными

программами или другими модулями. Драйвер сетевого адаптера и, возможно, другие модули, специфичные для физической сети передачи данных, предоставляют сетевой интерфейс для протокольных модулей семейства TCP/IP.

Все компоненты общаются через программные интерфейсы, называемые *границами* (boundaries). *Граница* — это унифицированный интерфейс между функциональными уровнями сетевой модели. Появление границ в качестве средств доступа к сетевым уровням открывает сетевые компоненты ОС для сторонних разработчиков и облегчает написание сетевых драйверов и служб. Пограничные слои делают сетевую архитектуру сетевой операционной системы модульной, предоставляя разработчикам базу для создания распределенных приложений. Например, разработчикам транспортных протоколов достаточно реализовать только один уровень, а не всю модель OSI целиком.

5.3.1. Спецификация интерфейса сетевых устройств

Драйверы NDIS -совместимых (Network Device Interface Specification, спецификация интерфейса сетевых устройств) сетевых устройств обеспечивают взаимодействие сетевого адаптера и программного, аппаратного и микропрограммного обеспечения компьютера. Сетевые устройства являются физическим интерфейсом между компьютером и сетевым кабелем.

Каждая сетевая плата может иметь один или несколько драйверов. Чтобы работать и надежно функционировать в ОС, они должны быть совместимы с данной спецификацией. Эта спецификация обеспечивает независимую привязку одного или более протоколов к одному или более драйверу сетевой платы.

Так как сетевые устройства и их драйверы не зависят от

протоколов, смена протокола не требует реконфигурации сетевых устройств.

NDIS определяет программный интерфейс, используемый протоколами для взаимодействия с драйверами сетевых плат. Любой протокол, совместимый с данной спецификацией, может взаимодействовать с любым **NDIS** -совместимым драйвером сетевой платы. Поэтому нет необходимости включать в сам протокол код для работы со специфическими драйверами сетевых адаптеров.

Канал связи между драйвером протокола и драйвером сетевым устройством устанавливается во время *привязки (binding)*.

Спецификация NDIS обеспечивает:

каналы связи между сетевыми платами и соответствующими драйверами;

независимость протоколов и драйверов сетевых плат;

неограниченное число сетевых плат;

неограниченное число протоколов, привязываемых к одной сетевой плате.

5.3.2. Протоколы

Протоколы организуют связь между двумя или более компьютерами. Некоторые протоколы часто называют транспортными, например, TCP/IP, NWLink, NetBEUI и AppleTalk. Протоколы расположены над уровнем интерфейса NDIS.

Существуют следующие виды протоколов:

Transmission Control Protocol/Internet Protocol (TCP/IP). Это маршрутизируемый протокол, поддерживающий глобальные вычислительные сети (Wide Area Network, WAN). Протокол TCP/IP используется в Интернете.

NWLink IPX/SPX -совместимый транспорт. Это версия протокола

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) совместимая со спецификацией NDIS.

NetBEUI. Очень быстрый и эффективный немаршрутизируемый протокол, который в основном полагается на широковещательную передачу и используется в небольших сетях.

Apple Talk. Используется на компьютерах под управлением Windows NT Server совместно с Services for Macintosh для поддержки клиентов Apple Macintosh.

Протокол TCP/IP

Семейство протоколов TCP/IP работает на любых моделях компьютеров, произведенных различными производителями компьютерной техники и работающих под управлением различных операционных систем. С помощью протоколов TCP/IP можно объединить практически любые компьютеры.

Архитектура протоколов TCP/IP предназначена для объединенной сети, состоящей из соединенных друг с другом шлюзами отдельных разнородных пакетных подсетей, к которым подключаются разнородные машины. Каждая из подсетей работает в соответствии со своими специфическими требованиями и имеет свою природу средств связи. Однако предполагается, что каждая подсеть может принять пакет информации (данные с соответствующим сетевым заголовком) и доставить его по указанному адресу в этой конкретной подсети. Не требуется, чтобы подсеть гарантировала обязательную доставку пакетов и имела надежный сквозной протокол. Таким образом, две машины, подключенные к одной подсети, могут обмениваться пакетами.

Сетевой протокол TCP/IP обеспечивает взаимодействие

компьютеров с различными архитектурами и ОС через взаимосвязанные сети. TCP/IP — это гибкий стек протоколов, созданных для глобальных вычислительных сетей (ГВС), легко адаптируемый к широкому спектру сетевого оборудования. TCP/IP можно применять для взаимодействия с системами на основе Windows NT, с устройствами, использующими другие сетевые продукты, с системами других фирм, например, с UNIX-системами.

TCP/IP — это маршрутизируемый сетевой протокол, предоставляющий такие средства как:

- стандартный маршрутизируемый корпоративный сетевой протокол;

- архитектура, облегчающая взаимодействия в гетерогенных средах;

- доступ к Интернету и его ресурсам.

Каждый компьютер в сети TCP/IP имеет адреса трех уровней:

Локальный адрес узла, определяемый технологией, с помощью которой построена отдельная сеть, в которую входит данный узел. Для узлов, входящих в локальные сети - это MAC-адрес сетевого адаптера или порта маршрутизатора, например, 23-B4-65-7C-DC-11. Эти адреса назначаются производителями оборудования и являются уникальными адресами, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC-адрес имеет формат 6 байтов: старшие 3 байта - идентификатор фирмы производителя, а младшие 3 байта назначаются уникальным образом самим производителем. Для узлов, входящих в глобальные сети, такие как X.25 или frame relay, локальный адрес назначается администратором глобальной сети.

IP-адрес, состоящий из 4 байт, например, 192.15.0.30. Этот адрес используется на сетевом уровне и назначается администратором во

время конфигурирования компьютеров и маршрутизаторов.

Символьный идентификатор-имя, например COMP21.AUD221.COM, также назначаемый администратором. Его также называют DNS-именем.

TCP/IP — это стек протоколов, созданный для межсетевого обмена. На рис.5.4 представлена структура протокола **TCP/IP**.

В **SNMP** (Simple Network Management Protocol) содержатся данные мониторинга MIB (Management Information Base). **Windows Sockets (WinSock)** - стандартный интерфейс между socket-приложениями и протоколами TCP/IP.

NetBT (NetBIOS над TCP/IP) - службы NetBIOS, в том числе службы- имен, дейтаграмм и сессий. Также предоставляет стандартный интерфейс между NetBIOS-приложениями и протоколами TCP/IP.

Протокол **TCP** (Transmission Control Protocol) представляет гарантированную доставку пакетов с установлением соединения.

Протокол **UDP** (User Datagram Protocol) представляет негарантированную доставку пакетов без установления соединения. Протоколы TCP и UDP предоставляют разные услуги прикладным процессам. Большинство прикладных программ пользуются только одним из них. Если вам нужна надежная и эффективная доставка по длинному и ненадежному каналу передачи данных, то лучшим может быть TCP. Если вам нужна доставка дейтаграмм и высокая эффективность на быстрых сетях с короткими соединениями, то лучше может быть UDP. Если ваши потребности не попадают ни в одну из этих категорий, то выбор транспортного протокола не ясен. Однако прикладные программы могут устранять недостатки выбранного протокола. Если вы выбрали TCP, а вам нужно

передавать записи, то прикладная программа должна вставлять маркеры в поток байтов так, чтобы можно было различить записи.

Протокол **ICMP** (Internet Control Message Protocol) обеспечивает специальную связь между хостами (host - главный компьютер, ведущий узел), отчет о сообщениях и ошибках доставки пакетов.

Протокол **IP** (Internet Protocol) выполняет функции адресации и маршрутизации.

Протокол **ARP** (Address Resolution Protocol) осуществляет отображение адресов IP в адреса подуровня управления доступом к среде передачи. Адрес IP обязателен для каждого компьютера, использующего TCP/IP. Он представляет собой логический 32-разрядный адрес, применяемый для идентификации TCP/IP-хоста. Подуровень управления доступом к среде передачи напрямую взаимодействует с сетевой платой и отвечает за безошибочную передачу данных между двумя компьютерами в сети. Другими словами, протокол ARP служит для определения локального адреса устройства по IP-адресу передаваемого пакета. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу - RARP (Reverse Address Resolution Protocol, реверсивный ARP)

Основные параметры протокола TCP/IP

Логический 32-разрядный **IP-адрес** адрес, используемый для идентификации TCP/IP-хоста, состоит из двух частей: идентификатора сети и идентификатора хоста и имеет длину 4 байта - первая определяет номер сети, вторая номер узла в сети. Каждый компьютер, использующий протокол TCP/IP, должен иметь уникальный адрес IP, например, 10. 0.0.2. более подробно об IP-

адресации будет рассмотрено в параграфе 5.5.

Подсеть — это сеть в многосетевой среде, использующая адреса IP с общим идентификатором сети. Применяя подсети, организация может разделить одну большую сеть на несколько физических сетей и соединить их маршрутизаторами. Для разбиения IP-адреса на идентификаторы сети и хоста служит маска подсети. При попытке соединения TCP/IP с помощью маски подсети определяет, находится ли целевой хост в локальной или удаленной сети. Пример маски подсети — 255.255.0.0. Чтобы взаимодействовать напрямую, компьютеры в сети должны иметь одинаковую маску подсети.

Чтобы действовала связь с хостом из другой сети, должен быть указан IP-адрес основного шлюза. Если на локальном хосте не указан маршрут до целевой сети, то TCP/IP посылает пакеты для удаленных сетей на **основной шлюз**. Если он не указан, связь будет ограничена только локальной сетью (подсетью). Например, адрес основного шлюза может быть 157.0.2.2.

Компьютеры IP-сетей обмениваются между собой информацией, используя в качестве адресов 4-байтные коды, которые принято представлять соответствующей комбинацией десятичных чисел, напоминающей нумерацию абонентов в телефонии, например: 157.104.15.15. Это означает, что каждое из четырех чисел в IP адресе больше или равно 0 и меньше или равно 255. Как можно увидеть на приведенном примере, числа условно отделяются друг от друга точками.

Протокол NWLink

Протокол NWLink IPX/SPX Compatible Transport — это разработанная Microsoft 32-разрядная NDIS 4.0-совместимая версия

протокола IPX/SPX (Internetwork Packet Exchange/ Sequenced Packet Exchange) фирмы Novell.

NWLink чаще всего применяется в сетевых средах, где компьютеры должны иметь доступ к клиент-серверным приложениям, выполняющимся на сервере Novell NetWare, или, наоборот, клиенты Novell должны обращаться к приложениям Windows NT. NWLink позволяет компьютерам под управлением Windows NT взаимодействовать с другими сетевыми устройствами, использующими IPX/SPX, такими как принтер-серверы. Протокол NWLink подходит и для малых сетевых сред, состоящих только из Windows NT и клиентов Microsoft.

NWLink поддерживает следующие сетевые протоколы API, обеспечивающие функции IPC:

- WinSock (Windows Sockets) поддерживает существующие Novell-приложения, написанные в соответствии с интерфейсом NetWare IPX/SPX Sockets. WinSock обычно используется для связи с NetWare Loadable Modules (NLM). Заказчики, реализующие клиент-серверные решения с помощью модулей NLM, могут перенести их в среду Windows NT Server и сохранить при этом совместимость со своими клиентами.

- NetBIOS над IPX, реализованный в виде NWLink NetBIOS, поддерживает взаимодействие между рабочими станциями Novell, применяющими NetBIOS, и компьютерами с Windows NT, использующими NWLink NetBIOS.

При установке и конфигурировании NWLink IPX/SPX необходимо указать тип пакетов и номер сети. Тип пакетов определяет способ, по которому сетевая плата будет форматировать данные для отправки по сети. Многие операционные системы позволяют автоматически определять тип передаваемых пакетов.

Протокол NetBEUI

Протокол NetBEUI (NetBIOS Extended User Interface) разработан для небольших локальных вычислительных сетей (ЛВС), состоящих из 20-200 компьютеров. Так как этот протокол немаршрутизируемый, он не подходит для глобальных сетей.

NetBEUI обеспечивает совместимость с существующими ЛВС, в которых применяется протокол NetBEUI, и обеспечивает взаимодействие со старыми сетевыми системами такими как Microsoft LAN Manager и Microsoft Windows.

Протокол NetBEUI реализует следующие возможности: связь между компьютерами с установлением или без установления соединения; автоматическую настройку; защиту от ошибок; невысокие требования к памяти.

Так как NetBEUI полагается на широковещательную передачу при выполнении многих функций, например, при обнаружении и регистрации имен, его применение приводит к увеличению широковещательного трафика по сравнению с другими протоколами.

Transport Driver Interface

Transport Driver Interface (TDI) — пограничный слой, предоставляющий общий программный интерфейс взаимодействия транспортных протоколов с драйверами файловой системы, такими как служба Workstation (Рабочая станция) — редиректор — или служба Server (Сервер). TDI обеспечивает их независимость друг от друга.

Так как TDI обеспечивает независимость сетевых компонентов друг от друга, можно добавлять, удалять или менять протоколы, не перенастраивая всю сетевую подсистему узла.

Драйверы файловой системы

Драйверы файловой системы служат для доступа к файлам. Всякий раз, когда Вы делаете запрос на чтение или запись файла, в работу включается драйвер файловой системы. Несколько основных сетевых компонентов реализованы в виде драйверов файловой системы, например службы Workstation (Рабочая станция) и Server (Сервер).

Редиректор

Диспетчер ввода/вывода определяет, кому адресован запрос на ввод/вывод локальному диску или сетевому ресурсу. Если последнему, редиректор перехватывает запрос и посылает (перенаправляет) его соответствующему сетевому ресурсу. ***Редиректор*** (RDR)— это компонент, расположенный над TDI и взаимодействующий с транспортными протоколами средствами TDI. Редиректор обеспечивает подключение к Windows for Workgroups, LAN Manager LAN Server и другим сетевым серверам Microsoft.

Редиректор реализован в виде драйвера. Это дает следующие преимущества:

приложения могут применять Windows NT API ввода/вывода для доступа к файлам как на локальном, так и на удаленном компьютере. С точки зрения диспетчера ввода/вывода, нет никакой разницы между обращением к файлам на локальном жестком диске и использованием редиректора для доступа к файлам на удаленном компьютере в сети;

редиректор может выполняться в режиме ядра и напрямую вызывать другие драйверы и компоненты, такие как диспетчер кэша, повышая таким образом производительность;

редиректор, как любой драйвер файловой системы, можно динамически загружать и выгружать;

редиректор СОС может сосуществовать с редиректорами сторонних производителей.

Сервер

Вторым компонентом сети является служба *Server* (Сервер). Как и редиректор, она располагается над TDI, реализована в виде драйвера файловой системы и напрямую взаимодействует с другими драйверами файловой системы, выполняя запросы на чтение и запись.

Server предоставляет соединения, запрашиваемые клиентскими редиректорами, и обеспечивает доступ к требуемым ресурсам.

Когда эта служба получает от удаленного компьютера запрос на чтение файла, который расположен на локальном диске сервера, происходит следующее:

сетевые драйверы нижнего уровня получают запрос и передают его Server;

server передает запрос на чтение файла соответствующему локальному драйверу файловой системы;

для доступа к файлу этот драйвер вызывает низкоуровневые драйверы дисков;

данные от них передаются локальному драйверу файловой системы;

тот передает их обратно Server; служба передает их низкоуровневому сетевому драйверу, который обеспечивает доставку данных до машины-клиента.

5.4. Адресация компьютеров в Интернет

Под *Internet* подразумевается совокупность сетей, базирующихся на IP-технологии обмена данными (IP -Internet

Protocol) и обеспечивающих пользователям наивысшую степень удобства на коммутируемых или выделенных линиях: максимально высокие скорости, работу с электронной почтой и предоставление самых современных услуг, в числе которых центральное место занимает **WWW-технология** (World Wide Web - Всемирная информационная паутина).

Каждый узел в объединенной сети, как указывалось выше, должен иметь свой уникальный IP адрес и состоит из двух частей - номера сети и номера узла. Какая часть адреса относится к номеру сети, а какая к номеру узла, определяется значениями первых битов адреса:

Если адрес начинается с 0, то сеть относят к классу А, и номер сети занимает один байт, а остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126 (рис 5.5). В таких сетях количество узлов должно быть больше 216, но не превышать 224.

Если первые два бита адреса равны 1, то сеть относится к классу В и является сетью средних размеров с числом узлов 28-216.

Если адрес начинается с последовательности 110, то это сеть класса С с числом узлов не больше 28 (см. рис. 5.5).

Если адрес начинается с последовательности 1110, то он является адресом класса D и обозначает особый, групповой адрес - multicast. Если в пакете в качестве адреса назначения указан адрес класса D, то такой пакет должны получить все узлы, которые образуют группу номером, указанным в поле адреса.

Если адрес начинается с последовательности 11110, то это адрес класса Е, он зарезервирован для будущих применений(рис 5.5).

В общем случае, такие числовые адреса могут иметь некоторое разнообразие трактовок, из которых приведем здесь следующую:

<класс сети><номер сети><номер компьютера>.

Такая комбинация подразумевает, что множество представимых числовых номеров делится на сети разного масштаба, а именно (рис. 5.5, 5.6):

С помощью специального механизма маскирования любая сеть, в свою очередь, может быть представлена набором более мелких сетей.

Определение номеров сети по первым байтам адреса не вполне гибкий механизм для адресации. На сегодняшний день получили широкое распространение маски. Маска - это тоже 32-разрядное число, она имеет такой же вид, как и IP-адрес. Маска используется в паре с IP-адресом, но не совпадает с ним.

Принцип определения номера сети и номера узла IP-адреса с использованием маски состоит в следующем: двоичная запись маски содержит единицы в тех разрядах, которые в IP-адресе должны представляться как номер сети и нули, в тех разрядах, которые представляются как номер хоста. Кроме того, поскольку номер сети является целой частью адреса, единицы в маске должны представлять непрерывную последовательность.

Каждый класс IP-адресов (А, В, С) имеет свою маску, используемую по умолчанию:

Класс А - 11111111.00000000.00000000.00000000 (255.0.0.0)

Класс В - 11111111.11111111.00000000.00000000 (255.255.0.0)

Класс С - 11111111.11111111.11111111.00000000
(255.255.255.0)

Например, если адресу 190.215.124.30 задать маску 255.255.255.0, то номер сети будет 190.215.124.0, а не 190.215.0.0, как это определяется правилами системы классов.

Доменные адреса

С ростом объемов информации в Internet, увеличилось и количество его узлов. В результате путешествие по глобальной сети с помощью адресов, представленных в виде чисел стало неудобным. На смену им пришли так называемые доменные адреса.

Домен (domain) -- - территория, область, сфера, - фрагмент, описывающий адрес в текстовой форме. Адрес конечного узла представляется в виде не цифрового кода как было указано выше, а в виде набора текстовой информации формата:

domain4.domain3.domain2.domain1

где domain 1 - буквенное обозначение страны, например ru, eng и др., или одной из следующих спецификаций:

com - коммерческие организации

edu - учебные и научные организации

gov - правительственные организации

mil - военные организации

net - сетевые организации разных сетей

org - другие организации

domain4, domain3, domain2 - описывают как правило, более низшие уровни адреса, например, наименование города, отдела, раздела и т.д.

5.5. Службы обмена данными

5.5.1. Сети X.25

Сети **X.25** являются на сегодняшний день самыми распространенными сетями с коммутацией пакетов, используемыми для построения корпоративных сетей.

Данные сети могут работать на ненадежных линиях передачи информации благодаря протоколам с установлением соединения и коррекцией ошибок на двух уровнях - канальном и сетевом.

Сети X.25 базируются на следующих основополагающих принципах организации, отличающих их от других:

наличие в структуре сети специального устройства - PAD (Packet Assembler Disassembler), предназначенного для выполнения операции сборки нескольких низкоскоростных потоков байт от алфавитно-цифровых терминалов в пакеты, передаваемые по сети и направляемые компьютерам для обработки;

наличие трехуровневого стека протоколов с использованием на канальном и сетевом уровнях протоколов с установлением соединения, управляющих потоками данных и исправляющих ошибки;

ориентация на однородные стеки транспортных протоколов во всех узлах сети - сетевой уровень рассчитан на работу только с одним протоколом канального уровня и не может подобно протоколу IP объединять разнородные сети.

Дополнительными устройствами в сети X.25 являются также коммутаторы (центры коммутации пакетов), расположенные в различных географических областях и соединенные высокоскоростными каналами связи, обеспечивающими обмен данными между ними (рис.5.7).

5.5.2. Уровень передачи данных АТМ

Технология передачи данных **АТМ** (Asynchronous Transfer Mode – асинхронный режим передачи) основана на передаче данных пакетами фиксированной длины размером 53 байта (рис. 5.8).

Сети АТМ предполагают передачу данных при установленном соединении, то есть сначала устанавливается соединение между источником информации и приемником и только затем начинается передача пакетов данных, после чего соединение разрывается.

5.5.3. Сети SDH

Появление стандартов синхронной цифровой иерархии передачи данных (SDH) в 1988 году ознаменовало собой новый этап развития транспортных сетей. Технология SDH широко используется для организации надежной передачи данных. SDH была разработана для того, чтобы получить стандартный протокол для взаимодействия **провайдеров** - поставщиков сетевых услуг; унифицировать американские, европейские и японские цифровые системы; обеспечить мультиплексирование цифровых сигналов на гигабитных скоростях; обеспечить поддержку функций эксплуатации и технического обслуживания OA&M (operation, administration and maintenance - функционирование, администрирование и техническое обслуживание).

Системы синхронной передачи не только преодолели ограничения систем-предшественниц (PDH), но и снизили накладные расходы на передачу информации. Ряд уникальных достоинств - доступ к низкоскоростным каналам без полного демультиплексирования всего потока, высокая отказоустойчивость, развитые средства мониторинга и управления, гибкое управление постоянными абонентскими соединениями, обусловили ее высокий темп развития, ставший основой первичных сетей нового поколения.

Стек протоколов SDH состоит из протоколов трех основных уровней (рис. 5.9):

- уровень соединения контролирует доставку данных между двумя конечными пользователями сети;
- уровень управления передачей данных поддерживает физическую целостность сети, поддерживает операции административного контроля, осуществляет различные операции реконфигурирования в случае отказа какого-либо элемента сети и др.;
- физический уровень, названный в стандарте фотонным (photonic), имеет дело с кодированием бит информации с помощью модуляции света.

На сегодняшний день технология SDH считается не только перспективной, но и достаточно апробированной технологией для создания транспортных сетей. Технология SDH обладает рядом важных достоинств с пользовательской, эксплуатационной и инвестиционной точек зрения:

- умеренная структурная сложность, снижающая затраты на монтаж, эксплуатацию и развитие сети, в том числе подключение новых узлов;

- широкий диапазон возможных скоростей - от 155,520 Мбит/с (STM-1) до 2,488 Гбит/с (STM-16) и выше;

- возможность интеграции с каналами PDH, поскольку цифровые каналы PDH являются входными каналами для сетей SDH;

- высокая надежность системы благодаря централизованному мониторингу и управлению, а также возможности использования резервных каналов;

- высокая степень управляемости системы благодаря полностью программному управлению;

- возможность динамического предоставления услуг - каналы для абонентов могут создаваться и настраиваться динамически, без внесения изменений в инфраструктуру системы;

- высокий уровень стандартизации технологии, что облегчает интеграцию и расширение системы, дает возможность применения оборудования различных производителей;

- высокая степень распространения стандарта в мировой практике.

Стандарт SDH обладает достаточной степенью зрелости, что делает его надежным для инвестиций.

В дополнение к перечисленным достоинствам, необходимо отметить развитие магистральных телекоммуникаций российских операторов связи на основе SDH, что предоставляет дополнительные возможности для привлекательных интеграционных решений. Перечисленные достоинства делают решения, основанные на технологии SDH, рациональными с точки зрения инвестиций. В настоящее время она может считаться базовой для построения современных транспортных сетей, как для корпоративных сетей различного масштаба, так и для сетей связи общего пользования.

Контрольные вопросы к главе 5

1. Какие эталонные модели построения сети Вы знаете и каковы их отличительные особенности?
2. В чем заключается назначение сетевого и транспортного уровней?
3. Дайте определение понятию "алгоритм маршрутизации".
4. Какие Вы знаете протоколы маршрутизации?
5. Для чего устанавливаются виртуальные соединения?
6. Что понимают под понятием драйвер?

7. Какие Вы знаете протоколы и каковы их отличительные черты?
8. Перечислите основные параметры протокола TCP/IP.
9. Какие способы адресации компьютеров в Internet Вы знаете?
10. Дайте определения службам редиirector и сервер.
11. Перечислите все известные Вам службы обмена данными и в чем их особенности организации?

