С.И. БАБАЕВ, Б.В. КОСТРОВ, М.Б. НИКИФОРОВ

КУРС

КОМПЬЮТЕРНЫЕ СЕТИ

СТАНДАРТЫ И ПРОТОКОЛЫ

ЧАСТЬ 3

УЧЕБНИК

INTERACTIVE ON-LINE

С.И. БАБАЕВ
Б.В. КОСТРОВ
М.Б. НИКИФОРОВ

КОМПЬЮТЕРНЫЕ СЕТИ

Часть 3
СТАНДАРТЫ И ПРОТОКОЛЫ

УЧЕБНИК

Рекомендовано Научно-методическим советом ФГБОУ ВО «Рязанский государственный радиотехнический университет» в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлениям подготовки 2.09.03.01, 2.09.04.01 «Информатика и вычислительная техника» (квалификация «бакалавр» и «магистр»), 1.02.03.03, 1.02.04.03 «Математическое обеспечение и администрирование информационных систем» (квалификация «бакалавр» и «магистр»), 5.38.03.05 «Бизнес-информатика»(квалификация «бакалавр»), 2.10.05.01 «Компьютерная безопасность» (квалификация «бакалавр»), 2.10.05.03 «Информационная безопасность автоматизированных систем» (квалификация «специалист»)

Москва
КУРС
2018

УДК 004(075.8)
ББК 32.973.202я73
Б12

Рецензенты:
Баранчиков А.И., д-р техн. наук, профессор кафедры ЭВМ Рязанского государственного радиотехнического университета;
Логинов А.А., канд. техн. наук, доцент, главный конструктор по направлению Государственного рязанского приборного завода

Бабаев С.И.,
Б12 Компьютерные сети. Часть 3. Стандарты и протоколы : учебник / С.И. Бабаев, Б.В. Костров, М.Б. Никифоров. — М.: КУРС, 2018. — 176 с.

ISBN 978-5-907064-28-7

Данный учебник предназначен для студентов (бакалавров, магистров), аспирантов и специалистов, которым необходимо получить базовые знания о принципах построения компьютерных сетей, понять особенности традиционных и перспективных технологий локальных и глобальных сетей, изучить способы создания крупных составных сетей и управления такими сетями. Книга может быть полезна начинающим специалистам в области сетевых технологий, которые имеют общие представления о работе сетей, но хотели бы получить базовые знания и навыки, позволяющие продолжить изучение сетевых технологий самостоятельно.

Данная книга имеет нестандартный характер изложения материала. Во всех технических разделах приведены не только теоретические сведения о рассматриваемом материале, но и описание практической реализации изучаемых технологий на реальном сетевом оборудовании. В качестве базового оборудования приводится система команд встроенной операционной системы Cisco IOS. К теоретическому материалу прилагается лабораторный практикум, поддерживающий основные разделы книги. Практические примеры конфигурирования реальной сети приводятся на базе виртуального эмулятора Emulate virtual environment next generation. Данный способ изложения облегчает освоение материала. Кроме этого, такая современная компоновка материала существенно отличает данную книгу от известных классических учебников по сетевым технологиям таких авторов, как В.Г. Олифер и Н.А. Олифер, Э. Таненбаум.

Возможность эмуляции реальной системы команд устройств ведущих мировых производителей, совместное изложение теории и практики делают эту книгу незаменимой для подготовки к базовым сертификационным экзаменам таких компаний, как Cisco, DLink, Huawei.

Учебник предназначен для студентов направлений 2.09.03.01, 2.09.04.01 «Информатика и вычислительная техника» (квалификация «бакалавр» и «магистр»), 1.02.03.03, 1.02.04.03 «Математическое обеспечение и администрирование информационных систем» (квалификация «бакалавр» и «магистр»), 5.38.03.05 «Бизнес-информатика» (квалификация «бакалавр»), 2.10.05.01 «Компьютерная безопасность» (квалификация «специалист»), 2.10.05.03 «Информационная безопасность автоматизированных систем» (квалификация «специалист»).

УДК 004(075.8)
ББК 32.973.202я73

ISBN 978-5-907064-28-7

СПИСОК СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ATM — Asynchronous Transfer Mode
IP — Internet Protocol
MAC — Media Access Control
TCI — Tag Control Information
TCP/IP — Transmission Control Protocol/Internet Protocol
URL — Uniform Resource Locator
DTE — Data Terminal Equipment
DCE — Data Circuit-Terminating Equipment
СУ — Сетевой узел
LAN — Local Area Network
WAN — Wide Area Network
MAN — Metropolitan Area Network
CIM — Computer Integrated Manufacturing
PSTN — Public Switched Telephone Network
PSDN — Public Switched Data Network
ISO — Intrenational Standard Organization
ITU — International Telecommunication Union
IEEE — Institute of Electrical and Electronics Engineers
OSI — Open System Interconnection
MAC — Medium Access Control
LLC — Logical Link Control
MAC — Media Access Channel
АОКД — Аппаратура окончания канала данных
CSMA/CD — Carrier Sense Multiply Access/Collision Detection
МДКН/ОК — Метод множественного доступа с контролем несущей и обнаружением конфликтов
CSMA/CA — Collision Avoidance
ArcNet — Attached Resource Computer Net
PH — Passive Hub
AH — Active Hub
ISU — Information Symbol Unit
MAU — Multistation Access Unit
PoE — Power over Ethernet
SW — Switch
NLP — Normal Link Pulse

OTN — Optical Transport Network
FDDI — Fiber Distributed Data Interface
IETF — Internet Engineering Task Force
XDR — External Data Representation
PPP — Point To Point Protocol
IPv4 — Internet Protocol version 4
IPv6 — Internet Protocol version 6

ВВЕДЕНИЕ

История любой области науки позволяет глубже понять сущность основных достижений в этой отрасли, осознать существующие тенденции и правильно оценить перспективность тех или иных направлений развития. Компьютерные сети появились сравнительно давно, в 70-х гг. прошлого столетия. Естественно, что компьютерные сети унаследовали много полезных свойств от других, более старых и распространенных телекоммуникационных сетей. В то же время компьютерные сети привнесли в телекоммуникационный мир нечто совершенно новое — они сделали общедоступными огромные объемы информации, созданные цивилизацией за несколько тысячелетий своего существования и продолжающие пополняться с растущей скоростью в наше время.

Результатом влияния компьютерных сетей на остальные типы телекоммуникационных сетей стал процесс их слияния. Этот процесс начался достаточно давно, одним из первых признаков сближения была передача телефонными сетями голоса в цифровой форме. Компьютерные сети также активно идут навстречу телекоммуникационным сетям, разрабатывая новые сетевые сервисы, которые ранее были прерогативой телефонных, радио- и телевизионных сетей — сервисы IP-телефонии, радио- и видеовещания. Процесс слияния продолжается, и о том, каким будет его конечный результат, с уверенностью пока говорить рано. Однако понимание истории развития сетей делает более понятными основные проблемы, стоящие перед разработчиками компьютерных сетей.

Компьютерные сети, которым посвящен данный учебник, отнюдь не являются единственным видом сетей.

Компьютерные сети, называемые также сетями передачи данных, являются логическим результатом эволюции двух важнейших научно-технических отраслей современной цивилизации — компьютерных и телекоммуникационных технологий.

С одной стороны, сети представляют собой частный случай распределенных вычислительных систем, в которых группа компьютеров согласованно решает набор взаимосвязанных задач, обмениваясь данными в автоматическом режиме. С другой стороны, компьютерные сети могут рассматриваться как средство передачи информации

на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

Однако до появления локальных сетей нужно было пройти еще большой путь, так как многотерминальные системы, хотя и имели внешние черты распределенных систем, все еще поддерживали централизованную обработку данных.

Глобальные компьютерные сети очень многое унаследовали от других, гораздо более старых и распространенных глобальных сетей — телефонных. Главное технологическое новшество, которое привнесли с собой первые глобальные компьютерные сети, состояло в отказе от принципа коммутации каналов, на протяжении многих десятков лет успешно использовавшегося в телефонных сетях. Так как прокладка высококачественных линий связи на большие расстояния обходится очень дорого, то в первых глобальных сетях часто использовались уже существующие каналы связи, изначально предназначенные совсем для других целей.

В конце 1980-х гг. отличия между локальными и глобальными сетями проявлялись весьма отчетливо.

Локальные компьютерные сети по определению отличаются от глобальных сетей небольшими расстояниями между узлами сети. Это в принципе делает возможным использование в локальных сетях более качественных линий связи.

Постепенно различия между локальными и глобальными сетевыми технологиями стали сглаживаться. Изолированные ранее локальные сети начали объединять друг с другом, при этом в качестве связующей среды использовались глобальные сети. Тесная интеграция локальных и глобальных сетей привела к значительному взаимопроникновению соответствующих технологий.

Сближение в методах передачи данных происходит на платформе цифровой передачи данных по волоконно-оптическим линиям связи. Высокое качество цифровых каналов изменило требования к протоколам глобальных компьютерных сетей. На первый план вместо процедур обеспечения надежности вышли процедуры обеспечения гарантированной средней скорости доставки информации пользователям, а также механизмы приоритетной обработки пакетов особенно чувствительного к задержкам трафика.

Начиная с 1990-х гг. компьютерные глобальные сети, работающие на основе скоростных цифровых каналов, существенно расширили спектр предоставляемых услуг и догнали в этом отношении локальные сети. Стало возможным создание служб, работа которых связана с доставкой пользователю больших объемов информации в реальном времени.

Компьютерные сети стали логическим результатом эволюции компьютерных и телекоммуникационных технологий. С одной стороны, они являются частным случаем распределенных компьютерных систем, а с другой — могут рассматриваться как средство передачи информации на большие расстояния, для чего в них применяются методы кодирования и мультиплексирования данных, получившие развитие в различных телекоммуникационных системах.

Раздел 1
КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Основные понятия сетей

Коммуникационная сеть — система, состоящая из объектов, осуществляющих функции генерации, преобразования, хранения и потребления продукта, называемых пунктами (узлами) сети, и линий передачи (связей, коммуникаций, соединений), осуществляющих передачу продукта между пунктами.

Информационная сеть — коммуникационная сеть, в которой продуктом генерирования, переработки, хранения и использования является информация.

Вычислительная сеть — это совокупность распределенных в пространстве вычислительных систем, между которыми организовано симметричное информационное взаимодействие, и предназначенных для информационного обслуживания пользователя и/или технических средств.

Оконечное оборудование данных (ООД или DTE — Data Terminal Equipment) — источники и приемники данных. В качестве ООД могут выступать ЭВМ, принтеры, плоттеры и другое вычислительное, измерительное и исполнительное оборудование автоматических и автоматизированных систем.

Аппаратурой окончания канала данных (АКД или DCE — Data Circuit-Terminating Equipment) осуществляется подготовка данных, передаваемых или получаемых ООД от среды передачи данных. АКД может быть конструктивно отдельным или встроенным в ООД блоком.

Станция данных — это ООД и АКД вместе, которую часто называют узлом сети. СУ = ООД + АКД.

1.2. Виды компьютерных сетей

Вычислительные сети классифицируются по ряду признаков:

- расстояние между связываемыми узлами;
- степень интеграции;
- топология соединений узлов сети;
- способ управления;
- степень однородности оборудования;
- право собственности на сети.

1. В зависимости от расстояний между связываемыми узлами различают следующие сети:

- локальные (ЛВС) LAN (Local Area Network) — охватывающие ограниченную территорию;
- корпоративные (масштаба предприятия) — совокупность связанных между собой ЛВС, охватывающих территорию, на которой размещено одно предприятие или учреждение в одном или нескольких близко расположенных зданиях;
- территориальные WAN (Wide Area Network) — охватывающие значительное географическое пространство, в них выделяют:
  - ✓ региональные сети MAN (Metropolitan Area Network) — сети масштаба региона;
  - ✓ глобальные сети — сети глобального масштаба. Особо выделяют единственную в своем роде глобальную сеть Интернет. Реализованная в ней информационная служба World Wide Web (WWW) переводится на русский язык как всемирная паутина — это сеть сетей со своей технологией. В Интернете существует понятие интрасетей (Intranet) — корпоративных сетей в рамках Интернета.

Отличительные особенности ЛВС

ЛВС — одноузловая сеть с единой средой передачи данных — моноканалом (МК), например, коаксиальный или оптоволоконный кабель или витая пара (рис. 1.1).

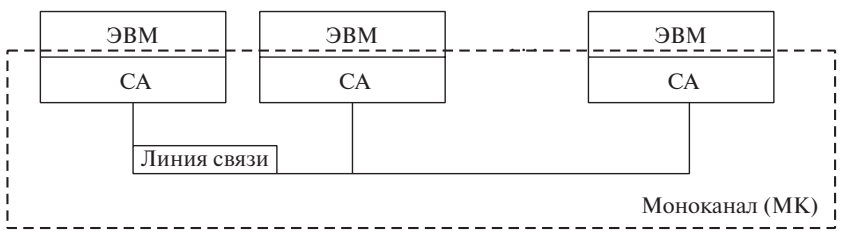


Рис. 1.1. ЛВС

Признаком ЛВС является небольшая протяженность. На практике — от нескольких метров до 10 км (в зависимости от СПД). При значительной протяженности через определенное расстояние в МК должны быть предусмотрены усилители сигнала (репитеры).

Отличительные особенности ТВС

ТВС (WAN) — это многоузловая сеть. Соединение между несколькими узлами осуществляется с помощью коммутаторов (маршрутизаторов) или шлюзов (рис. 1.2).

Шлюз — средство коммутации различных кабельных систем. Соединения узлов могут быть избыточными.

Основной признак ТВС — наличие многих узлов и большая протяженность — до нескольких тысяч километров.

Корпоративные ВС занимают промежуточное положение между ЛВС и ТВС и используются в масштабах одного предприятия.

2. В зависимости от степени интегрированности различают интегрированные и неинтегрированные сети и подсети.

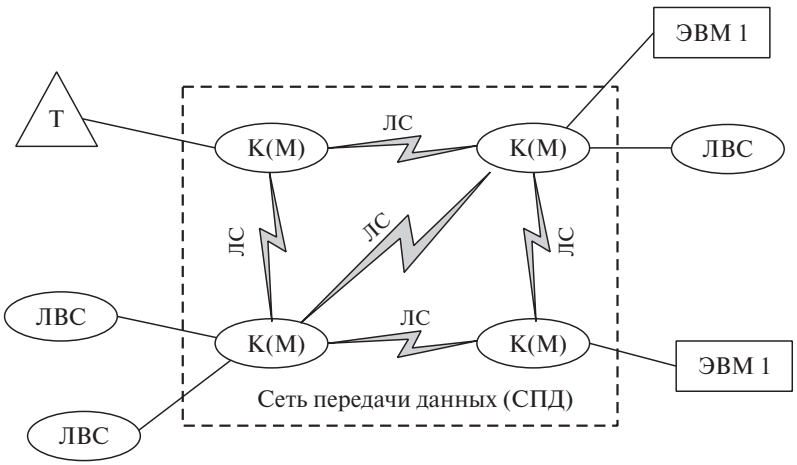


Рис. 1.2. ТВС

Интегрированная вычислительная сеть (интерсеть) представляет собой взаимосвязанную совокупность многих вычислительных сетей, которые в интерсети называются подсетями.

Интерсети нужны для объединения таких подсетей, а также для объединения технических средств автоматизированных систем проектирования и производства в единую систему комплексной автоматизации (CIM — Computer Integrated Manufacturing). Обычно интерсети приспособлены для различных видов связи: телефонии, электронной почты, передачи видеоинформации, цифровых данных и т.п., и в этом случае они называются сетями интегрального обслуживания.

3. В зависимости от топологии соединений узлов различают сети структур:

- шинная (магистральная);
- кольцевая;
- звездообразная;
- иерархическая;
- смешанная.

Среди ЛВС наиболее распространены:

- шинная (bus) — локальная сеть, в которой связь между любыми двумя станциями устанавливается через один общий путь и данные, передаваемые любой станцией, одновременно становятся доступными для всех других станций, подключенных к этой же среде передачи данных (последнее свойство называют широковещательностью);
- кольцевая (ring) — узлы связаны кольцевой линией передачи данных (к каждому узлу подходят только 2 линии); данные, проходя по кольцу, поочередно становятся доступными всем узлам сети;
- звездная (star) — имеется центральный узел, от которого расходятся линии передачи данных к каждому из остальных узлов (рис. 1.3).

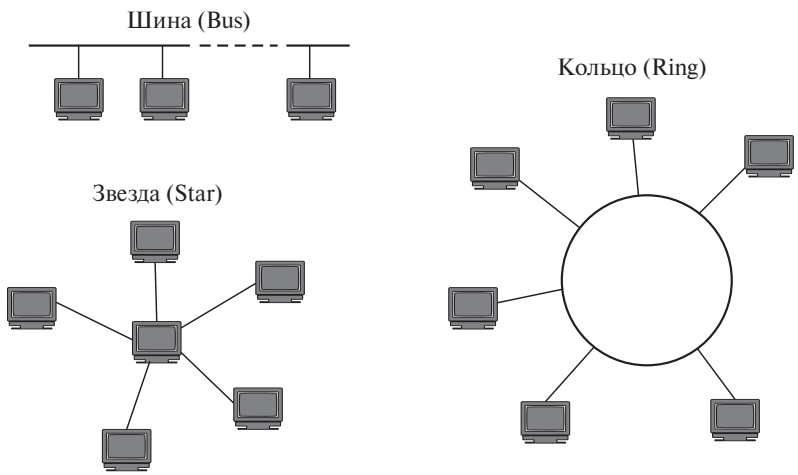


Рис. 1.3. Основные топологические структуры локальных вычислительных сетей

4. В зависимости от способа управления различают сети:

- клиент–сервер — 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;

- 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, то каждый узел в одноранговых сетях может выполнять функции и клиента, и сервера;
- сетецентрические — пользователь имеет лишь дешевое оборудование для обращения к удаленным компьютерам, а сеть обслуживает заказы на выполнение вычислений и получения информации. То есть пользователю не нужно приобретать программное обеспечение для решения прикладных задач, ему нужно лишь платить за выполненные заказы. Подобные компьютеры называют тонкими клиентами или сетевыми компьютерами.

5. В зависимости от того, одинаковые или неодинаковые ЭВМ применяют в сети, различают сети:

- однотипных ЭВМ, называемые однородными;
- разнотипных ЭВМ — неоднородные (гетерогенные).

В крупных автоматизированных системах (АСУ), как правило, сети оказываются неоднородными.

6. В зависимости от прав собственности на сети последние могут быть:

- сетями общего пользования (public);
- частными (private).

Среди сетей общего пользования выделяют телефонные сети (PSTN — Public Switched Telephone Network) и сети передачи данных (PSDN — Public Switched Data Network).

Классификация сетей показана на рис. 1.4.

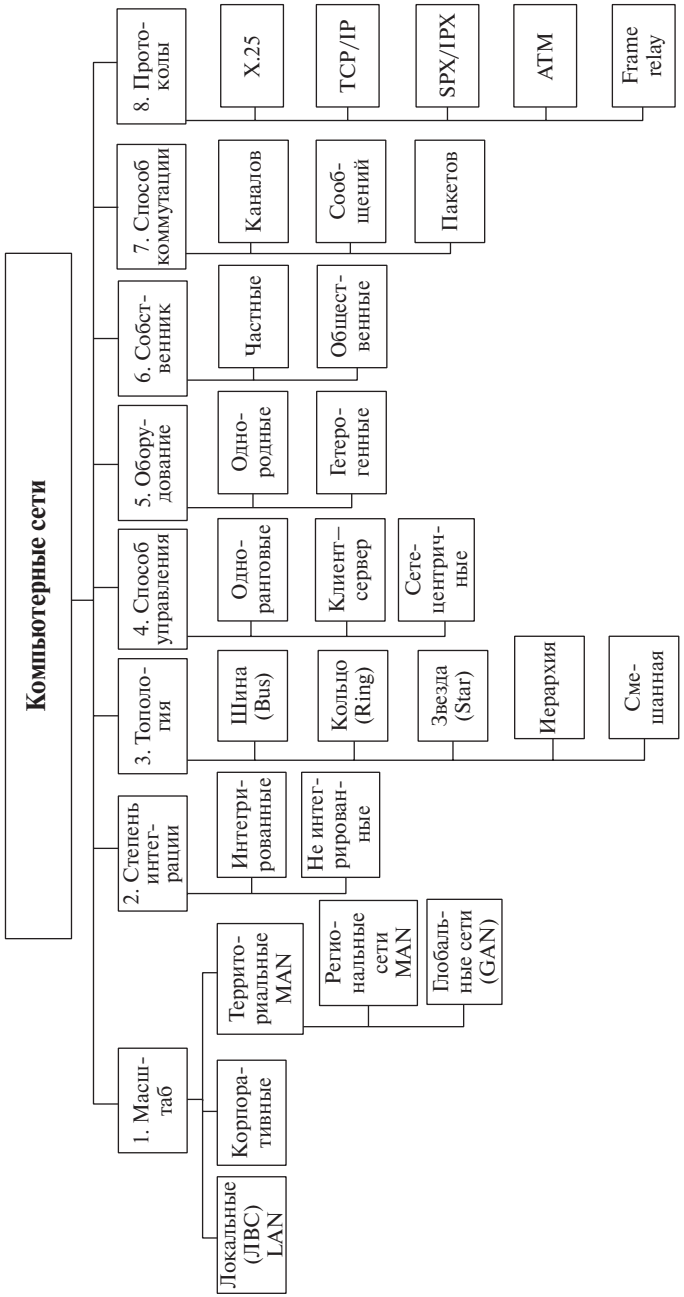


Рис. 1.4. Общая классификация компьютерных сетей

1.3. Контрольные вопросы

1. Что понимается под архитектурой вычислительной сети?
2. Какие устройства относятся к АКД?
3. Какие устройства относятся к ООД?
4. Перечислить основные функции узла сети.
5. Что такое сетевой узел?

6. Классификация вычислительных сетей по размеру.
7. Что такое WAN, LAN, MAN, PAN?
8. Основные отличия одноранговых ЛВС от ЛВС типа «клиент–сервер».
9. Какие достоинства и недостатки присущи одноранговым ЛВС и ЛВС типа «клиент–сервер»?
10. Какие топологии наиболее широко применяются в ЛВС?

Раздел 2
ПРОТОКОЛЫ ПЕРЕДАЧИ ДАННЫХ

2.1. Стандарты и протоколы

Протоколы — это набор семантических и синтаксических правил, определяющий поведение функциональных блоков сети при передаче данных.

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 для сети ARPANET и применяемые в глобальной сети Интернет, объединяют под названием TCP/IP;
- протоколы открытых систем Международной организации по стандартизации (ISO — Intrenational Standard Organization);
- протоколы Международного телекоммуникационного союза (ITU — International Telecommunication Union, ранее называвшегося CCITT);
- протоколы Института инженеров по электротехнике и электронике (IEEE — Institute of Electrical and Electronics Engineers).
- Протоколы ISO являются семиуровневыми и известны как протоколы базовой эталонной модели взаимосвязи открытых систем (ЭМВОС).

2.2. Эталонная модель взаимодействия открытых систем

Базовая ЭМВОС — это модель, принятая ISO для описания общих принципов взаимодействия информационных систем. ЭМВОС признана всеми международными организациями как основа для стандартизации протоколов информационных сетей, более известна как OSI — Open System Interconnection.

В OSI информационная сеть рассматривается как совокупность функций, которые делятся на группы, называемые уровнями.

Разделение на уровни позволяет вносить изменения в средства реализации одного уровня без перестройки средств других уровней, что значительно упрощает и удешевляет модернизацию средств по мере развития техники.

OSI содержит семь уровней. Ниже приведены их номера, названия и выполняемые функции (рис. 2.1).

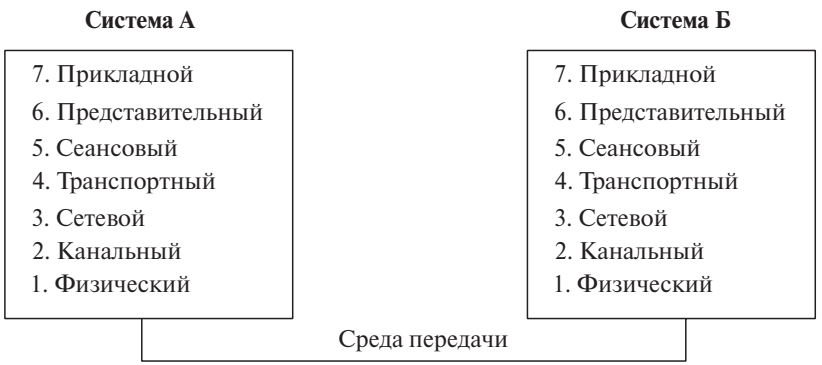


Рис. 2.1. Интерпретация передачи данных по модели OSI

7-й уровень — прикладной (Application): включает средства управления прикладными процессами; эти процессы могут объединяться для выполнения поставленных заданий, обмениваться между собой данными. На этом уровне определяются и оформляются в блоки те данные, которые подлежат передаче по сети. Уровень включает, например, такие средства для взаимодействия прикладных программ, как прием и хранение пакетов в «почтовых ящиках» (mail-box).

Уровень приложений модели OSI поддерживает компоненты, определяющие взаимодействие пользователей с компьютерами. Этот уровень ответствен за идентификацию и установление доступности

предполагаемого партнера по диалогу. Здесь же определяется, достаточно ли ресурсов для взаимодействия.

6-й уровень — представительный (Presentation): реализуются функции представления данных (кодирование, форматирование, структурирование). Например, на этом уровне выделенные для передачи данные преобразуются из кода EBCDIC в ASCII и т.п.

5-й уровень — сеансовый (Session): предназначен для организации и синхронизации диалога, ведущегося объектами (станциями) сети. На этом уровне определяются тип связи (дуплекс или полудуплекс), начало и окончание заданий, последовательность и режим обмена запросами и ответами взаимодействующих партнеров.

4-й уровень — транспортный (Transport): предназначен для управления сквозными каналами в сети передачи данных. На этом уровне обеспечивается связь между оконечными пунктами (в отличие от следующего сетевого уровня, на котором обеспечивается передача данных через промежуточные компоненты сети). К функциям транспортного уровня относятся мультиплексирование и демультиплексирование (сборка-разборка пакетов), обнаружение и устранение ошибок в передаче данных, реализация заказанного уровня услуг (например, заказанной скорости и надежности передачи).

3-й уровень — сетевой (Network): на этом уровне происходит:

1) формирование пакетов по правилам тех промежуточных сетей, через которые проходит исходный пакет и маршрутизация пакетов, т.е. определение и реализация маршрутов, по которым передаются пакеты;

2) образование логических каналов. Логическим каналом называется виртуальное соединение двух или более объектов сетевого уровня, при котором возможен обмен данными между этими объектами. Понятию логического канала необязательно соответствие некоего физического соединения линий передачи данных между связываемыми пунктами. Это понятие введено для абстрагирования от физической реализации соединения;

3) контроль нагрузки на сеть с целью предотвращения перегрузок, отрицательно влияющих на работу сети.

2-й уровень — канальный (Link, уровень звена данных): предоставляет услуги по обмену данными между логическими объектами предыдущего сетевого уровня и выполняет функции, связанные с формированием и передачей кадров, обнаружением и исправлением ошибок, возникающих на следующем, физическом, уровне. Кадром называется пакет канального уровня, поскольку пакет на предыдущих уровнях может состоять из одного или многих кадров.

1-й уровень — физический (Physical): предоставляет механические, электрические, функциональные и процедурные средства для установления, поддержания и разъединения логических соединений между логическими объектами канального уровня. Реализует функции передачи битов данных через физические среды. Именно на физическом уровне осуществляются представление информации в виде электрических или оптических сигналов, преобразования формы сигналов, выбор параметров физических сред передачи данных.

В конкретных случаях может возникать потребность в реализации лишь части названных функций, тогда соответственно в сети имеется лишь часть уровней.

Так, в простых (неразветвленных) ЛВС отпадает необходимость в средствах сетевого и транспортного уровней. В то же время сложность функций канального уровня делает целесообразным его разделение в ЛВС на два подуровня:

- управление доступом к каналу (MAC — Medium Access Control);
- управление логическим каналом (LLC — Logical Link Control). К подуровню LLC в отличие от подуровня MAC относится часть функций канального уровня, не связанных с особенностями передающей среды.

Передача данных через разветвленные сети происходит при использовании инкапсуляции/декапсуляции порций данных.

Так, сообщение, пришедшее на транспортный уровень, делится на сегменты, которые получают заголовки и передаются на сетевой уровень.

Сегментом обычно называют пакет транспортного уровня.

Сетевой уровень организует передачу данных через промежуточные сети. Для этого сегмент может быть разделен на части (пакеты), если сеть не поддерживает передачу сегментов целиком. Пакет снабжается своим сетевым заголовком (т.е. происходит инкапсуляция).

При передаче между узлами промежуточной ЛВС требуется инкапсуляция пакетов в кадры с возможной разбивкой пакета. Приемник декапсулирует сегменты и восстанавливает исходное сообщение.

2.3. Базовая сеть передачи данных

Пара абонентов сети взаимодействуют друг с другом через сеть передачи данных (СПД), которая представляет собой программно-аппаратную среду (рис. 2.2).

СПД построена таким образом, что физическое место расположения прикладных процессов не играет роли. Они могут выполняться внутри сетевого узла или быть удалены на тысячи километров.

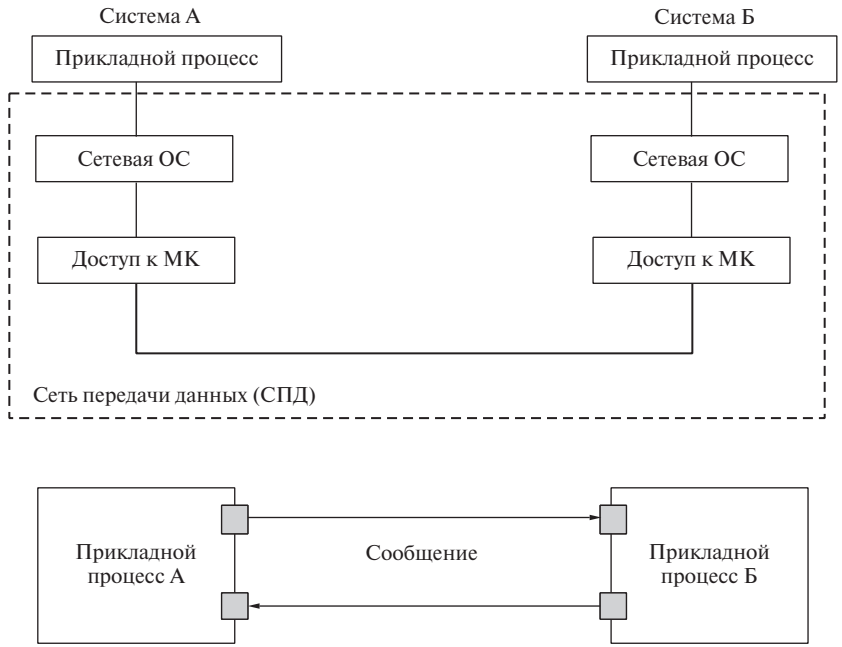


Рис. 2.2. БСПД

Так как сообщения могут иметь произвольную длину, то длинные сообщения могут надолго занять соответствующую среду передачи, поэтому в большинстве современных сетевых технологий среда используется в мультипликативном режиме между различными парами абонентов и произвольные сообщения делятся на пакеты фиксированной длины (0,5–4 Кб) (рис. 2.3).

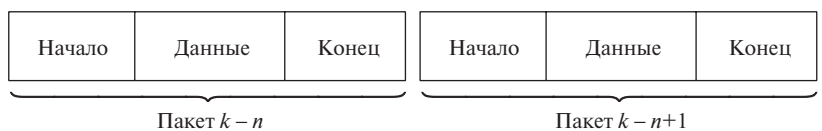


Рис. 2.3. Последовательность пакетов

Два прикладных процесса обмениваются между собой сообщениями через соответствующие логические порты.

Надо учитывать большие накладные расходы:

- увеличивается процент передачи служебной информации при маленьких пакетах;
- при больших пакетах нарушается динамика использования МК;
- увеличиваются накладные расходы по доставке испорченных пакетов.

Для обеспечения прозрачности взаимодействия двух абонентов (квазинезависимости взаимодействия абонента от аппаратной и программной реализации среды и отдельных компонентов среды) взаимодействие между двумя абонентами разбивается на несколько уровней. Каждый уровень решает свой набор задач сетевого взаимодействия.

Организация ISO и МККТТ предлагают использование семиуровневого взаимодействия через сеть. Этот стандарт называется семиуровневой эталонной моделью взаимодействия открытых систем.

Каждому уровню взаимодействия соответствует свой протокол (рис. 2.4).

Рис. 2.4. Уровни взаимодействия

Окончательная цель — обеспечение взаимодействия прикладных процессов на уровне 7. Многоуровневая организация обеспечивает независимость реализации протоколов верхних уровней от конкретной аппаратно-программной организации протоколов на нижних уровнях.

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 (табл. 2.1).

Таблица 2.1

<table>
<tr><td colspan="2">Уровень ЭМВОС (модельOSI)</td><td colspan="4">Виды протокольных стеков, используемых в ЛВС</td></tr>
<tr><td>№</td><td>Название</td><td>X.25</td><td colspan="2">SPX/IPX</td><td>TCP/IP</td></tr>
<tr><td>7</td><td>Прикладной</td><td>X.399</td><td rowspan="3"></td><td rowspan="3">NCP, SAP</td><td rowspan="4">FTP, TFTP, TelNet, WWW, SNMP, SMTP, DSN</td></tr>
<tr><td>6</td><td>Представительный</td><td>X.226</td></tr>
<tr><td>5</td><td>Сеансовый</td><td>X.225</td><td>Эмулятор Net Bios</td></tr>
<tr><td>4</td><td>Транспортный</td><td>X.224</td><td colspan="2">SPX</td><td>TCP, UDP</td></tr>
<tr><td>3</td><td>Сетевой</td><td>X.25</td><td colspan="2">IPX, RIP, NLSP</td><td>IP, RIP, OSPF, ICMP, IGMP</td></tr>
<tr><td>2</td><td>Канальный</td><td>BSC, SDLC/ HDLC</td><td colspan="2" rowspan="2">IEEE802</td><td>IEEE804, SLIP, PPP, CLIP, 2 MAC, 2 LLC</td></tr>
<tr><td>1</td><td>Физический</td><td>X.21, X.21bis</td><td></td></tr>
</table>

Протокол — правило взаимодействия одноименных уровней управления в разных системах.

Интерфейс — правило взаимодействия смежных уровней управления в одной и той же системе.

Протокол i-го уровня реализуется с помощью интерфейса с $(i-1)$-м уровнем и протокола $(i-1)$-го (более низкого) уровня и т.д.

Протоколы значительно сложнее и важнее интерфейсов, так как они должны обеспечивать корректное взаимодействие объектов, находящихся в разных системах, в условиях, когда поведение другой системы неизвестно и непредсказуемо.

2.4. Функции уровней управления сетью

Физический уровень (протокол) определяет правило взаимодействия различных сетевых узлов на битовом уровне, определяет амплитуду, длительность, полярность, синхронизацию, правила пере-

дачи импульсов и т.п. Предоставляет механические, электрические, функциональные и процедурные средства для установления, поддержания и разъединения логических соединений между логическими объектами канального уровня. Реализует функции передачи битов данных через физические среды.

Именно на физическом уровне осуществляются представление информации в виде электрических или оптических сигналов, преобразования формы сигналов, выбор параметров физических сред передачи данных.

Для большинства ЛВС в среде передачи передается цифровая информация (последовательности «0» и «1»). Протокол физического уровня также может описывать сжатие данных.

Минимизация числа проводников для экономии средств приводит к отсутствию специального провода для передачи синхроимпульсов, поэтому используют так называемое манчестерское кодирование, которое позволяет по одной паре передавать одновременно и информацию, и синхроимпульсы.

Канальный уровень (протокол) отвечает за передачу каждого отдельного кадра между сетевыми узлами, определяет формат и типы кадров, правила взаимодействия кадров различных типов (информационного и служебного).

Кадром называется пакет канального уровня, поскольку пакет на верхних уровнях может состоять из одного или многих кадров.

Канальный уровень предоставляет услуги по обмену данными между логическими объектами сетевого уровня и выполняет функции, связанные с формированием и передачей кадров, обнаружением и исправлением ошибок, возникающих на физическом уровне.

Основными являются два механизма: квитирования и тайм-аута. Основная их функция — повышение достоверности передаваемых данных, что происходит за счет этих механизмов и наличия в формате кадра CRC.

Наиболее типичный формат кадра, включающего пакет данных, представлен на рис. 2.5.

Маркер начала	Адрес приемника	Адрес источника	Тип пакета	ДАННЫЕ	CRC	Маркер конца

Рис. 2.5. Структура кадра

При анализе CRC происходит проверка правильности принятой последовательности бит.

Суть квитирования и тайм-аута: на каждый полученный информационный пакет приемник отвечает квитанцией (положительной или отрицательной).

СУ источника до получения положительной квитанции сохраняет в памяти информационный пакет и при получении отрицательной квитанции повторяет передачу этого испорченного пакета (рис. 2.6).

Если квитанция вообще не пришла (неисправен приемник и/или линия связи), включается механизм тайм-аута и после истечения определенного времени СУ источника ведет повторную попытку передачи.

Для ускорения работы в надежных сетях иногда посылается групповая квитанция — на несколько кадров.

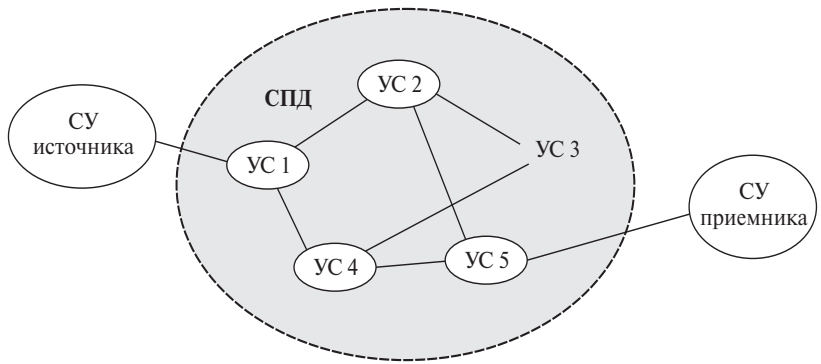


Рис. 2.6. Передача информации через узлы связи

Сетевой уровень (протокол) решает задачу продвижения пакета через всю СПД от узла связи, смежного с абонентом-источником, до УС, смежного с абонентом-приемником.

Сетевой протокол, например, на рис. 1.10 обеспечивает передачу от УС1 до УС5. УС — узел связи (коммутатор или маршрутизатор).

Так как чисто локальные сети являются одноузловыми, то этот уровень не нужен (не применяется).

Основная задача сетевого уровня — оптимальная маршрутизация передаваемых пакетов, т.е. определение и реализация маршрутов, по которым передаются пакеты. В общем случае пути прохождения различных логически связанных пакетов между одной и той же парой абонентов могут не совпадать.

Основная задача коммуникационного компьютера — определение дальнейшего маршрута (наиболее выгодного) для пакета.

При определении оптимального маршрута учитываются следующие факторы:

- время доставки пакета;
- стоимость доставки;
- пропускная способность линии связи;
- надежность доставки (правильность информации).

На сетевом уровне, помимо решения задач маршрутизации пакетов, также решаются следующие задачи:

1. Установление логического соединения. Другими словами, маршрутизация сводится к образованию логических каналов. Логическим каналом называется виртуальное соединение двух или более объектов сетевого уровня, при котором возможен обмен данными между этими объектами. Понятию логического канала необязательно соответствие некоего физического соединения линий передачи данных между связываемыми пунктами. Это понятие введено для абстрагирования от физической реализации соединения.

2. Контроль нагрузки на сеть с целью предотвращения перегрузок, отрицательно влияющих на работу сети.

Транспортный уровень (протокол) предназначен для управления сквозными каналами в сети передачи данных и определяет правило взаимодействия сетевого узла с СПД (рис. 2.7). Это протокол взаимодействия типа компьютер–компьютер. На этом уровне обеспечивается связь между оконечными пунктами (в отличие от сетевого уровня, на котором обеспечивается передача данных через промежуточные компоненты сети). Выше транспортного уровня обмен уже идет сообщениями.

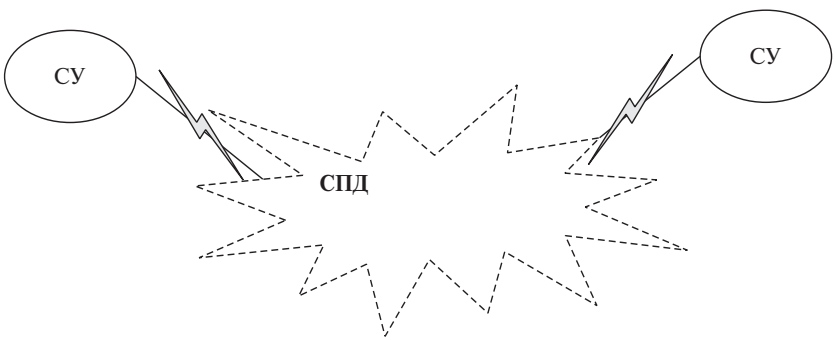


Рис. 2.7. Транспортный уровень

К функциям транспортного уровня относятся:

- разбиение передаваемого сообщения на отдельные пакеты на передающей стороне — мультиплексирование и демультиплексирование (сборка-разборка пакетов);
- сборка из отдельных пакетов всего сообщения на приемной стороне. Обычно пакеты приходят в произвольной последовательности;
- обнаружение и устранение ошибок в передаче данных;
- реализация заказанного вида услуг (скорость, надежность передачи данных).

В общем случае существуют два режима передачи пакетов через СПД:

- дейтаграммный режим. Сеть отвечает за доставку отдельного пакета, не обеспечивая подтверждение доставки. Пример дейтаграммного протокола — протокол UDP в протокольном стеке TCP/IP;
- режим виртуального (логического) канала. Обеспечивает организацию некоторого логического канала связи между двумя абонентами, и сеть обеспечивает достоверность доставки каждого пакета, что является основной задачей организации 5-го уровня. Пример протокола виртуального канала — протокол TCP в протокольном стеке TCP/IP.

Сеансовый уровень (протокол) предназначен для организации и синхронизации диалога, ведущегося объектами (станциями) сети. Описывает формат и правило взаимодействия специальных служебных пакетов, с помощью которых создается, а затем разрушается сетевой виртуальный канал. На этом уровне определяются тип связи (дуплекс или полудуплекс), начало и окончание заданий, последовательность и режим обмена запросами и ответами взаимодействующих партнеров.

Основными служебными пакетами являются: установление соединения (инициатором может быть любой абонент), подтверждение соединения, разъединение, подтверждение разъединения.

Основная задача уровня — гарантированная доставка всего сообщения (через виртуальный канал).

Представительный уровень (протокол) унифицирует форму представления сообщения для сети конкретного типа. Реализуются функции представления данных (кодирование, форматирование, структурирование).

Прикладной уровень. На нем функционируют любые прикладные процессы пользователя, а также служебные прикладные процессы

верхнего уровня (например, протокол удаленного запуска задания). Обмен сообщениями осуществляется через логические порты, включает средства управления прикладными процессами; эти процессы могут объединяться для выполнения поставленных заданий, обмениваться между собой данными. На этом уровне определяются и оформляются в блоки те данные, которые подлежат передаче по сети.

Среди протоколов модели OSI различают сетезависимые и сетенезависимые. Физический, канальный, сетевой уровни (1–3) — сетезависимые. Транспортный уровень (4) — промежуточный. Сеансовый, представительный и прикладной (5–7) — сетенезависимые.

2.5. Особенности многоуровневого управления сетью в ЛВС

В конкретных случаях может возникать потребность в реализации лишь части названных функций, тогда, соответственно, в сети имеется лишь часть уровней. В чистой ЛВС (так как они одноранговые) отключены функции 3-го (сетевого) уровня, но это не означает, что в сетевых ОС, рассчитанных на работу в ЛВС, отсутствует поддержка этого уровня.

В простых (неразветвленных) ЛВС не требуется обеспечивать большинство функций, относящихся к сетевому и транспортному уровням ЭМВОС, поэтому выполняемые функции разделены между физическим и канальным уровнями, причем сложность функций канального уровня делает целесообразным его разделение (расщепление) в ЛВС на два подуровня (рис. 2.8):

Рис. 2.8. Многоуровневое управление сетью в ЛВС

- управление доступом к среде (MAC — Media Access Channel) обеспечивает правила доступа к моноканалам;
- управление логическим каналом (канальный уровень) (LLC) — логическая передача данных.

К подуровню LLC в отличие от подуровня MAC относится часть функций канального уровня, не связанных с особенностями передающей среды.

Передача данных через разветвленные сети происходит при использовании инкапсуляции/декапсуляции порций данных. Так, сообщение, пришедшее на транспортный уровень, делится на сегменты, которые получают заголовки и передаются на сетевой уровень. Сегментом обычно называют пакет транспортного уровня.

Сетевой уровень организует передачу данных через промежуточные сети. Для этого сегмент может быть разделен на части (пакеты), если сеть не поддерживает передачу сегментов целиком. Пакет снабжается своим сетевым заголовком (т.е. происходит инкапсуляция).

При передаче между узлами промежуточной ЛВС требуется инкапсуляция пакетов в кадры с возможной разбивкой пакета. Приемник декапсулирует сегменты и восстанавливает исходное сообщение.

Многоуровневая эталонная модель взаимодействия открытых систем для источника, промежуточного узла и пункта назначения показана на рис. 2.9.

Три самых нижних уровня — физический, линии связи и сетевой — выполняют основные сетевые функции.

В результате в связке, охватывающей узел-источник, промежуточный узел и узел назначения, все семь уровней модели используются только у первого и третьего узлов, или у источника и получателя.

В промежуточном узле исполняются только сервисы трех нижних уровней, необходимые для сетевой маршрутизации и соединения.

Родоначальниками большинства канальных протоколов в различных сетях стали байт-ориентированный протокол BSC и бит-ориентированный протокол HDLC. Особенно популярны разновидности HDLC. К таким протоколам можно отнести канальные протоколы IEEE 802.X, протокол LAPB для сетей X.25 и др.

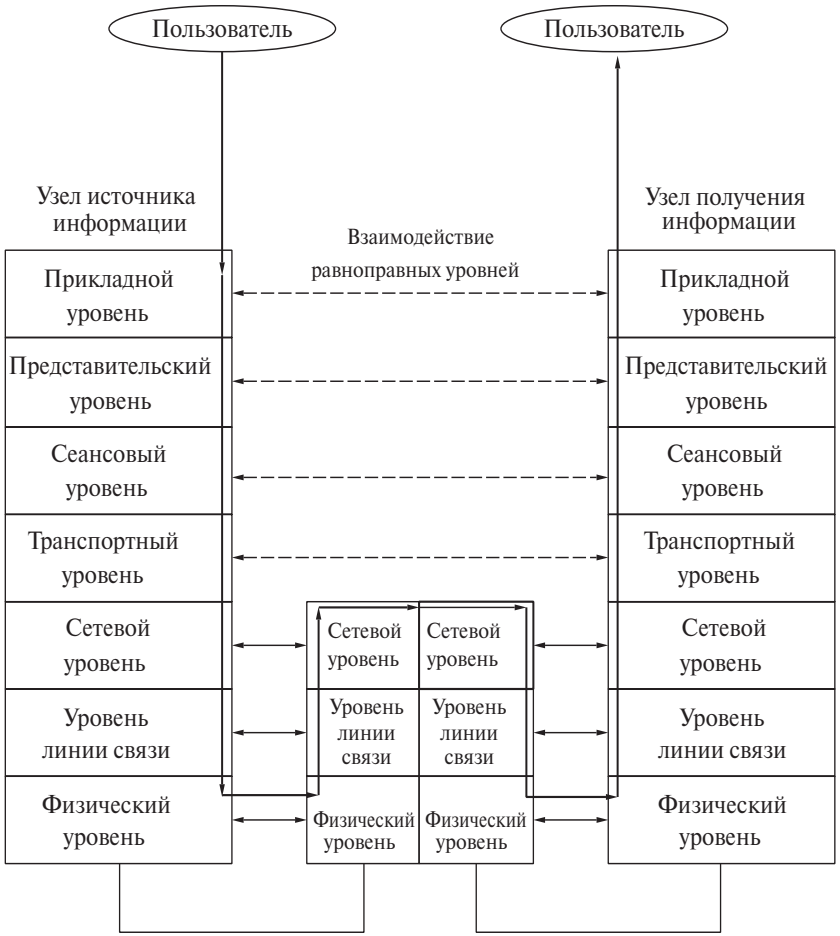


Рис. 2.9. Модель взаимодействия открытых систем

2.6. Контрольные вопросы

1. Назначение многоуровневой модели взаимодействия открытых систем.
2. В чем отличие ISO от OSI?
3. Нарисовать OSI-модель.
4. Перечислить уровни OSI-модели.
5. Основные функции каждого уровня OSI-модели.
6. На каком уровне OSI-модели реализуются функции доступа к среде передачи данных?
7. На каком уровне OSI-модели реализуются функции маршрутизации?
8. На каком уровне OSI-модели появляется свойство адресуемости?
9. Какая топология СПД обладает максимальной (минимальной) надежностью?
10. Какая топология СПД обладает максимальным (минимальным) временем доставки сообщений?
11. Какая топология СПД обладает максимальной (минимальной) производительностью?
12. В чем отличие логической топологии от физической?

Раздел 3
МЕТОДЫ ДОСТУПА К СРЕДЕ ПЕРЕДАЧИ ДАННЫХ

3.1. Особенности доступа

Одной из важнейших характеристик конкретной сетевой технологии ЛВС является метод доступа к МК.

Среды передачи ЛВС — любые, кроме сотовой и спутниковой связи. Типичная среда передачи данных в ЛВС — отрезок (сегмент) коаксиального кабеля. К нему через аппаратуру окончания канала данных (АОКД) подключаются узлы — компьютеры и, возможно, общее периферийное оборудование.

Поскольку среда передачи данных общая, а запросы на сетевые обмены у узлов появляются асинхронно, то возникает проблема разделения общей среды между многими узлами, другими словами, проблема обеспечения доступа к сети.

Доступом к сети называют взаимодействие станции (узла сети) со средой передачи данных для обмена информацией с другими станциями. Управление доступом к среде — это установление последовательности, в которой станции получают доступ к среде передачи данных.

Методы доступа к моноканалу определяют правила общего (совместного) использования МК всеми подключенными к нему узлами. Возможность использования того или иного метода доступа зависит от топологии сети.

Для различных топологий ЛВС применяются соответствующие методы доступа, причем одни могут использоваться во всех топологиях, другие — только в некоторых или даже только в одной.

Существуют различные методы доступа к МК, чтобы не было интерференции сигналов в средах передачи.

Различают случайные и детерминированные методы доступа.

Наибольшее распространение нашел случайный метод доступа к МК, когда каждая станция в любой момент времени может передавать независимо от других.

Из-за возникновения коллизии между двумя СУ происходит существенная потеря пропускной способности МК.

Случайный метод доступа может быть использован только в шинных и магистральных сетях.

Конфликтом называется ситуация, при которой две или более станции «одновременно» пытаются захватить линию.

Понятие «одновременность событий» в связи с конечностью скорости распространения сигналов по линии конкретизируется как отставание событий во времени не более чем на величину 2×Td, называемую окном столкновений, где Td — время прохождения сигналов по линии между конфликтующими станциями.

Если какие-либо станции начали передачу в окне столкновений, то по сети распространяются искаженные данные.

Это искажение и используется для обнаружения конфликта либо сравнением в передатчике данных, передаваемых в линию (неискаженных) и получаемых из нее (искаженных), либо по появлению постоянной составляющей напряжения в линии, что обусловлено искажением используемого для представления данных манчестерского кода.

Обнаружив конфликт, станция должна оповестить об этом партнера по конфликту, послав дополнительный сигнал затора, после чего станции должны отложить попытки выхода в линию на время Td.

Очевидно, что значения Td должны быть различными для станций, участвующих в столкновении (конфликте); поэтому Td — случайная величина. Ее математическое ожидание должно иметь тенденцию к росту по мере увеличения числа идущих подряд неудачных попыток захвата линии.

3.2. Случайные методы доступа

Существуют следующие случайные методы доступа:

1. Простейший случайный метод доступа.
2. Синхронный случайный метод доступа.
3. Множественный доступ с контролем несущей и обнаружением коллизии.
4. Множественный доступ с контролем несущей и устранением коллизии.

3.2.1. Простейший случайный метод доступа

Каждый СУ может начать передачу в любой произвольный момент времени, но такую передачу могут одновременно начать два и более СУ. В подобных случаях происходит столкновение пакетов

(взаимное искажение), называемое коллизией. Каждый СУ должен уметь обнаруживать это событие.

При обнаружении коллизии каждый СУ, передавший пакет, вырабатывает случайный момент времени (тайм-аут), в течение которого этот узел будет ожидать момента для следующей попытки передачи данных.

Способы выявления коллизии:

1) побитовое сравнение переданной и принятой информации (рис. 3.1);

2) с помощью амплитудного компаратора:

а) два сигнала складываются в МК;

б) основан на применении манчестерского кода. Средние составляющие напряжения сигнала «0» и сигнала «1» одинаковы по модулю и противоположны по знаку относительно некоторой средней линии. При отсутствии коллизии и манчестерском кодировании через МК передается практически меандр.

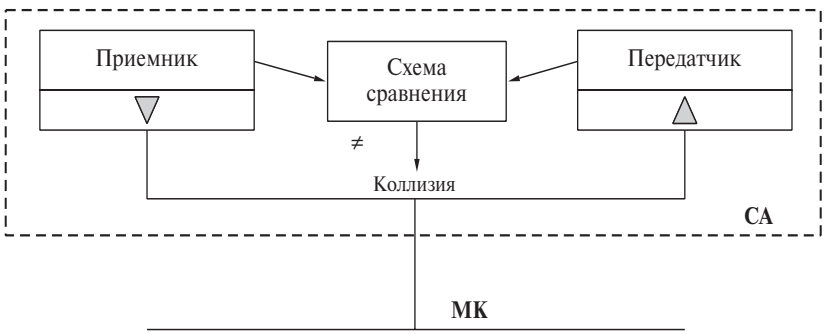


Рис. 3.1. Структура сравнения информации

Если условно провести пунктирную линию между уровнями «0» и «1» и с некоторым приближением принять ее за линию нулевого значения, то интеграл от разнополярных сигналов будет близок к нулю при успешной передаче и отличен от нуля при коллизии. Виртуальная средняя линия при коллизии отклонится от нуля, и сработает амплитудный компаратор.

В реальных сетях в начале пакета передают преамбулу, чтобы сразу легко определить коллизию.

Важной характеристикой любого метода доступа является интервал коллизии — интервал времени, в течение которого два пакета могут потенциально столкнуться.

Для анализа пропускной способности МК в зависимости от интенсивности потока пакетов, которые нужно передать, введем величины:

- относительная приведенная пропускная способность МК измеряется в числе пакетов, переданных за время передачи одного пакета:
  - ✓ S[пак/T] , S = 0÷1, причем S = f(G);
  - ✓ G[пак/T] — относительная приведенная интенсивность пакетов — число пакетов, которые генерируются всеми СУ для передачи, т.е. тех, которые нужно передать в единицу времени;
- при определенной загрузке сети существует некоторое оптимальное значение времени тайм-аута — $\tau_{опт}$.

3.2.2. Синхронный случайный метод доступа

При его реализации можно начинать передачу информации не в произвольные моменты времени, а только в фиксированные, отстающие друг от друга на величину T (рис. 3.2).

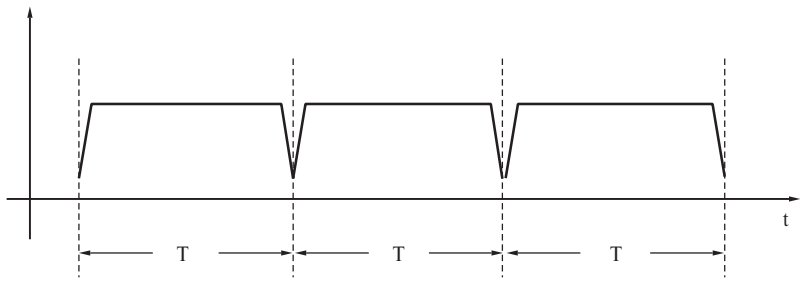


Рис. 3.2. Синхронный случайный метод доступа

В этом случае коллизия может произойти в течение этого времени T, так как отсутствует контроль занятости МК перед началом передачи.

Обнаружив коллизию, станция все равно продолжает передавать пакет до конца.

3.2.3. Множественный доступ с контролем несущей и обнаружением коллизии (CSMA/CD — Carrier Sense Multiply Access / Collision Detection)

Среди случайных методов наиболее известен метод множественного доступа с контролем несущей и обнаружением конфликтов (МДКН/ОК).

Англоязычное название метода — Carrier Sense Multiple Access / Collision Detection (CSMA/CD).

Суть метода МДКН/ОК, применяющегося в Ethernet, состоит в следующем.

Этот метод основан на контроле несущей в линии передачи данных и устранении конфликтов, возникающих из-за попыток одновременного начала передачи двумя или более станциями, путем повторения попыток захвата линии через случайный отрезок времени.

МДКН/ОК является широковещательным (broadcasting) методом.

Все станции при применении МДКН/ОК равноправны по доступу к сети.

Если линия передачи данных свободна, то в ней отсутствуют электрические колебания, что легко распознается любой станцией, желающей начать передачу. Такая станция захватывает линию.

Любая другая станция, желающая начать передачу в некоторый момент времени t, если обнаруживает электрические колебания в линии, то откладывает передачу до момента t + td, где td — задержка.

Каждый СУ при наличии информации, готовой к передаче, сначала прослушивает МК (впрочем, он это делает постоянно в течение всего времени работы) и, если он свободен, начинает передачу. В противном случае если он занят, то существует несколько разновидностей поведения СУ:

- настойчивые станции (PN = 1);
- ненастойчивые (PN = 0);
- настойчивые со степенью настойчивости P = 0÷1.

Ненастойчивые СУ, застав МК занятым, откладывают повторную передачу на случайное время τ, по истечении которого они опять будут контролировать, свободен ли МК или еще нет. В ненастойчивом МДКН/ОК задержка td является случайной величиной.

Настойчивые СУ продолжают прослушивать МК до момента его освобождения, и как только он освободится, сразу начинают передачу (рис. 3.3). Таким образом, попытка захвата канала происходит сразу после его освобождения, что допустимо при слабой загрузке сети. С ростом количества настойчивых станций вероятность столкновения увеличивается, но если их мало, они обладают высоким приоритетом, что позволяет им передавать пакеты за меньшее время. При заметной загрузке велика вероятность того, что несколько станций будут претендовать на доступ к сети сразу после ее освобождения, и, следовательно, конфликты станут частыми.

СУ с некоторой вероятностью настойчивости ведет себя в некоторых случаях как настойчивая станция, а в других — как ненастойчивая.

Рассмотрим два наиболее удаленных СУ, которым одновременно нужно передавать.

В реальных сетевых технологиях (Ethernet) необходима устойчивая фиксация коллизии всеми станциями сети.

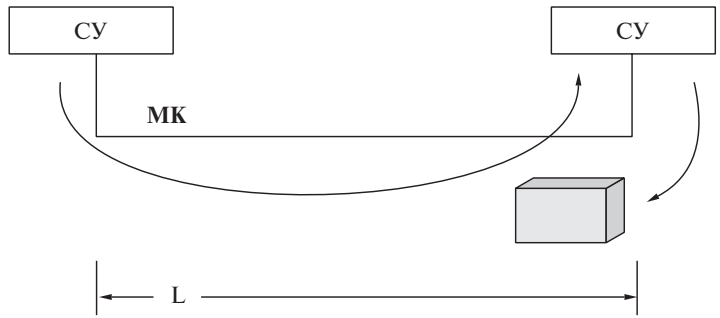


Рис. 3.3. Ненастойчивый СУ

Каждый узел после обнаружения коллизии продолжает передавать специальную последовательность бит (010101...) длиной порядка 30 бит для более четкой фиксации коллизии.

Сравнение случайных методов доступа приведено на рис. 3.4.

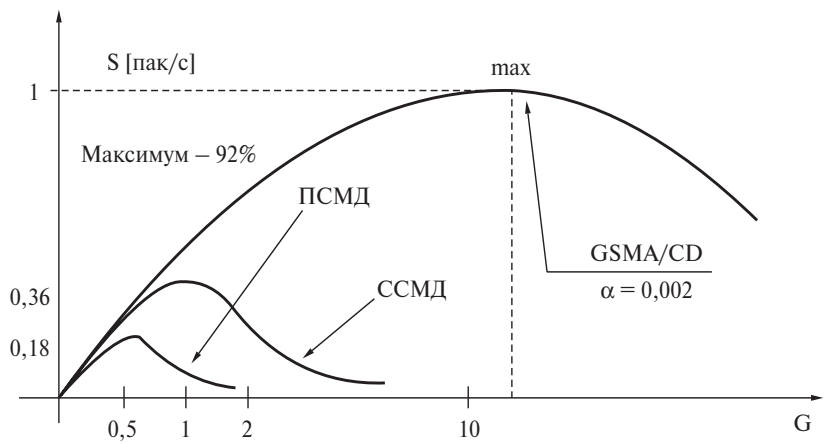


Рис. 3.4. Сравнение методов доступа

При работе сети каждая станция анализирует адресную часть передаваемых по сети кадров с целью обнаружения и приема кадров, предназначенных для нее.

На рис. 3.5 представлены алгоритмы приема и передачи данных в одном из узлов при МДКН/ОК.

3.2.4. Случайный метод доступа CSMA/CA (Collision Avoidance) с устранением коллизий

Здесь на 100% исключается столкновение информационных пакетов за счет того, что СУ, которому необходима порция информации, предварительно посылает в МК специальный электрический сигнал. Если этот сигнал не сталкивается с другими, то все станции его фиксируют, они «уведомлены» о начале передачи и пославшему узлу предоставляется определенное время на передачу. Подобным методом коллизия обнаруживается легче и дешевле, так как аппаратно для этого достаточно лишь амплитудного компаратора.

При обнаружении коллизии работает механизм случайного тайм-аута.

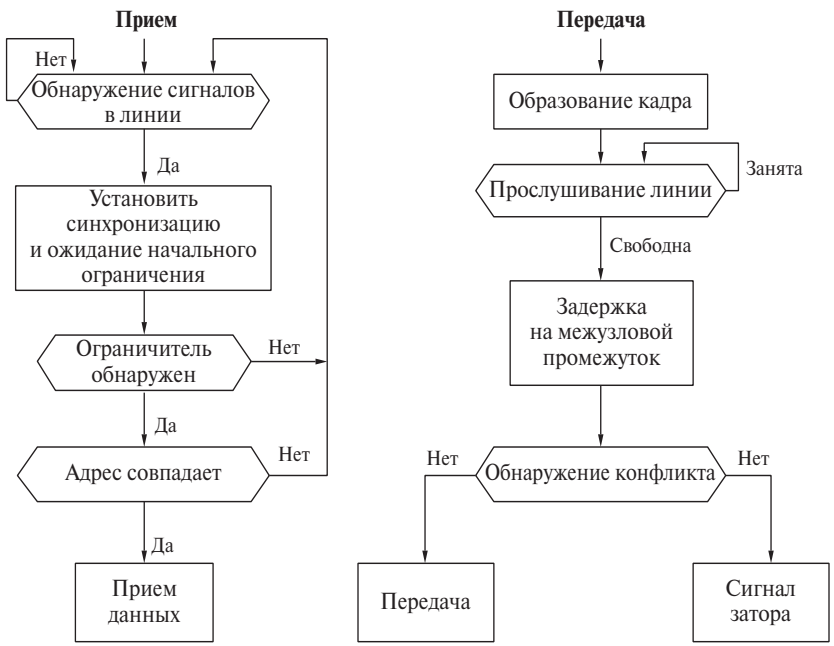


Рис. 3.5. Алгоритмы приема и передачи данных

Схемы алгоритма CSMA/CD для настойчивой с вероятностью P станции представлены на рис. 3.6.

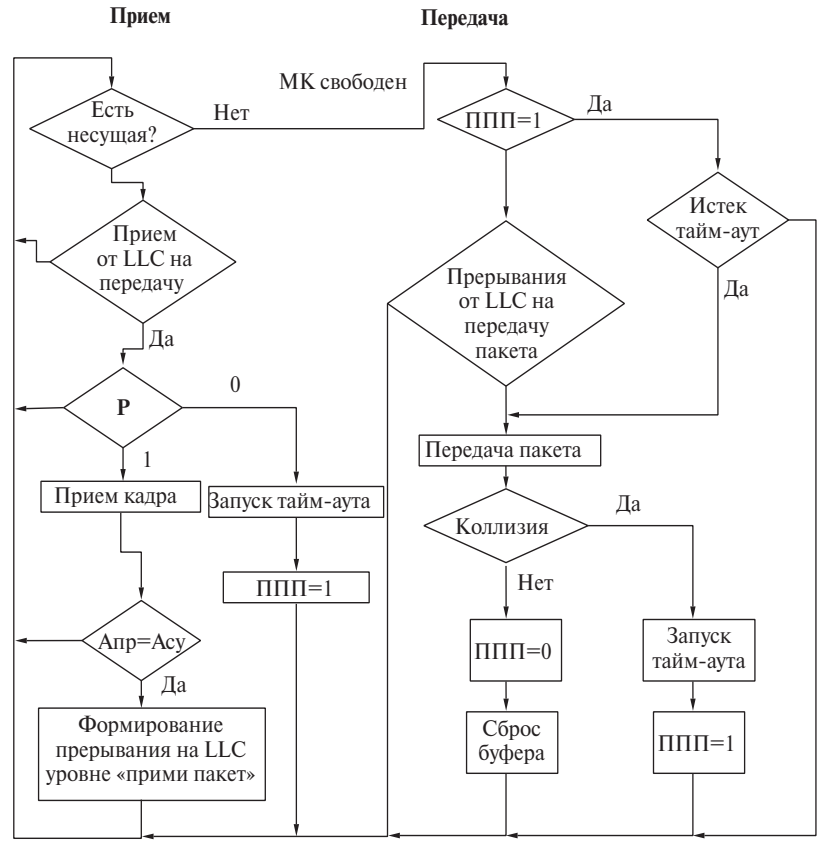


Рис. 3.6. Алгоритмы доступа по методу МДКН/ОК

Все устройства сетевого адаптера работают параллельно. Прием ведется всегда, независимо от передачи, поэтому схема алгоритма частично упрощена (на ней не отражено разделение процессов во времени).

3.2.5. Устранение самоблокировки в ЛВС со случайным методом доступа

Основная идея ликвидации самоблокировки сети — увеличение среднего значения случайной величины тайм-аута. Алгоритм работы сетевых узлов: если данному СУ несколько раз не удается передать пакет, то он увеличивает среднее значение τ в 2 раза, т.е. среднее

время ожидания повторной попытки передачи удваивается. Если после такого увеличения не удается передать пакет, то τ увеличивается еще в 2 раза и т.д. Обычно есть какое-либо τ-ном и если коллизий нет (СУ несколько раз успешно передает пакет с первой попытки), то он уменьшает τ в 2 раза и т.д. до τ минимально допустимого. Вид зависимости S = f(G) для механизма подбора среднего значения тайм-аута представлен на рис. 3.7.

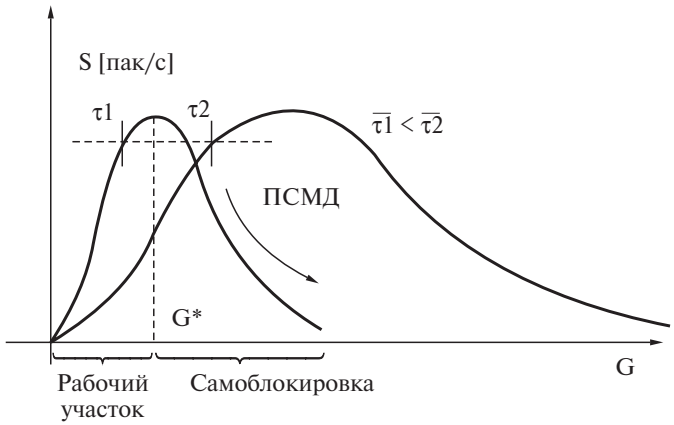


Рис. 3.7. Зависимость S = f(G) для механизма подбора среднего значения тайм-аута

3.3. Детерминированные методы доступа в ЛВС

Среди детерминированных методов доступа наибольшей популярностью пользуются следующие:

1) метод последовательного опроса (Polling);
2) метод запроса;
3) маркерный метод доступа (Token);
4) метод кольцевых слотов (метод зазора);
5) метод вставки регистров.

3.3.1. Метод последовательного опроса

Метод последовательного опроса предполагает наличие главного (Host) компьютера, на который возлагается задача опроса других сетевых устройств.

Host-компьютер последовательно опрашивает каждый сетевой узел на предмет наличия у него информации, готовой к передаче. Каждый сетевой узел отвечает специальной посылкой, в которой

содержится информация: «есть» или «нет». Если у сетевого узла имеется информация, готовая к передаче, то возможны два варианта:

1) для топологии типа «звезда»: Host просто принимает информацию, которую сетевой узел-источник желает передать и передает ее сетевому узлу-приемнику, которому эта информация предназначалась;

2) для топологии типа «шина»: Host выделяет определенное время сетевому узлу-источнику на использование моноканала.

Метод последовательного опроса имеет существенное преимущество в «звездообразной» топологии — характеризуется повышенной степенью защищенности передаваемой информации.

Недостатки метода — при малой загруженности моноканала возможность для передачи информации будет предоставляться не часто.

3.3.2. Метод запроса

Метод запроса можно считать разновидностью метода последовательного опроса. Разница заключается только в том, где физически реализуется расписание опросов.

В методе последовательного опроса (Polling) запрос реализуется по всей ЛВС.

В методе запроса запрос опросов реализуется внутри Host, т.е. периферийные сетевые узлы заранее в Host посылают запросы, где организуется определенная очередь, и Host в определенном порядке опрашивает очередь, предоставляя сетевым узлам интервалы времени на передачу информации.

Достоинство метода — повышенная степень защищенности передаваемой информации.

3.3.3. Маркерный метод доступа

Маркерные методы доступа преобладают среди детерминированных методов.

Маркерные методы доступа характеризуются тем, что право использования среды передачи от узла к узлу передается с помощью уникального кадра, называемого маркером, с использованием адресов узлов.

Маркерный метод — метод доступа к среде передачи данных в ЛВС, основанный на передаче полномочий передающей станции с помощью специального информационного объекта, называемого маркером.

Маркер — это специальный служебный пакет, получение которого сетевым узлом означает получение права на передачу пакета данных (если таковой имеется).

Под полномочием понимается право инициировать определенные действия, динамически предоставляемые объекту, например станции данных в информационной сети.

Применяется ряд разновидностей маркерных методов доступа.

Различают маркерный метод доступа в сети с топологией шина — Token Bus и в сети с кольцевой топологией — Token Ring.

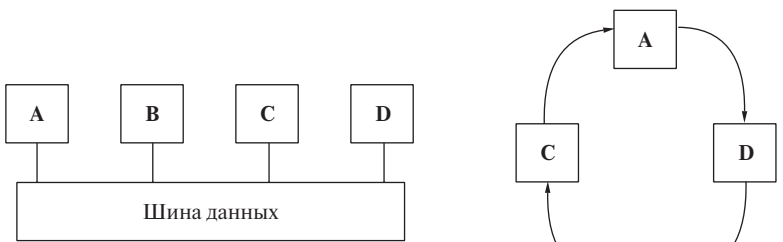
В эстафетном методе передача маркера выполняется в порядке очередности.

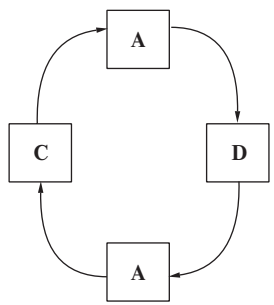
В способе селекторного опроса (квантированной передачи) сервер опрашивает станции и передает полномочия одной из тех станций, которая готова к передаче.

В кольцевых одноранговых сетях широко применяется тактируемый маркерный доступ, при котором маркер циркулирует по кольцу и используется станциями для передачи своих данных.

Оригинальный метод, рассматриваемый далее, применен в высокоскоростных сетях FDDI.

Передача данных по сети осуществляется в соответствии с логическим кольцом расписаний (ЛКР) (рис. 3.8).





Логическое кольцо расписаний (ЛКР)

Рис. 3.8. Схема передачи данных по кольцу

В соответствии с логическим кольцом расписания (ЛКР) между сетевыми узлами передается маркер.

Во время нормальной работы узлы находятся большую часть времени в состоянии прослушивания сети. Получив маркер, сетевой узел анализирует его, и при отсутствии данных сетевой узел обеспечивает продвижение маркера к следующему сетевому узлу в соответствии с логическим кольцом расписаний. Если у сетевого узла есть информация для передачи, то он задерживает у себя маркер и передает данные, после этого передает маркер вслед за данными. Завершив передачу данных и маркера, сетевой узел переходит в состояние прослушивания. Если полученный кадр является информационным, то узел переходит в состояние приема кадра, затем возвращается в состояние прослушивания.

Описанный алгоритм работы называют ранним освобождением памяти.

При реализации данного метода доступа существуют две принципиальные ситуации, которые связаны:

1) с необходимостью подключения новых станций к ЛКР,

2) с необходимостью регенерировать маркер при аварийном отключении некоторых станций (у которых был маркер).

Для того чтобы упростить протокол и реализацию маркерного метода доступа, подключение новой станции сводят к аварийному выключению станции, которое, в свою очередь, связано с потерей маркера. Новый сетевой узел, который должен войти в ЛКР, во время передачи маркера посылает по шине специальный пакет, искажающий этот маркер (происходит коллизия маркера и пакета от той станции, которая должна войти в ЛКР). Факт потери маркера фиксируется с помощью следующих средств.

Сетевой узел, пославший маркер другому сетевому узлу, в течение определенного фиксированного интервала времени следит за появлением маркера от следующей станции. Если в течение этого интервала времени маркер в шине не обнаружен, то данный узел, который зафиксировал этот факт, переводит сеть в состояние смены ЛКР. Этот сетевой узел становится активным монитором. Для этого он посылает специальный служебный пакет (широковещательный) и начинает в порядке возрастания или убывания адресов опрашивать все сетевые узлы с адресами от 1 до A_{max} и по каждому адресу посылается запрос. Если по этому адресу есть станция, то либо придет ответ, либо по истечении TimeOut — не придет. Эти ответы фиксируют все станции, которые находятся в активном состоянии в сети, и по результатам этих ответов составляется новое ЛКР. После этого станция активного монитора запускает маркер.

Особенности маркерного метода в сети с кольцевой топологией

Основное отличие данного метода от предыдущего заключается в топологии среды передачи данных. В топологии «шина» сигналы, передаваемые сетевым узлом, распространяются по всей

среде в обе стороны; в топологии «кольцо» сигналы распространяются через однонаправленные пути в одном направлении. При этом сигналы в каждом узле передаются внутри самого узла от приемного входа к передающему. Во время этой передачи сигналы могут модифицироваться и анализироваться сетевым узлом, например, усиливаться.

По кольцу в одном направлении постоянно циркулирует маркер — короткий служебный пакет (рис. 3.9).

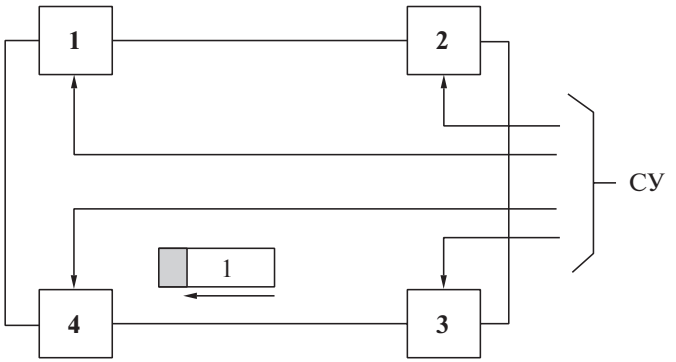


Рис. 3.9. Передвижение маркера

Узел, получивший этот маркер и не имеющий готовой информации для передачи, ретранслирует его дальше по кольцу.

Узел, имеющий информацию для передачи, добавляет к этому маркеру, как к «паровозу», свои информационные «вагоны» (данные, которые необходимо передать). При этом в маркере устанавливается бит занятости. Далее этот «состав» (кадр с маркером и данными) продвигается по кольцу до узла, который опознает свой адрес.

Тогда узел-приемник копирует данные в свой буфер, устанавливая в кадре признак получения данных. Далее маркер с данными передается другим узлам до узла-отправителя.

Получив маркер, узел-источник сбрасывает флажки занятости и приема в маркере.

Один и тот же узел не может передавать данные два раза подряд, т.е. после получения маркера с информацией о том, что данные переданы успешно, он не может передавать новую порцию данных. Вместо этого он сбрасывает флажки занятости и приема, удаляет пакет данных из кадра и передает свободный маркер дальше другому (соседнему) сетевому узлу (рис. 3.10).

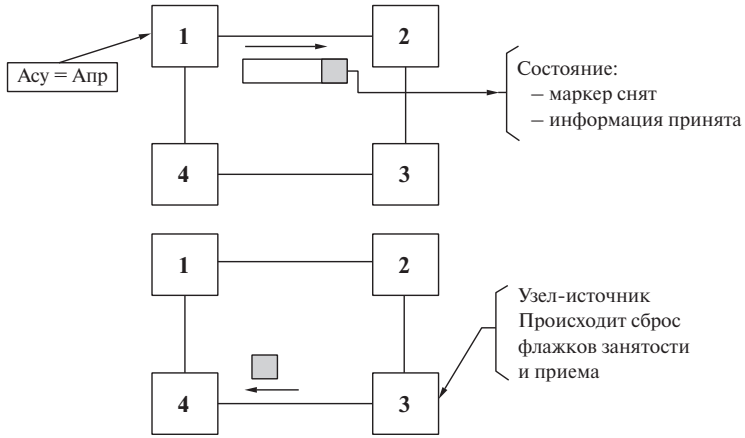


Рис. 3.10. Схема движения маркера

С помощью данного метода доступа реализуется одновременно и механизм квитирования, так как узел-источник получает подтверждение о приеме посылаемых им данных.

Для увеличения надежности функционирования маркерного кольца в данном методе доступа используется не совсем «чисто» децентрализованный метод. Один из сетевых узлов играет здесь особую роль — временного активного монитора кольца. Это сделано для защиты от возможных случайных потерь маркера. Для этого в формат маркера вводится специальный бит (бит мониторинга) и в функции сетевого узла у монитора вводится обязанность устанавливать этот бит в 1. Любой другой сетевой узел обязан сбросить этот бит в 0. Поэтому получение монитором маркера с установленным битом монитора означает, что в сети какие-то проблемы.

Функции узла монитора:

1) регенерация маркера в случае его потери;
2) формирование ЛКР.

Необходимо отметить, что монитором может быть любой узел сети.

Есть специальный механизм передачи прав монитора (например, станции, имеющей минимальный адрес). С этой точки зрения все сетевые узлы равноправны.

Приоритетный доступ к кольцу

Любой кадр данных или маркер имеет приоритет, устанавливаемый видами приоритета от 0 до 7.

Сетевой узел может воспользоваться монитором, если у него есть кадр для передачи с приоритетом не ниже, чем приоритет маркера.

Сетевой узел с кадром, у которого приоритет ниже, чем приоритет маркера, не может захватить маркер, но может поместить наибольший приоритет своих ожидающих передачи кадров в резервные виды маркера, но только в том случае, если записанный в этих видах приоритет не ниже его собственного. В результате в резервном бите устанавливается наивысший приоритет сетевого узла, который пытается получить доступ к кольцу, но не может сделать этого из-за более высокого приоритета маркера.

Сетевой узел, захвативший маркер, передает свои кадры, а затем передает маркер соседу. При этом он переписывает значение поля резервного приоритета в поле приоритета маркера, а резервное поле обнуляется.

При инициализации кольца резервные и основные приоритеты маркера равны нулю.

Хотя механизм приоритета в технологии Token Ring имеется, он начинает работать только в том случае, когда либо приложение, либо прикладной протокол решает его использовать.

Это связано с тем, что приоритеты кадра поддерживаются не во всех технологиях. В современных сетях это решается с помощью коммутаторов и маршрутизаторов.

3.3.4. Метод зазора (кольцевых слотов)

Этот метод по своей идеологии близок к маркерному методу для ЛВС с кольцевой топологией. Основное отличие от маркерного метода доступа в том, что все кольцо рассматривается как единый циклический сдвиговый регистр.

Разряды этого регистра сдвига составляются как из внутренних задержек самих СУ, так и задержек передачи двоичной информации через линии связи (линии задержки).

Вследствие небольших задержек распространения сигнала в линиях связи и небольшой разрядности сдвиговых регистров внутри СУ, общая разрядность всего кольца, как регистра сдвига, выбирается небольшой (NR = 30—50 бит) (рис. 3.11).

В моноканале в каждый момент времени циркулирует целое число двоичных сигналов, представляющих собой мини-пакеты с промежутками и зазорами.

Зазором называется кадр, который непрерывно циркулирует по кольцу как по сдвиговому регистру. Сетевые узлы должны на ходу

вставлять в этот зазор передаваемую и снимать считываемую информацию.

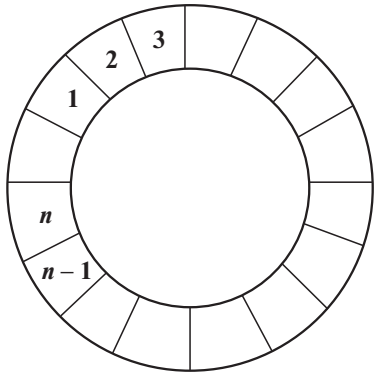


Рис. 3.11. Кольцевой слот

В зазоре имеется два служебных бита:

1) бит занятости — используется для определения состояния зазора;

2) бит приема — используется для определения состояния приема информации СУ приемником.

СУ у которого есть информация, готовая для передачи, при прохождении через него зазора контролирует бит занятости; и если он сброшен (зазор свободен), то этот СУ записывает туда информацию для передачи и заполняет поля *Адрес приемника* и *Адрес источника*.

Зазор, далее продвигаясь по кольцу, доходит до СУ приемника, который, распознав свой адрес, снимает данные и устанавливает бит приема в 1.

Зазор, двигаясь дальше, делает полный круг и доходит до СУ источника, который анализирует бит приема (получает положительную или отрицательную квитанцию).

СУ источника обязан сбросить бит занятости и отправить свободный зазор по кольцу (не имеет права дважды занимать один и тот же зазор подряд несколько раз).

Если кольцо короткое (помещается десяток бит), то в нем циркулирует только один зазор.

Если длина кольца превышает некоторый порог, то в нем генерируется еще один зазор и т.д. (главное, чтобы голова одного зазора не наступала на хвост другого или на свой собственный).

В случае отсутствия за определенное тайм-аутом время начала зазора СУ, обнаруживший это, становится монитором. Этот СУ генерирует новые зазоры и запускает их в кольцо ЛВС. При этом сам он не имеет права первоначально захватывать зазоры.

Достоинства:

- относительно высокая скорость;
- высокая эффективность (при увеличении СУ генерируются дополнительные зазоры);
- гарантированная доставка информации адресату (вероятность доставки, квитирование доставки);
- надежность работы сети гарантируется режимом монитора работы одного из СУ (любого).

Недостатки:

- при увеличении числа СУ в ЛВС могут возрасти задержки в доставке информации;
- сложное масштабирование в ЛВС.

3.3.5. Метод вставки регистра

В отличие от маркерного метода и метода зазора здесь разрядность кольца, как сдвигового регистра, все время меняется. Это сделано за счет вставки в сетевой адаптер специального регистра сдвига (рис. 3.12).

СА имеет сдвоенный переключатель с двумя положениями:

- исходное положение (транзитная передача информации);
- передача собственных данных.

В нормальном состоянии регистр практически отключен от кольца. Переключатель находится в положении A. В этом состоянии СУ анализирует и считывает информацию, поступающую на вход.

Когда нет передающих СУ, разрядность почти равна нулю (имеется служебная информация — несколько бит).

Если информация предназначена для данного СУ, то переключатель IN переходит в положение *b* и информация поступает в регистр сдвига, а из него в СУ. Помимо этого, уже считанная информация передается в сеть.

СУ, которому надо передать информацию, загружает ее предварительно в сдвиговый регистр и добавляет его в кольцо, тем самым увеличивая разрядность кольца (это могут делать все СУ одновременно).

Если СУ есть, что передавать, то по сигналу Y1 информация загружается в регистр сдвига. После чего контролируется занятость

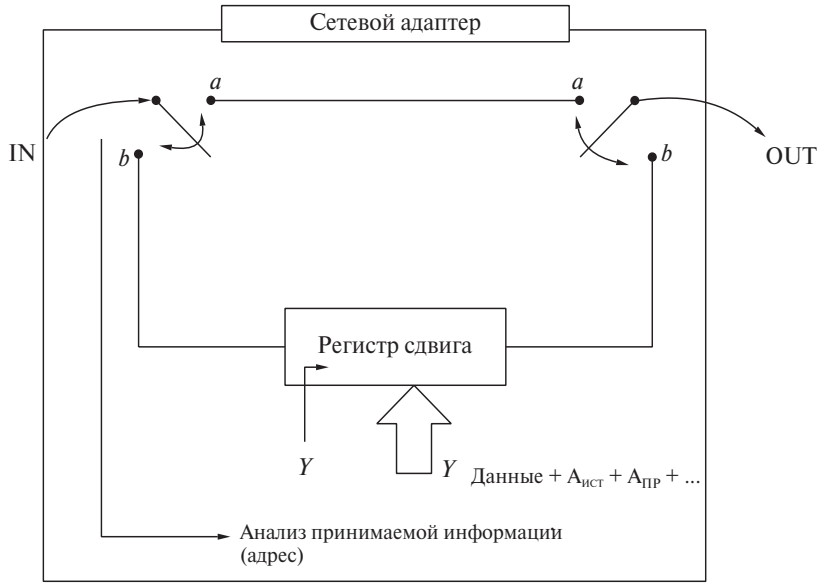


Рис. 3.12. Схема сетевого адаптера

линии связи IN, если занята — переключатель в положение «a», как только IN свободен — переключатель в положение «b», после чего подается управляющий сигнал Y2 для передачи кадра в кольцо по линии OUT. Если в это время на входе IN появится кадр от другого СУ, он не теряется, а попадает в освобождающиеся разряды регистра сдвига и после выдвижения своего собственного кадра через выход OUT будет ретранслирован дальше по кольцу.

Среди всех детерминированных методов доступа самым эффективным по коэффициенту использования пропускной способности моноканала является метод вставки регистра (здесь отсутствуют холостые пробеги маркера — разрядность кольца автоматически подстраивается под число передаваемой информации).

Недостаток метода: если выключение СУ произойдет в момент передачи чужой информации, то она теряется.

3.3.6. Сравнение детерминированных методов доступа

В детерминированных методах доступа самоблокировка отсутствует, так как общий ресурс (моноканал) равномерно распределяется среди всех активных станций.

В детерминированных методах доступа можно гарантировать заранее определенное, фиксированное время доставки (не более определенного промежутка времени), чего нельзя гарантировать для случайного метода доступа. Это может быть очень важным обстоятельством в системах управления производством, технологическим процессом.

При малом числе активных станций случайный метод более эффективен, чем большинство детерминированных методов доступа (кроме метода вставки регистра). Если на передачу работает только одна станция, то только она одна и занимает весь моноканал. Отобразим последнее сравнение качественно в виде графика (рис. 3.13).

Случайные методы доступа при N < M более эффективны, чем детерминированные методы, так как тратится время на организацию маркера или опроса.

При большой загруженности сети (N > M) случайный метод доступа более медленно и менее эффективно перестраивается к растущей нагрузке, вследствие чего резко возрастает среднее время передачи одного пакета.

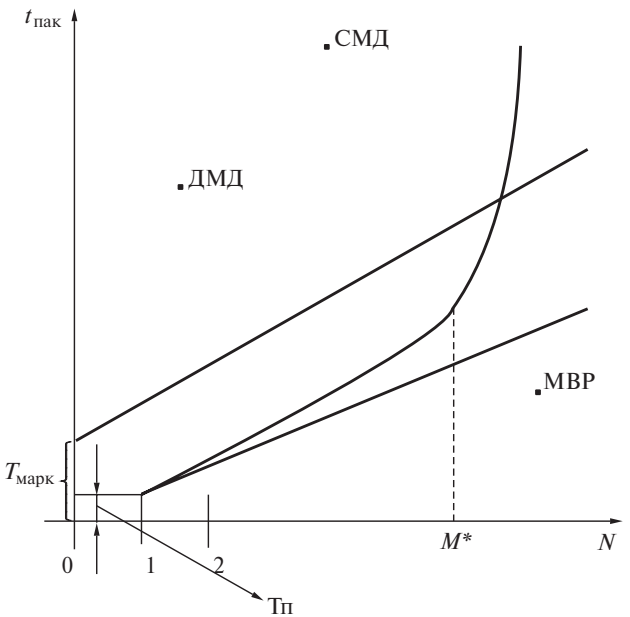


Рис. 3.13. График детерминированных методов

3.4. Контрольные вопросы

1. В чем отличие метода доступа CSMA/CAот CSMA/CD?
2. В чем суть маркерного метода доступа?
3. Что представляет собой маркер?
4. Какие способы передачи маркера используются в ЛВС?
5. В чем суть метода раннего освобождения маркера и в каких ЛВС он применяется?
6. Какой метод доступа используется в сетях Ethernet?
7. Что такое ЛКР?
8. Что такое сигнал затора и где он применяется?

Раздел 4
БАЗОВОЕ СЕТЕВОЕ ОБОРУДОВАНИЕ

4.1. Сетевое оборудование и модель OSI

Репитеры (повторители, концентраторы, хабы) предназначены для электрического усиления и размножения электрического сигнала, не имеют памяти и алгоритмических функций. Поддерживают физический уровень управления сетью (1-й уровень в модели ОС) (рис. 4.1).

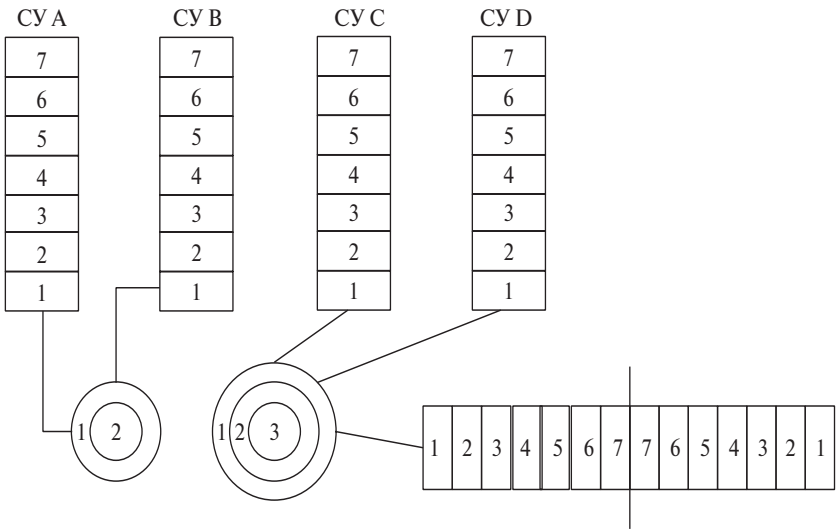


Рис. 4.1. Схема подключения СУ

Мосты предназначены для соединения различных сетевых сегментов, в которых используются различные сетевые технологии. Мост распознает MAC-адрес СУ, и если им получен пакет с MAC-адресом другой сети, то только в этом случае он ретранслирует пакет. Мост не распространяет пакеты по всем направлениям. Мост реализует два нижних уровня управления сетью. От наличия некоторых элементов маршрутизации встречаются устройства, которые называются Bridge-Router, Router-Bridge, — это еще не маршрутизаторы.

Маршрутизаторы (Router) имеют память, в которой хранится полная таблица маршрутизации всех СУ, известных данному маршрутизатору. Данное устройство реализует соответствующий метод маршрутизации, который обеспечивает наиболее оптимальный метод доставки пакета.

Шлюзы предназначены для объединения СПД, использующих разную архитектуру. Взаимодействие между сетями осуществляется на уровне сообщений, поэтому шлюз реализует пять нижних уровней управления сетью (все уровни управления сетью реализуют только СУ, выполняющие функции серверов и рабочих станций).

Коммутатор (Switch) соединяет сегменты с одной и той же технологией, но, возможно, работающих на разных скоростях или соединяющих разную среду передачи, в отличие от моста коммутатор способен обеспечить $n/2$ соединений, где n — число портов.

Соответствие функций различных устройств сети различным уровням модели OSI представлено в табл. 4.1.

Таблица 4.1

<table>
<tr><th>Уровни модели OSI</th><th colspan="8">Сетевой сервер, рабочая станция, ШЛЮЗ</th><th>Уровни модели OSI</th></tr>
<tr><td>Прикладной</td><td>7</td><td colspan="6" rowspan="4"></td><td>7</td><td>Прикладной</td></tr>
<tr><td>Представительский</td><td>6</td><td>6</td><td>Представительский</td></tr>
<tr><td>Сеансовый</td><td>5</td><td>5</td><td>Сеансовый</td></tr>
<tr><td>Транспортный</td><td>4</td><td>4</td><td>Транспортный</td></tr>
<tr><td>Сетевой</td><td>3</td><td colspan="4">МАРШРУТИЗАТОР</td><td>3</td><td>Сетевой</td></tr>
<tr><td>Канальный</td><td>3</td><td>2</td><td colspan="3">МОСТ/КОММУТАТОР, сетевой адаптер</td><td>2</td><td>3</td><td>Канальный</td></tr>
<tr><td>Физический</td><td>3</td><td>2</td><td>1</td><td colspan="3">Физический</td><td>1</td><td>2</td><td>3</td><td></td></tr>
<tr><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3"></td><td colspan="5"></td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td colspan="5">Логические сегменты</td></tr>
<tr><td colspan="6">Сети/Подсети</td></tr>
<tr><td></td><td colspan="8">Интерсети</td><td></td></tr>
</table>

4.2. Контрольные вопросы

1. Назначение повторителей и концентраторов.
2. Что такое репитер и хаб?
3. Нарисовать структуру ЛВС с повторителем.
4. Достоинства и недостатки использования повторителей и концентраторов для увеличения размеров ЛВС.
5. На каком уровне OSI-модели работают повторители и концентраторы?
6. Что такое сетевой шлюз?

Раздел 5
РЕАЛИЗАЦИЯ РАЗЛИЧНЫХ ТЕХНОЛОГИЙ КАНАЛЬНОГО УРОВНЯ

5.1. Сеть PolyNet (Cambridge Ring)

Эта сеть имеет топологию — кольцо (Ring).

Тактовая частота передачи информации в кольце — 10 МГц (10 Мб/с). Протяженность сети — 300–400 м, возможно использование репитеров для удлинения кольца.

В качестве среды передачи информации используется коаксиальный кабель с задержкой в распространении сигнала 4 нс/м.

Подключение к кольцу осуществляется с помощью розетки и вилки. При вынутой вилке кольцо замыкается через эту розетку. Кольцо питается от специального дополнительного источника, который подключается к сети с помощью дополнительной пары проводов и обеспечивает работу всех приемников и передатчиков сети.

В этой сети в качестве метода доступа к МК используется метод зазора (кольцевых слотов). Данный метод соответствует стандарту ISO/DIS 8802/7.

Стандарт ISO/DIS 8802/7 допускает генерацию в кольце от 1 до 255 зазоров, в зависимости от длины зазора. Реально используемое число зазоров — 2–3 зазора (табл. 5.1).

Таблица 5.1

42, 58, 74, 82 бит									
19 бит					16, 32, 48, 56	7 бит			
1 бит	1 бит	1 бит	8 бит	8 бит		2 бита	2 бита	1 бит	2 бита
Маркер начала	Флаг занятости	Бит мониторинга	Адрес приемника	Адрес источника	Данные	Тип кадра	Биты приема	Бит нечетности	Биты заполнения

В зазоре имеется два служебных бита: занятости и приема.

Вследствие небольших задержек распространения сигнала в линиях связи и небольшой разрядности сдвиговых регистров внутри

СУ общая разрядность всего кольца как регистра сдвига выбирается небольшой.

Длина одного зазора для сети PolyNet (Cambridge Ring) L ∈ {42, 58, 74, 82 бит}.

Флаг занятости — зазор занят — 1, зазор свободен — 0. Бит монитора используется для повышения надежности функционирования сети путем осуществления возможности захвата полномочий активным СУ (СУ-монитор) для решения конфликтов (формирования зазоров).

Адреса СУ 8-битные, что позволяет адресовать до 28 = 256 СУ, принадлежащих к единой кабельной системе.

Тип кадра определяет возможные четыре градации длины поля данных:

- 00 — 16 бит;
- 01 — 32 бит;
- 10 — 48 бит;
- 11 — 56 бит.

Биты приема используются для определения состояния приема информации СУ приемником: 00 — сетевой узел не может принять пакет (например, в сетевом адаптере не хватает памяти); 01 — пакет принят; 10 — станция пакет видела, но не приняла данные (в случае несовпадения CRC или невозможности опознать адрес источника); 11 — станция отключена от сети. 2 бита заполнения добавляются в конце для четкого разграничения конца одного пакета от начала другого.

Достоинства:

- относительно высокая скорость (10 Мбит/с);
- высокая эффективность (при увеличении СУ генерируются дополнительные зазоры);
- гарантированная доставка информации адресату (вероятность доставки, квитирование доставки);
- надежность работы сети гарантируется режимом монитора работы одного из СУ (любого).

Недостатки:

- при увеличении числа СУ в ЛВС могут возрасти задержки в доставке информации;
- сложное масштабирование ЛВС.

5.2. Технология ArcNet

Технология ArcNet (Attached Resource Computer Net) разработана в 1977 г. фирмой Data Point Corporation. Точного стандарта на нее нет, но близкий стандарт маркерного метода — IEEE 802.4 (Token Bus).

Использует детерминированный маркерный метод доступа (Token Bus) для шины с эстафетной передачей полномочий.

Скорость передачи $V = f_T = 2{,}5$ Мбит/с — единственный недостаток технологии, все остальные параметры лучше, чем у других технологий.

Пакеты могут включать до 516 байт.

Максимальное число узлов 254. Все станции сети принадлежат к единой кабельной системе, где максимальное общее число станций $НСУ_{max} = 254$ (так как разрядность адреса — 8 бит, адрес «00000000» не используется, адрес «00000001» служит для широковещательной рассылки).

В отличие от сетевых адаптеров Ethernet, где сетевой адрес разрядности 48 бит уникален и зашит внутри него (248 комбинаций адреса гарантирует при выпуске отсутствие повторений), в ArcNet адрес выставляется с помощью восьми переключателей. В одной кабельной системе все адреса должны быть разными, иначе ситуация с одинаковыми адресами обнаруживается и выдается предупредительный сигнал. Однако есть и СА Ethernet с изменяемым адресом.

Сеть может иметь расстояние между узлами до 70 м и может содержать до восьми узлов без дополнительных коммуникационных средств (рис. 5.1).

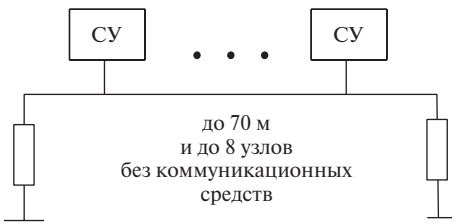


Рис. 5.1. Схема подключения по технологии ArcNet

Пример простейшей односегментной сети

Коммутационные сетевые средства — концентраторы (хабы) двух типов:

- PH (Passive Hub) — без усилителя выполняется на 4 разъема (рис. 5.2);
- AH (Active Hub) — с усилителями по каждому порту на 4, 8, 16, 32 разъема.

Посредством PH создаются простейшие дешевые конфигурации сети.

Для увеличения длины сети используют AH, что позволяет удлинять каждый луч коаксиального кабеля до 600 м (витой пары — до 300 м).

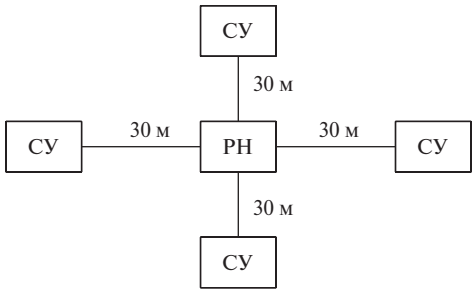


Рис. 5.2. Схема подключения по технологии РН

Максимальное число последовательно включенных АН может быть 9, отсюда предельная длина (9 + 1) × 600 = 6 км. Максимальная удаленность между двумя станциями — L = 6 км.

Применяются две среды передачи:

- коаксиальный кабель RG62 с Rв = 93 Ом или отечественный аналог РК100 Rв = 100 Ом, РК75 Rв = 75 Ом;
- витая пара (для ТР все длины уменьшаются в два раза; L = 3 км). Технология непритязательна к виду кабеля, так что можно использовать 75-омные кабельные линии, но тогда терминатор R = 75 Ом приходится делать самим и гарантированная длина уменьшается до 4 км (рис. 5.3).

В сетях ArcNet нельзя заземлять кабельную систему (соединять землю терминатора с корпусом компьютера) при использовании коаксиальных кабелей.

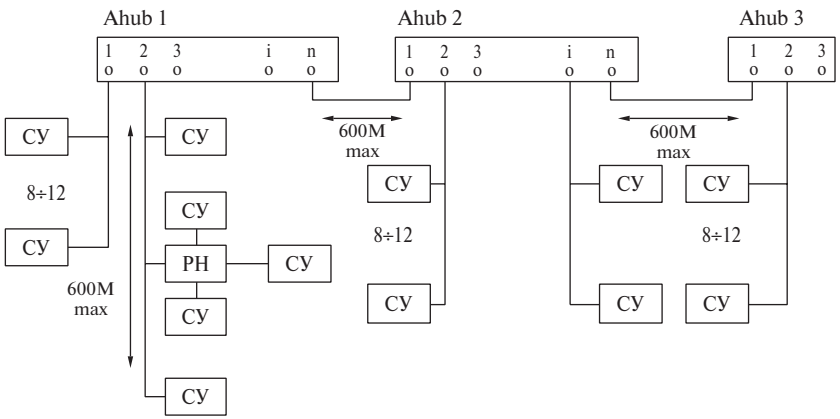


Рис. 5.3. Схема подключения по технологии АН

Внутри АН уже стоят терминаторы, а на каждом конце луча их подсоединяют при компоновке сети. Так как практически все СА ArcNet выпускаются со встроенным внутри резистором-терминатором и переключателем, то внешний терминатор можно не использовать, т.е. на всех «средних» узлах они должны быть отключены, а на последнем — включены, либо на всех отключены, а на конце кабеля — включены.

Форматы кадров в ArcNet

В сетях ArcNet минимальная информационная единица — не байт, а так называемый Information Symbol Unit (ISU) разрядностью 11 бит.

Три первых бита играют роль старт-стоповых битов для синхронизации. В кадрах лишь поле АВ, играющее роль начального разделителя, имеет длину 6 бит, все остальные поля кратны ISU. При реализации маркерного метода доступа в сетях ArcNet используются кадры пяти различных форматов.

IIT выполняет роль маркера. Получение такого пакета означает приобретение права на передачу.

1) FBE — запрос готовности к приему данных.
2) DATA — кадр данных.
3) ACK (Asked Knowlege) — квитанция, в адресации не нуждается.
4) NAK — негативная квитанция.

СУ, получивший маркер (кадр IIT) и имеющий информацию, готовую к передаче (если не имеет — передает его дальше согласно ЛКР), посылает кадр запроса готовности к приему FBE СУ-приемнику, которому он хочет передать информацию и ожидает от него в течение тайм-аута t = 75,6 мкс квитанции (подтверждения о готовности принять данные). В ответ может прийти ACK, NAK или ничего. При неудаче СУ делает повторный запрос и при двух отрицательных запросах СУ передает маркер следующей станции. Если же получена положительная квитанция, СУ-передатчик посылает кадр DATA СУ-приемнику. После приема данных приемник отсылает квитанцию ACK об удачном или NAK о несостоявшемся приеме. При любом исходе СУ посылает маркер другому СУ, следующему по ЛКР.

В ситуации реконфигурирования сети происходит потеря маркера. СУ, который последним послал маркер, прослушивает шину, чтобы отследить маркер (840 мкс), и если его нет, то этот СУ посылает специальный служебный кадр, который извещает всю сеть о переходе в режим реконфигурации и при его получении все СУ вклю-

чают у себя тайм-аут, время которого вычисляется по формуле tTA = 146×(258-ID) [мкс]. ID — адрес данной станции. Тайм-аут раньше кончится у СУ с максимальным сетевым адресом и далее по порядку. Именно этот СУ и будет производить опрос наличия всех СУ с адресами 1-IDmax, и на каждый запрос станция отвечает положительной квитанцией, если такой адрес существует. По результатам ответа все СУ составляют новое ЛКР, и сеть переходит в обычный режим работы. Станция, осуществившая реконфигурацию, первой посылает маркер, т.е. запускает логическое кольцо расписания.

Достоинства и недостатки технологии ArcNet

Оба варианта аппаратуры дешевле своих аналогов в технологии Ethernet.

Несмотря на надежность и удобство инсталляции и эксплуатации, сеть применяется все реже из-за малого размера адреса (недостаточной для современных систем распределенных вычислений) и сравнительно невысокой скорости (2,5 Мбит/с), передача полномочий происходит только после того, как закончена передача пакета по установленному соединению, для чего необходимо наличие факта установленного соединения.

В начале 1990-х гг. эти сети занимали 30% рынка ЛВС в мире, и долгое время технология не совершенствовалась. Для повышения быстродействия разработана модификация ArcNet Plus. При большой нагрузке каналов связи информация проходит намного быстрее, чем в Ethernet 100, и время доставки гарантировано. В технологии ArcNet Plus скорость передачи данных и пропускная способность хабов 25 Мбит/с.

Популярность технологии продолжает падать, так как на отечественный рынок не поставляется технология ArcNet Plus, а простой ArcNet резко проигрывает в стоимости. Однако есть области узкоспециализированного применения, где сетевая технология является единственно разрешенной (для некоторых объектов, работающих в реальном масштабе времени, где недопустимы непредвиденные задержки передачи данных).

Отечественный улучшенный аналог технологии — Viola Net, Tomsk Net.

5.3. Стандарт IEEE 802.5 Token Ring

Из кольцевых ЛВС наиболее распространены сети с передачей маркера по кольцу и среди них:

1) ЛВС типа Token Ring (сеть с таким названием была разработана фирмой IBM и послужила основой для стандарта IEEE 802.5);

2) сети FDDI (Fiber Distributed Data Interface) на основе ВОЛС.

Сеть Token Ring первоначально была разработана компанией IBM в 1970 г. Она по-прежнему является основной технологией IBM для локальных сетей (LAN) , уступая по популярности среди технологий LAN только Ethernet/IEEE 802.3. Спецификация IEEE 802.5 почти идентична и полностью совместима с сетью Token Ring IBM. Спецификация IEEE 802.5 была фактически создана по образцу Token Ring IBM, и она продолжает отслеживать ее разработку. Термин «Token Ring» обычно применяется как при ссылке на сеть Token Ring IBM, так и на сеть IEEE 802.5.

Сети Token Ring и IEEE 802.5 в основном почти совместимы, хотя их спецификации имеют относительно небольшие различия. Сеть Token Ring IBM оговаривает звездообразное соединение, причем все конечные устройства подключаются к устройству, называемому «устройством доступа к многостанционной сети» (MSAU), в то время как IEEE 802.5 не оговаривает топологию сети (хотя виртуально все реализации IEEE 802.5 также базируются на звездообразной сети). Имеются и другие отличия, в том числе тип носителя (IEEE 802.5 не оговаривает тип носителя, в то время как сети Token Ring IBM используют витую пару) и размер поля маршрутной информации (см. далее в этом разделе обсуждение характеристик полей маршрутной информации).

На практике реализованы две скорости передачи — 4 Мбит/с и 16 Мбит/с, различающиеся качеством кабельной системы (если используются высококачественные экранированные витые пары, то возможна передача на скорости 16 Мбит/с).

Сети эффективны при загрузке более 30% (в несколько раз лучше по сравнению с Ethernet за счет отсутствия коллизии, повторных передач и т.д.), но менее распространены из-за своей высокой стоимости (в несколько раз дороже Ethernet).

Технология строится не только на одних сетевых адаптерах.

Объединение осуществляется с помощью так называемых блоков MAU (Multistation Access Unit) — концентраторов на 4, 8, 12 портов (рис. 5.4).

Станции сети IBM Token Ring напрямую подключаются к MAU, которые могут быть объединены с помощью кабелей, образуя одну большую кольцевую сеть (см. рис. 5.4). Кабели-перемычки соединяют MAU со смежными MAU. Кабели-лепестки подключают MAU к станциям. В составе MAU имеются шунтирующие реле для исключения станций из кольца.

Концентраторы служат для удобства управления сетью, в частности, отключения от кольца неисправных узлов.

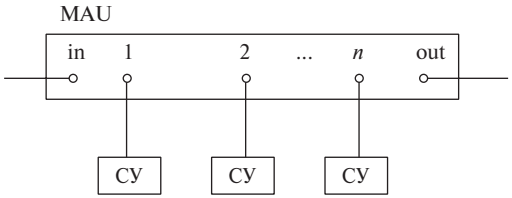


Рис. 5.4. Концентратор MAU

MAU представляет собой фрагмент кольца с двумя специальными портами IN и OUT и портами для подключения СУ (рис. 5.5).

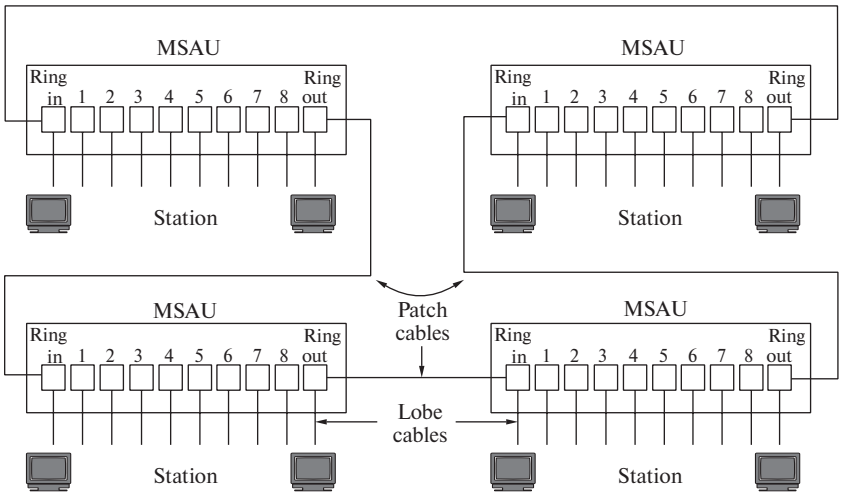


Рис. 5.5. Структурная схема сети

В СУ стоят сетевые адаптеры Token Ring (рис. 5.6).

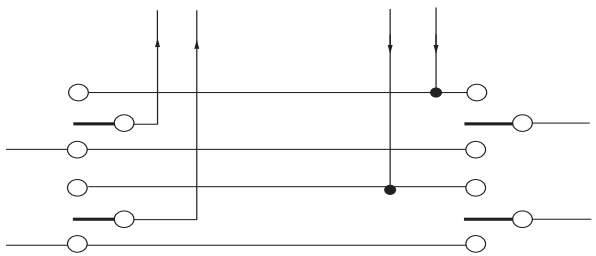


Рис. 5.6. Структурная схема сети MAU

Если сеть небольшая (8–12 СУ), то она может состоять из одного блока MAU и порты IN и OUT замыкать не надо (они замкнуты внутри).

При большем числе станций блоки MAU соединяются последовательно в кольцо.

Территориально MAU можно разместить вместе.

Для отключения узла достаточно левые переключатели поставить в верхнее, а правые переключатели — в нижнее положение (в нормальном режиме положение переключателей противоположное).

Существует два типа сетей, два способа реализации, геометрия которых показана на рис. 5.7, а характеристики в табл. 5.2:

1) стационарные (непередвигаемые);

2) гибкие (подвижные).

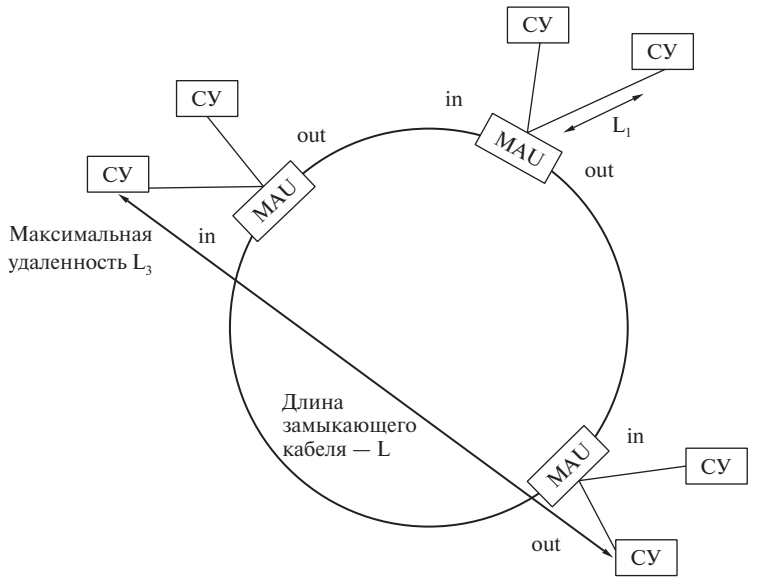


Рис. 5.7. Геометрия сети

Таблица 5.2

Характеристика	Тип исполнения сети	
	Гибкое	Стационарное
Максимальная длина кабеля между двумя концентраторами L1 или между концентратором и станцией L2, м	L1 = L2 = 45	L1 = L2 = 100

Окончание табл. 5.2

Характеристика	Тип исполнения сети	
	Гибкое	Стационарное
Максимальное число концентраторов MAU в кольце	12	3
Максимальное число СУ в кольце	96	260
Предельное расстояние (максимальная длина замыкающего кабеля) L, м	120	360
Максимальная территориальная удаленность L3, м	150	380
Скорости передачи данных, Мбит/с	4 или 16	4 или 16

Отличия состоят в качестве кабельной системы.

Сеть Token Ring рассчитана на меньшие предельные расстояния и число станций, чем Ethernet, но лучше приспособлена к повышенным нагрузкам.

Формат кадра Token Ring

Сети Token Ring определяют два типа блока данных: блоки маркеров и блоки данных / блоки команд. Оба формата представлены на рис. 5.8.

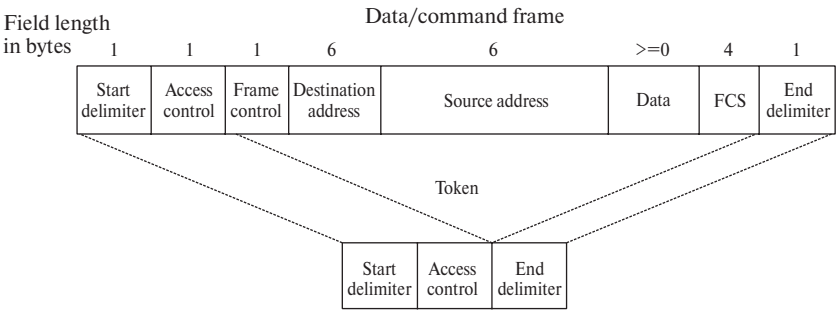


Рис. 5.8. Формат кадра

В технологии используется три типа кадра:

- маркер;
- данные/управление;
- прерывание последовательности.

1. Кадр «маркер» содержит три 8-битовых поля.

Поля SD и ED (Start Delimiter и End Delimiter) — начальный и конечный разделители, используются во всех типах кадров и представляют собой специфическую последовательность электрических сигналов, имеющих другие параметры по амплитуде и длительности, чтобы не перепутать их с обычными информационными байтами.

Поле ED несет также информационную нагрузку, состоящую из двух информационных битов:

- бит промежуточного кадра S (если S = 1, то пакет не последний в цепочке, S = 0 — последний или единственный);
- бит ошибки E (E = 1 устанавливается любым СУ, если при прохождении через него пакета контрольная сумма не совпадает с расчетной). Остальные поля — обычные битовые последовательности.

Поле AC (Access Control) — 8-битовое поле управления доступом, имеет формат: PPP-T-M-RRR:

PPP — биты приоритета, позволяют обеспечить поддержку приоритетов СУ (0–7, наивысший — 7);

RRR — резервные биты для реализации механизмов назначения приоритетов;

T — Token-бит (если T = 1, то идет маркер, при T = 0 — кадр данных управления, т.е. маркер+данные);

M — бит механизма мониторинга для повышения устойчивости работы кольца.

Некоторый СУ может в том случае занять свободный маркер, если его приоритет равен или выше приоритета в битах PPP. Если через станцию проходит занятый маркер, то она делает заявку на будущую передачу, устанавливая в битах RRR свой приоритет только в том случае, если ее приоритет выше, чем указанный. В момент освобождения маркера (после считывания информации СУ-приемником) биты RRR копируются в биты PPP, и приоритет из заявленного становится фактическим.

2. Данные/управление (табл. 5.3).

Блок данных и блок команд могут иметь разные размеры в зависимости от размеров информационного поля. Блоки данных переносят информацию для протоколов высших уровней; блоки команд содержат управляющую информацию, в них отсутствует информация для протоколов высших уровней.

В блоке данных / блоке команд за байтом управления доступом следует байт управления блоком данных. Байт управления блоком данных указывает, что содержит блок — данные или управляющую информацию. В управляющих блоках этот байт определяет тип управляющей информации.

За байтом управления блоком следуют два адресных поля, которые идентифицируют станции пункта назначения и источника. Для IEEE 802.5 длина адресов равна 6 байтам.

За адресными полями идет поле данных. Длина этого поля ограничена временем удержания маркера кольца, которое определяет максимальное время, в течение которого станция может удерживать маркер.

За полем данных идет поле последовательности проверки блока (FCS). Станция-источник заполняет это поле вычисленной величиной, зависящей от содержания блока данных. Станция назначения повторно вычисляет эту величину, чтобы определить, не был ли блок поврежден при прохождении. Если это так, то блок отбрасывается.

Так же как и маркер, блок данных / блок команд заканчивается ограничителем конца.

Таблица 5.3

SD	AC	FC	DA	SA	INFO	FCS	ED	FS

Поле AC (Access Control) — 8-битовое поле управления доступом, формат аналогичен кадру маркера.

Поле FC (Frame Control) — поле управления кадром имеет структуру FF-CCCCCC.

FF — биты, определяющие, какому уровню управления сетью соответствует данный кадр:

FF = 00 — уровень 2.1.MAC;

FF = 01 — уровень 2.2.LLC;

FF = 10 и FF = 11 — резервные комбинации.

В битах CCCCCC (Command) зашифрована команда, которая передается с помощью данного кадра для обеспечения правильного функционирования кольца или обеспечения реализации соответствующего протокола:

- 000011 — кадр-заявка, эту команду отправляет резервный монитор, если основной «умер» или «умирает» (когда возникают сомнения в активности);
- 000000 — тест дублирования адреса, отправляется СУ, который впервые подключается к кольцу с целью проверки уникальности его собственного адреса;
- 000101 означает, что активный (главный) монитор «жив», т.е. главный монитор извещает сеть о своей активности и посылает этот кадр так часто, как только это возможно;

- 000010 — «сигнал», СУ отправляет кадр в случае обнаружения серьезных проблем в кольце (обрыв кабеля и проблемы с захватом кабеля вне очереди);
- 000110 — «очистка», отправляется после инициализации кольца, после того как новый главный монитор захватил кольцо.

Поля DA (Destination Adress) и SA (Source Adress) — 48 бит адреса приемника и источника.

Поле INFO имеет переменную длину (1–8 Кбайт). Когда кольцо загружено слабо, то длина выбирается максимальной и при повышении степени загруженности кольца длина кадра постепенно уменьшается, чтобы мелкими порциями, но часто давать возможность всем желающим что-то передать.

Поле FS (Frame Status) — поле состояния кадра (служебная информация для настройки кольца).

Поле FCH (Frame CheckSum) — контрольная сумма кадра.

Так как поле FS находится вне зоны действия контрольной суммы, информационные биты передаются в двух экземплярах.

Наличие контрольной суммы, битов E в ED и AC в FS позволяет более точно локализовать проблемы, возникающие в кольце. Точно локализуется место ошибки в сегменте кольца.

3. Кадр «прерывание последовательности».

Кадр предназначен для обрыва передачи данных (прекращения циркулирования маркера по кольцу). Одноименные поля в разных кадрах имеют одну структуру. Последние версии технологии поддерживают многомаркерные сети.

Функционирование сети Token Ring

Token Ring и IEEE 802.5 являются главными примерами сетей с передачей маркера. Сети с передачей маркера перемещают вдоль сети небольшой блок данных, называемый маркером. Владение этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки, он просто переправляет маркер к следующей конечной станции. Каждая станция может удерживать маркер в течение определенного максимального времени.

Если у станции, владеющей маркером, имеется информации для передачи, она захватывает маркер, изменяет у него один бит (в результате чего маркер превращается в последовательность «начало блока данных»), дополняет информацией, которую он хочет передать, и, наконец, отсылает эту информацию к следующей станции кольцевой сети. Когда информационный блок циркулирует по кольцу, маркер в сети отсутствует (если только кольцо не обеспечи-

вает «раннего освобождения маркера» — early token release), поэтому другие станции, желающие передать информацию, вынуждены ожидать. Следовательно, в сетях Token Ring не может быть коллизий. Если обеспечивается раннее высвобождение маркера, то новый маркер может быть выпущен после завершения передачи блока данных.

Информационный блок циркулирует по кольцу, пока не достигнет предполагаемой станции назначения, которая копирует информацию для дальнейшей обработки. Информационный блок продолжает циркулировать по кольцу; он окончательно удаляется после достижения станции, отославшей этот блок. Станция отправки может проверить вернувшийся блок, чтобы убедиться, что он был просмотрен и затем скопирован станцией назначения.

В отличие от сетей CSMA/CD (например, Ethernet) сети с передачей маркера являются детерминистическими сетями. Это означает, что можно вычислить максимальное время, которое пройдет, прежде чем любая конечная станция сможет передавать. Эта характеристика, а также некоторые характеристики надежности, которые будут рассмотрены дальше, делают сеть Token Ring идеальной для применений, где задержка должна быть предсказуема и важна устойчивость функционирования сети. Примерами таких применений является среда автоматизированных станций на заводах.

По сети циркулирует маркер, имеющий структуру:

<ограничитель-P-T-M-R-ограничитель>.

Сети Token Ring используют сложную систему приоритетов, которая позволяет некоторым станциям с высоким приоритетом, назначенным пользователем, более часто пользоваться сетью. Блоки данных Token Ring содержат два поля, которые управляют приоритетом: поле приоритетов и поле резервирования.

Только станции с приоритетом, который равен или выше величины приоритета, содержащейся в маркере, могут завладеть им. После того как маркер захвачен и изменен (в результате чего он превратился в информационный блок), только станции, приоритет которых выше приоритета передающей станции, могут зарезервировать маркер для следующего прохода по сети. При генерации следующего маркера в него включается более высокий приоритет данной резервирующей станции. Станции, которые повышают уровень приоритета маркера, должны восстановить предыдущий уровень приоритета после завершения передачи.

Если T = 0, то маркер свободен. Тогда если он проходит мимо станции, имеющей данные для передачи, и приоритет станции не

ниже значения, записанного в P, то станция преобразует маркер в информационный кадр: устанавливает T = 1 и записывает между R и конечным ограничителем адрес получателя, данные и другие сведения в соответствии с принятой структурой кадра.

Информационный кадр проходит по кольцу, при этом: 1) каждая станция, готовая к передаче, записывает значение своего приоритета в R, если ее приоритет выше уже записанного в R значения; 2) станция-получатель, распознав свой адрес, считывает данные и отмечает в конце кадра (в бите «статус кадра») факт приема данных.

Совершив полный оборот по кольцу, кадр приходит к станции-отправителю, которая анализирует состояние кадра. Если передача не произошла, то делается повторная попытка передачи. Если произошла, то кадр преобразуется в маркер указанной выше структуры с T = 0. При этом также происходят действия:

P := R; R := 0, где *P* и *R* — трехбитовые коды.

При следующем обороте маркер будет захвачен той станцией-претендентом, у которой на предыдущем обороте оказался наивысший приоритет (именно его значение записано в P).

Механизмы управления передачей

Сети Token Ring используют несколько механизмов обнаружения и компенсации неисправностей в сети. Например, одна станция в сети Token Ring выбирается «активным монитором» (active monitor). Эта станция, которой в принципе может быть любая станция сети, действует как централизованный источник синхронизирующей информации для других станций кольца и выполняет разнообразные функции для поддержания кольца. Одной из таких функций является удаление из кольца постоянно циркулирующих блоков данных. Если устройство, отправившее блок данных, отказало, то этот блок может постоянно циркулировать по кольцу. Это может помешать другим станциям передавать собственные блоки данных и фактически блокирует сеть. Активный монитор может выявлять и удалять такие блоки и генерировать новый маркер.

Звездообразная топология сети IBM Token Ring также способствует повышению общей надежности сети. Так как вся информация сети Token Ring просматривается активными MSAU, эти устройства можно запрограммировать так, чтобы они проверяли наличие проблем и при необходимости выборочно удаляли станции из кольца.

Алгоритм Token Ring, называемый «сигнализирующим» (beaconing), выявляет и пытается устранить некоторые неисправ-

ности сети. Если какая-нибудь станция обнаружит серьезную проблему в сети (например, такую, как обрыв кабеля), она высылает сигнальный блок данных. Сигнальный блок данных указывает домен неисправности, в который входят станция, сообщающая о неисправности, ее ближайший активный сосед, находящийся выше по течению потока информации (NAUN), и все, что находится между ними. Сигнализация инициализирует процесс, называемый «автореконфигурацией» (autoreconfiguration), в ходе которого узлы, расположенные в пределах отказавшего домена, автоматически выполняют диагностику, пытаясь реконфигурировать сеть вокруг отказавшей зоны. В физическом плане MSAU может выполнить это с помощью электрической реконфигурации.

5.4. Стандарт IEEE 802.3 Сети Ethernet

5.4.1. Семейство технологий построения сетей Ethernet

Одной из первых среди ЛВС шинной структуры была создана сеть Ethernet, разработанная и реализованная фирмой Xerox в 1975 г.

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI. Ethernet в основном описывается стандартами IEEE группы 802.3. Ethernet стал самой распространенной технологией ЛВС в середине 1990-х гг., вытеснив такие устаревшие технологии, как Token Ring, FDDI и ARCNET.

Название «Ethernet» (буквально «эфирная сеть» или «среда сети») отражает первоначальный принцип работы этой технологии: все, передаваемое одним узлом, одновременно принимается всеми остальными (т.е. имеется некое сходство с радиовещанием). В настоящее время практически всегда подключение происходит через коммутаторы (switch), так что кадры, отправляемые одним узлом, доходят лишь до адресата (исключение составляют передачи на широковещательный адрес) — это повышает скорость работы и безопасность сети.

Технология Ethernet наиболее распространена в ЛВС. Так, по данным на 1996 г. 85% всех компьютеров в ЛВС были в сетях Ethernet.

Общее количество сетей с технологиями Ethernet насчитывает несколько миллионов.

Для сетей Ethernet разрабатывается оборудование рядом фирм (3COM, D-Link, Cisco и др.).

В стандарте первых версий (Ethernet v1.0 и Ethernet v2.0) указано, что в качестве передающей среды используется коаксиальный кабель, в дальнейшем появилась возможность использовать витую пару и оптический кабель.

Преимущества использования витой пары по сравнению с коаксиальным кабелем:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля витой пары;
- более высокая надежность сетей: при использовании витой пары сеть строится по топологии «звезда», поэтому обрыв кабеля приводит лишь к нарушению связи между двумя объектами сети, соединенными этим кабелем (при использовании коаксиального кабеля сеть строится по топологии «общая шина», для которой требуется наличие терминальных резисторов на концах кабеля, поэтому обрыв кабеля приводит к неисправности сегмента сети);
- уменьшен минимально допустимый радиус изгиба кабеля;
- большая помехоустойчивость из-за использования дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт Power over Ethernet, PoE);
- гальваническая развязка трансформаторного типа. В условиях СНГ, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто приводило к выходу из строя сетевых карт в результате электрического пробоя.

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей.

Метод управления доступом (для сети на коаксиальном кабеле) — множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD, Carrier Sense Multiple Access with Collision Detection), скорость передачи данных 10 Мбит/с, размер кадра от 64 до 1518 байт, описаны методы кодирования данных. Режим работы полудуплексный, т.е. узел не может одновременно передавать и принимать информацию. Количество узлов в одном разделяемом сегменте сети ограничено предельным значением в 1024 рабочих станции (спецификации физического уровня могут устанавливать более жесткие ограничения, например, к сегменту тонкого коаксиала может подключаться не более 30 рабочих станций, а к сегменту толстого коаксиала — не более 100). Однако сеть, построенная на одном разделяемом сегменте, становится неэффективной задолго до достижения предельного значения количества узлов, в основном по причине полудуплексного режима работы.

В 1995 г. принят стандарт IEEE 802.3u Fast Ethernet со скоростью 100 Мбит/с и появилась возможность работы в режиме «полный дуплекс». В 1997 г. был принят стандарт IEEE 802.3z Gigabit Ethernet со скоростью 1000 Мбит/с для передачи по оптическому волокну и еще через два года — для передачи по витой паре.

Разновидности Ethernet

В зависимости от скорости передачи данных и передающей среды существует несколько вариантов технологии. Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех нижеперечисленных вариантах.

В этом разделе дано краткое описание всех официально существующих разновидностей. По некоторым причинам в дополнение к основному стандарту многие производители рекомендуют пользоваться другими запатентованными носителями — например, для увеличения расстояния между точками сети используется волоконно-оптический кабель.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных, используя автоопределение (autonegotiation) скорости и дуплексности для достижения наилучшего соединения между двумя устройствами. Если автоопределение не срабатывает, скорость подстраивается под партнера и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10BASE-T и 100BASE-TX, а порт Ethernet 10/100/1000 — поддерживает стандарты 10BASE-T, 100BASE-TX и 1000BASE-T.

В настоящее время унифицировано несколько вариантов (технологий) Ethernet, отличающихся:

- топологией;
- скоростями передачи информации;
- особенностями физической среды передачи данных.

Имеется ряд технологий Ethernet:

- Ethernet 10 Base;
- Fast Ethernet 100 Base;
- Giga Ethernet 1000 Base;
- Ethernet 10G;
- Ethernet 40G и 100G.

Последние две технологии исторически являются развитием первых. На уровне второй иногда ставят технологию мультисетей 100 VG-AnyLAN (Ethernet & Token Ring) со скоростью 100 Мбит/с.

Методы доступа:

- случайный метод доступа с контролем несущей и обнаружением коллизии МДКН/ОК (CSMA/CD), стандарт IEEE 802.3;
- детерминированный метод доступа с эстафетной передачей маркера, стандарт IEEE 802.4.

Тактовая частота передаваемой информации: fT = {10, 100, 1000} Mbit/s.

Топология — шинная.

Среды передачи:

- коаксиальный кабель;
- витая пара;
- оптоволокно;
- радиоканал.

Максимальная удаленность между сетевыми узлами (без использования репитеров, хабов и коммутаторов):

- коаксиальный кабель: 185–500 м — 10 Мбит/с;
- витая пара: 2,5 км — 10 Мбит/с; 250 м — 100 Мбит/с, 100 м — 1 Гбит/с;
- оптоволокно: 412 м — 100 Мбит/с, 25 м — 1 Гбит/с;
- радиоканал — в пределах прямой видимости.

Зона четкой фиксации коллизий при увеличении частоты уменьшается.

Формат кадра Ethernet

Стандарт IEEE 802.3-2008 определяет следующую структуру кадра, обязательную для всех MAC-реализаций, как показано в табл. 5.4.

Таблица 5.4

7 байт	7 байт	6 байт	6 байт	4 байта (опционально)	2 байта	42–1500 байта	4 байта	
Preamble	SFP	Destination Address	Sourse Address	Tag 802.1Q	Length/ Type	Data PAD	FCS	Extension
	64–1522 байта							

На практике существует четыре формата кадров Ethernet:

- Кадр Ethernet II (Ethernet v.2 или DIX Ethernet);
- Кадр IEEE 802.3/LLC;
- Кадр Ethernet SNAP;
- Кадр Raw802.3(Novell 802.3).

Разные типы кадра имеют различный формат и значение MTU (MaximumTransmissionUnit), но могут сосуществовать в одной физической среде.

Наибольшее распространение получил кадр Ethernet II.

Кадр IEEE 802.3/LLC показан на рис. 5.9.

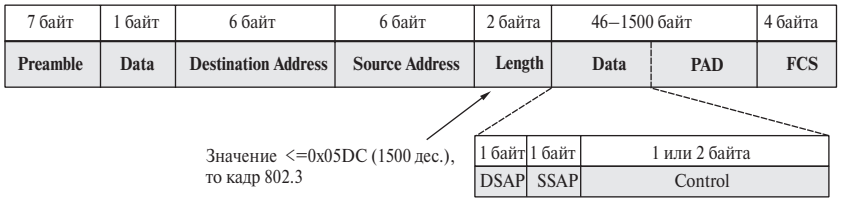


Рис. 5.9. Кадр IEEE 802.3/LLC

- **Preamble (преамбула)**– состоит из семи синхронизирующихся байт 10101010.
- **Start-of-Frame-Delimiter (SFP, начальный ограничитель кадра) — содержит** значение 10101011. Эта комбинация указывает на то, что следующий байт — начало заголовка кадра.
- **Destination Address (DA, адрес назначение)** — MAC-адрес получателя кадра.
- **Source Address (SA, адрес источника)** — MAC-адрес отправителя кадра.
- **Length (длина)** — если значение меньше или равно 0x05DC (1500 дес.), то поле указывает на длину поля данных в кадре.
- **Data (данные)** — поле данных переменной длины. Минимальная длина поля 46 байт, максимальная длина поля 1500 байт.
- **Pad (Padding, заполнение)** — состоит из такого количества байт заполнителей, которое обеспечивает минимальную длину поля данных в 46 байт. Это обеспечивает корректное распознавание коллизий. Если длина поля данных достаточна, поле заполнения в кадре отсутствует.
- **Frame Check Sequence (FCS, поле контрольной суммы)** — содержит контрольную сумму кадра. Служит для проверки, не искажен ли кадр. Значение поля вычисляется на основе содержимого полей DA, SA, длина и поля данных с помощью 32-разрядного циклического избыточного кода (Cyclic Redundancy Code, CRC).

Кадр Ethernet II показан на рис. 5.10.

Поле **Type (тип)** используется для указания типа протокола, вложившего пакет в поле данных кадра.

Кадр Ethernet SNAP показан на рис. 5.11.

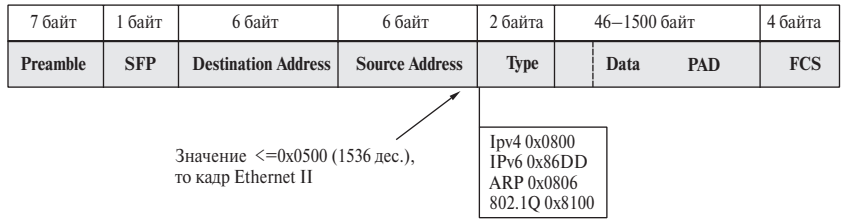


Рис. 5.10. Кадр Ethernet II

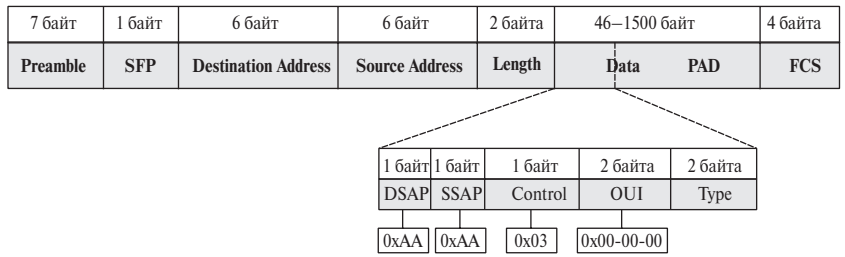


Рис. 5.11. Кадр Ethernet SNAP

Коды протоколов в полях SAP кадра 802.3/LLC имеют длину 1 байт, поле Type в кадре Ethernet II — 2 байта. Один и тот же протокол кодируется разными кодами. Для устранения разнобоя в кодировках типов протоколов комитетом 802.2 был разработан формат Ethernet SNAP (SNAP — Sub Network Access Protocol).

Кадр Ethernet SNAP — расширение кадра 802.3/LLC, добавился:

- **заголовок** протокола SNAP;
- **OUI (Organizational Unique Identifier)** — идентификатор организации, которая контролирует коды в поле Type;
- **Type (тип)** — аналогично полю Тип кадра Ethernet II.

Кадр Raw 802.3 (Novell 802.3) показан на рис. 5.12.

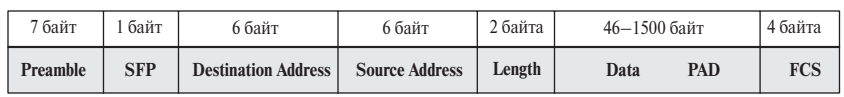


Рис. 5.12. Кадр Raw 802.3 (Novell 802.3)

Кадр представляет собой внутреннюю модификацию IEEE 802.3 без заголовка LLC.

В настоящее время Novell использует кадр IEEE 802.3/ LLC.

Алгоритм определения формата кадра представлен на рис. 5.13.

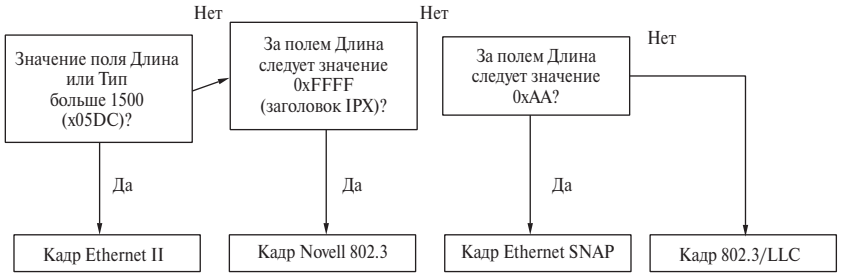


Рис. 5.13. Определение формата кадра

Стандарт IEEE 802.3 определяет два режима работы MAC-подуровня:

- *Полудуплексный (half-duplex)* — использует метод CSMA/CD для доступа узлов к разделяемой среде. Узел может только принимать или передавать данные в один момент времени, при условии получения доступа к среде передачи.
- *Полнодуплексный (full-duplex)* — полнодуплексный Ethernet позволяет паре узлов, имеющих соединение «точка–точка», одновременно принимать и передавать данные. Для этого каждый узел должен быть подключен к выделенному порту коммутатора.

Физический уровень технологии Ethernet

- Все технологии семейства Ethernet имеют одинаковую реализацию MAC-подуровня — форматы кадров и способы доступа к среде передачи.
- Все технологии семейства Ethernet отличаются реализацией физического уровня, который определяет различные скорости передачи сигналов и типы среды передачи.

Структура физического подуровня представлена на рис 5.14.

Jumbo-кадры

Jumbo-кадр (англ. jumbo frame) — понятие в компьютерных сетях, обозначающее кадр сети Ethernet, в котором можно передать данные, по размеру превышающие 1500 байт, заданные стандартами группы IEEE 802.3 (MTU более 1500 байт). Традиционно jumbo-кадры могут передавать до 9000 байтов данных, но существуют другие варианты и требуется обращать внимание на совместимость между различными сетевыми устройствами и их настройки. Многие сетевые карты и сетевые коммутаторы стандарта Gigabit Ethernet поддерживают jumbo-кадры. Некоторые Fast Ethernet (100 Мбит/с) коммутаторы и карты также могут работать с jumbo-кадрами.

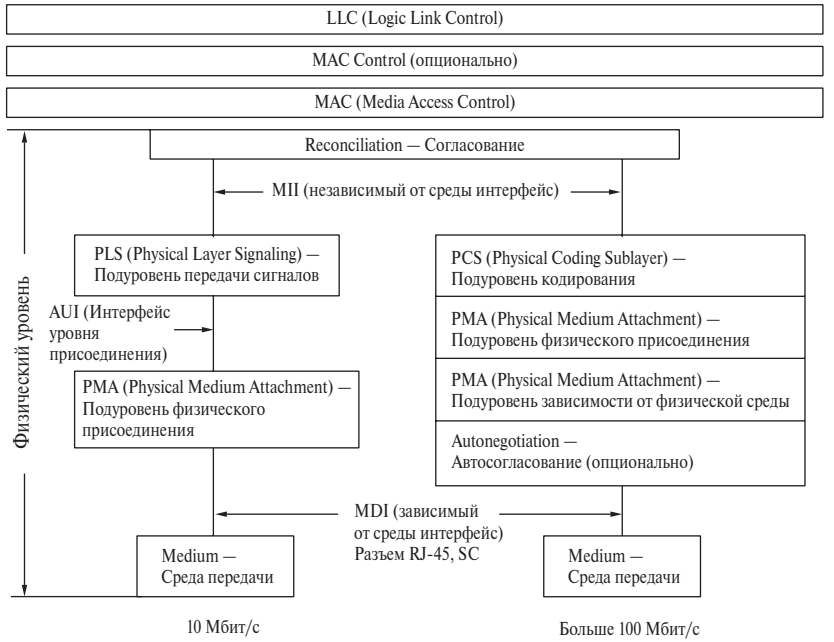


Рис. 5.14. Структура физического подуровня Ethernet

Jumbo-кадры разрешены во многих национальных исследовательских и образовательных сетях (например, Internet II, National LambdaRail, ESnet, GÉANT, AARNet), но не допускаются в коммерческие сети большинства интернет-провайдеров.

Каждый кадр в сети Ethernet должен обрабатываться в процессе передачи между элементами сети. Обработка одного большого кадра может быть более предпочтительной, чем обработка того же количества данных, разбитых на несколько кадров меньшего размера, так как многие накладные расходы могут быть связаны с количеством кадров (например, количество прерываний процессора, количество действий при получении адресов из заголовка кадра и выбор порта назначения и т.п.). Также снижается соотношение объема служебных данных (заголовка) к полезным данным и уменьшается общее количество пакетов для обработки. В качестве обработки можно представить пересылку в одном письме нескольких страниц текста в сравнении с передачей каждой страницы текста в отдельном конверте — это экономит количество конвертов и снижает затраты на сортировку писем.

Jumbo-фреймы получили начальное распространение в конце 1990-х гг., когда фирма Alteon Web Systems ввела их поддержку в адаптерах ACEnic Gigabit Ethernet. Многие производители оборудования реализовали такой же максимальный размер кадра, однако jumbo-кадры не стали частью официальных стандартов Ethernet IEEE 802.3.

По стандартам Ethernet максимальный размер ethernet-кадра составляет 1518 байт.

В каждом кадре заголовки занимают по 18 байт, а данные (поле «payload») могут занимать до MTU = 1500 байт.

При разработке новых стандартов Ethernet (10 Mbit/s, 100 Mbit/s, 1 Gbit/s и др.) величина MTU оставалась неизменной. Это позволяло не делить кадры на части/фрагменты (предотвращало фрагментацию) и позволяло не собирать кадры из частей на стыках между сетями, построенными по разным стандартам Ethernet.

Jumbo-кадр — ethernet-кадр, в котором поле «payload» может занимать от 1500 байт до 16 000 байт. Как правило, размер поля «payload» не превышает 9000 байт, поскольку в сетях Ethernet для проверки целостности используется алгоритм CRC-32. CRC-32 (32-битная контрольная сумма CRC) теряет свою эффективность, если размер данных превышает 12 000 байт. К тому же 9000 байт вполне достаточно для передачи 8-килобайтной дейтаграммы (например, по протоколу NFS).

Каждый раз получая ethernet-кадр из сети, сетевая плата поднимает аппаратное прерывание. Чем больше размер кадра, тем больше данных можно передать в одном кадре. Следовательно, для передачи данных понадобится меньше кадров и сетевая плата будет реже прерывать работу процессора.

Jumbo-кадры могут применяться в следующих случаях:

- при передаче данных на длинные расстояния для увеличения производительности сети;
- для уменьшения нагрузки на центральный процессор;
- при передаче данных по протоколу PPPoE.

В полудуплексной технологии Ethernet независимо от стандарта физического уровня существует понятие домена коллизий.

Домен коллизий (collisiondomain) — это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети коллизия возникла.

Сеть Ethernet, построенная на повторителях, образует один домен коллизий.

Пример доменов коллизий показан на рис. 5.15.

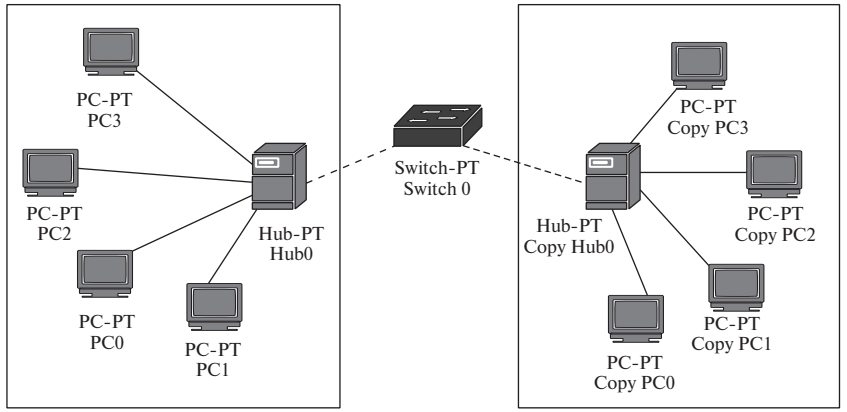


Рис. 5.15. Домены коллизий

Широковещательный домен (сегмент) (англ. broadcast domain) — логический участок компьютерной сети, в котором каждое устройство может передавать данные любому другому устройству непосредственно, без использования маршрутизатора. В общем случае данный термин применим ко второму (канальному) уровню сетевой модели OSI, однако иногда применяется и к третьему уровню с соответствующей оговоркой.

Устройства, ограничивающие широковещательный домен, — маршрутизаторы, работающие на третьем, сетевом, уровне модели OSI, и коммутаторы на втором уровне модели OSI, поддерживающие технологию VLAN или сегментацию трафика. Устройства первого

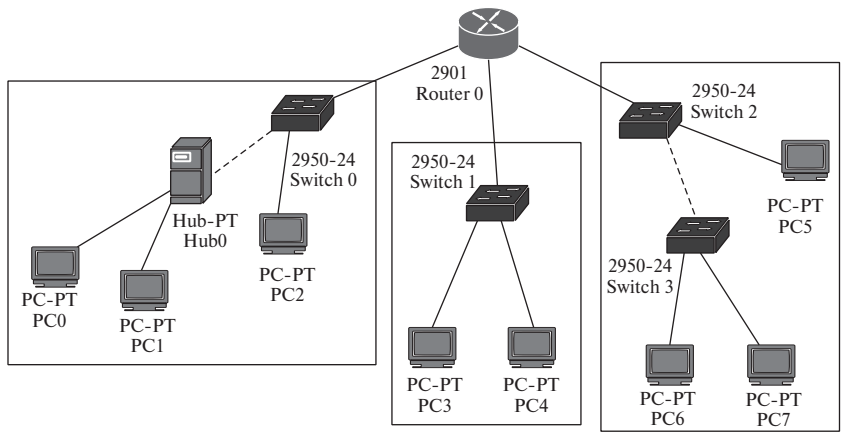


Рис. 5.16. Широковещательные домены

уровня — концентраторы и повторители, а также коммутаторы без поддержки VLAN или сегментации трафика широковещательный домен не ограничивают.

Структура широковещательных доменов показана на рис. 5.16.

5.4.2. Технология построения сетей Ethernet 10 Base

Структура стандартов Ethernet 10 Base представлена в табл. 5.5.

Таблица 5.5

Стандарт	Тип кабеля	Максимальная длина сегмента, м
10BASE5	Первоначальный стандарт, использующий коаксиальный кабель. Известен как «толстый Ethernet», Манчестерское кодирование, топология «шина»	500
10BASE2	Коаксиальный кабель. Известен как «тонкий Ethernet», Манчестерское кодирование, топология «шина»	185
10BASE-T	Кабель на основе витой пары категории 3 или 5 (для приема и передачи используется 2 пары проводников), Манчестерское кодирование, топология «звезда», »дерево»	100
10BASE-FL	Многомодовый оптический кабель 62.5/125, Манчестерское кодирование, топология «звезда», »дерево»	2000 (дуплекс)

Стандарт 10BASE-2

10BASE-2 позволял создавать сегменты размером до 180 м, к каждому сегменту могли подключаться до 30 компьютеров. При использовании 4 повторителей (5 сегментов) максимальный размер сети увеличивался до 900 м.

Название 10BASE-2 происходит от некоторых физических свойств передающей среды. Число 10 означает максимальную скорость передачи данных в 10 Мбит/с. BASE является сокращением от «Baseband» и отражает тот факт, что сигнал, передаваемый по линии связи, модулируется только одной несущей — в данном случае имеющей частоту 10 МГц, т.е. вся полоса пропускания занимается одним сигналом (в отличие от широкополосных методов — «Broadband», когда для передачи по одной физической линии связи используется несколько несущих частот, что позволяет одновременно передавать

несколько сигналов, каждый с использованием своей несущей частоты); 2 — соответствует внешней толщине кабеля, равной примерно 0,2 дюйма или 5 мм («толстый коаксиал» по толщине равен примерно 0,5 дюйма — отсюда название 10Base-5).

При монтаже сети 10BASE-2 необходимо уделить особое внимание прочности соединения кабелей с Т-коннекторами (рис. 5.17) и правильной установке нужных терминаторов. Некачественные контакты и короткие замыкания сложно диагностируемы, даже при помощи дорогих специальных устройств. Неполадки в любом сегменте приводят к полной нефункциональности сети целиком. По этой причине сети типа 10BASE-2 было сложно поддерживать, и чаще всего они заменялись сетями типа 10BASE-T на базе витой пары и топологии «звезда», которые также представляли отличные возможности для апгрейда до типа 100BASE-TX.

Рис. 5.17. Коннекторы

При этом у сети типа 10BASE-2 множество преимуществ по сравнению с 10BASE-T. В частности, для нее не нужен коммутатор, поэтому стоимость оборудования будет намного ниже, а для подключения нового устройства к сети достаточно подключиться к кабелю ближайшего компьютера. Эти характеристики делают сеть на основе 10BASE-2 идеальной для маленькой сети из двух-трех компьютеров, например дома, но не для сети большого предприятия, где этот стандарт будет очень неэффективен.

Стандарт Ethernet 10Base-5

10BASE-5 (также известен как «толстый Ethernet») — оригинальный (первый) «полный вариант» спецификации кабельной системы Ethernet, использовал специальный коаксиальный кабель

типа RG-8X. Это жесткий кабель, диаметром примерно 9 мм, с волновым сопротивлением 50 Ом, с жесткой центральной жилой, пористым изолирующим заполнителем, защитным плетеным экраном и защитной оболочкой. Внешняя оболочка, как правило, имела желто-оранжевую окраску из этилена и пропилена (для огнестойкости), из-за чего часто использовался термин «желтый Ethernet» или, иногда в шутку, «желтый замерзший садовый шланг» (англ. frozen yellow garden hose).

Название 10BASE-5 происходит от некоторых физических свойств передающей среды. Число 10 означает максимальную скорость передачи данных в 10 Мбит/с. Слово «BASE» является сокращением от англ. «baseband», означающего передачу сигналов без модуляции, а пятерка может отсылать к числу 500 — максимальной длине сегмента сети, либо соответствует внешней толщине кабеля, равной примерно 0,5 дюйма.

10BASE-5 рассчитан так, что можно делать дополнительные подключения без отключения остальной сети и разрыва кабеля. Это достигается использованием так называемых «трезубцев» или «вампирчиков» (англ. vampire tap) — устройства, которое с довольно большим усилием «прокусывало» кабель, при этом центральный шип контактировал с центральной жилой коаксиального кабеля, а два боковых шипа входили в контакт с экраном основного кабеля. Как правило, «трезубец» совмещался в одном устройстве с приемопередатчиком (рис. 5.18).

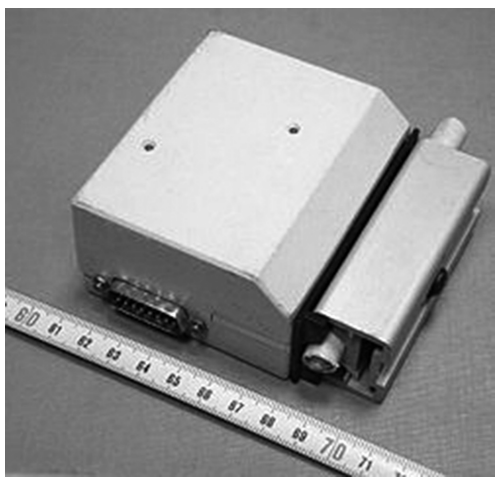


Рис. 5.18. Приемопередатчик

От приемопередатчика к узлу сети (большая ЭВМ, персональный компьютер, принтер и т.п.) подходил кабель Attachment Unit Interface (AUI). Этот интерфейс использует 15-контактный двухрядный разъем D-subminiature, но с дополнительными клипсами, вместо обычно применяемых винтов, для удержания разъема и удобства монтажа.

Практическое максимальное число узлов, которые могут быть соединены с 10BASE-5 сегментом, ограничено 100, а длина сегмента может составлять не более 500 м. Приемопередатчики устанавливаются только с интервалом в 2,5 м. Это расстояние грубо соответствует длине волны сигнала. Подходящие места установки приемопередатчиков отмечаются на кабеле черными метками.

Кабель должен прокладываться единым цельным сегментом, Т-образных связей не допускается. На концах кабеля должны устанавливаться терминаторы 50 Ом (рис. 5.19).

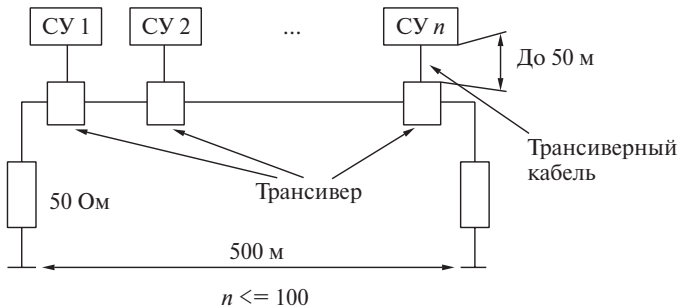


Рис. 5.19. Простейшая односегментная сеть «толстого Ethernet»

Максимальная длина трансиверного кабеля не превышает 50 м.

Технология на коаксиальном кабеле позволяет объединять между собой до пяти сегментов (четыре повторителя), удлиняя тем самым протяженность сети до 2500 м (рис. 5.20).

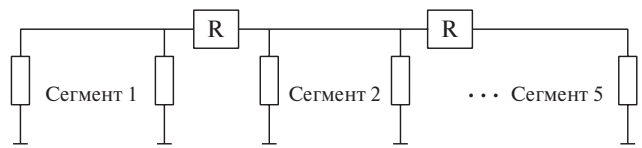


Рис. 5.20. Построение сети на коаксиальном кабеле

Объединение производится через специальные устройства — повторители (repeater — репитер), которые подключены к источнику питания, причем возможно соединять различные типы сегментов

в любом порядке (комбинации тонкий/толстый). У репитера могут быть входы и для тонкого, и для толстого Ethernet.

Ограничение на количество сегментов вызвано трудностями с фиксацией коллизии крайними, наиболее удаленными СУ. Только три сегмента из пяти могут быть нагруженными.

В сетях на коаксиале сложное тестирование и масштабирование.

Технология на коаксиальном кабеле позволяет объединять между собой до пяти сегментов. Объединение производится через специальные устройства — повторители (repeater — репитер), которые подключены к источнику питания, причем возможно соединять различные типы сегментов в любом порядке (комбинации тонкий/толстый). У репитера могут быть входы и для тонкого, и для толстого Ethernet.

Стандарт 10BASE-T

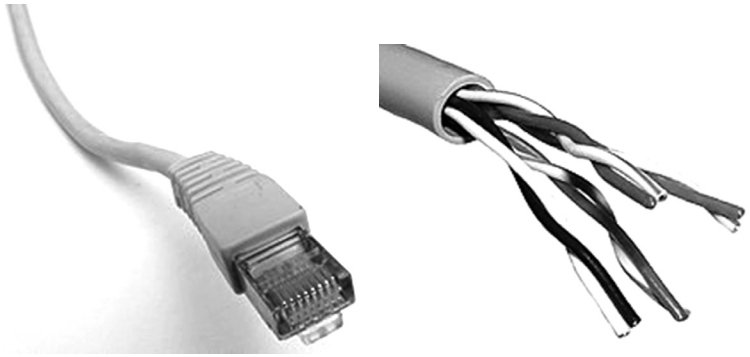
10BASE-T — физический интерфейс Ethernet, позволяющий компьютерам связываться при помощи кабеля типа «витая пара» (twisted pair). Название 10BASE-T происходит от некоторых свойств физической основы (кабеля). «10» ссылается на скорость передачи данных в 10 Мбит/с. Слово «BASE» — сокращение от «baseband» signaling (метод передачи данных). Это значит, что Ethernet-сигнал передается без модуляции, или, иначе говоря, с нулевой несущей частотой, и соответственно полоса сигнала начинается от 0 Гц. Другими словами, не используется мультиплексирование (multiplexing), как в широкополосных каналах. Буква «T» происходит от словосочетания «twisted pair» (витая пара), обозначая используемый тип кабеля.

10BASE-T стал первым независимым от производителя стандартом реализации Ethernet с использованием витой пары. Однако на самом деле это была эволюционная переработка стандарта StarLAN фирмы AT&T, который имел версии со скоростями 1 Мбит/с и 10 Мбит/с.

Используется неэкранированный кабель, содержащий четыре свитых между собой пары проводников (UTP). Требуется кабель по меньшей мере 3-й категории (Cat 3).

10BASE-T использует разъемы типа 8P8C, обжатые согласно таблицам T568A или T568B, определенным в стандарте TIA/EIA-568-B. Используются только вторая и третья пара (оранжевая и зеленая), как показано на рис. 5.21.

Сеть Twisted Pair Ethernet — это кабельная сеть с использованием витых пар проводов и концентраторов, называемых также распределителями, или хабами (Hub) (рис. 5.22).



а) *б*)

Рис. 5.21. Кабель UTP и разъем

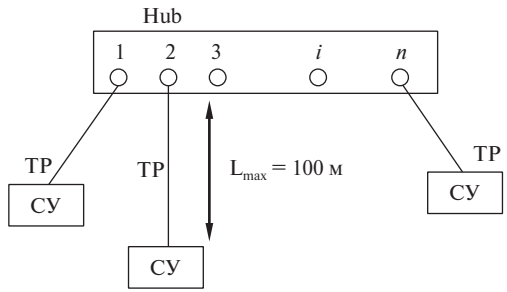


Рис. 5.22. Коммутационное оборудование

В состав сетевого оборудования входят активные (АН) и пассивные (РН) распределители (Active and Passive Hubs), различие между которыми заключается в отсутствии или наличии усиления сигналов, соответственно, и в количестве портов (рис. 5.23).

Принятое обозначение варианта Ethernet 10Base-T; стандарт IEEE 802.3i.

По физической топологии 10Base-T может быть вариантом «звезда», «дерево» и т.п. Однако в такой сети вполне возможна реализация метода доступа МДКН/ОК, и для пользователя (любого отдельного узла) разветвленная сеть из витых пар и концентраторов, по которой происходит широковещательная передача, есть просто среда передачи данных, такая же, как шина. Поэтому по логической организации сеть 10Base-T есть сеть типа Ethernet «шина» (рис. 5.24).

В качестве среды передачи используется витая пара — четыре пары неэкранированных витых проводников Twisted Pair (TP) 3, 4 или 5-й категории (отличаются частотами, шагом скрутки, макси-

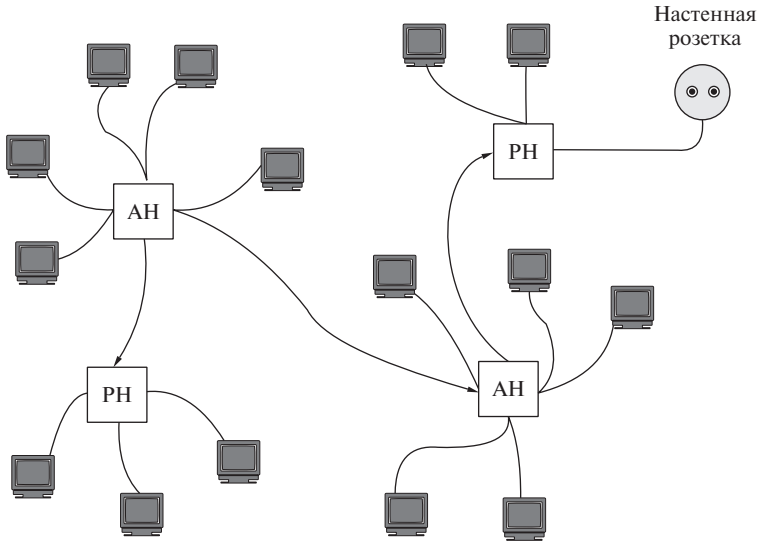


Рис. 5.23. Среда передачи данных на витой паре и концентраторах

мальными длинами, электромагнитными характеристиками). Категории витой пары представлены в табл. 5.6.

Таблица 5.6

ANSI/TIA /EIA-568	**Полоса частот (МГц)**	Приложения	Дополнения и комментарии
Категория 1 **CAT1**	Определена до 0,1 МГц		Телефонный кабель. Используется только для передачи голоса или данных при помощи аналогового или ADSL-модема
Категория 2 **CAT2**	Определена до 1 МГц	Token Ring — 4 Мбит/с	2-парный кабель. Сейчас не используется
Категория 3 **CAT3**	Определена до 16 МГц	Token Ring — 4 Мбит/с 10BASE-T — 10 Мбит/с	2-парный кабель. Основное применение — передача голоса
Категория 4 **CAT4**	Определена до 20 МГц	Token Ring — 16 Мбит/с 10BASE-T — 10 Мбит/с 100BASE-T4 — 100 Мбит/с	4-парный кабель. Комитетом TIA/EIA в дальнейшем не рассматривается

Окончание табл. 5.6

ANSI/TIA /EIA-568	**Полоса частот (МГц)**	Приложения	Дополнения и комментарии
Категория 5 **CAT5**	Определена до 100 МГц	10BASE-T/100BASE-TX (2 пары) — 10/100 Мбит/с, 1000BASE-T (4 пары) — 1 Гбит/с	4-парный кабель. Комитетом TIA/EIA в дальнейшем не рассматривается
Категория 5e **CAT5e**	Определена до 125 МГц	10BASE-T/100BASE-TX (2 пары) — 10/100 Мбит/с, 1000BASE-T (4 пары) —1 Гбит/с	4-парный кабель. Наиболее распространен в современных сетях
Категория 6 **CAT6**	Определена до 250 МГц	10BASE-T — 10 Мбит/с, 100BASE-TX — 100 Мбит/с, 1000BASE-T — 1 Гбит/с , 10GBASE-T — 10 Гбит/с	4-парный кабель. Ограничивает максимальное расстояние передачи для 10GBASE-T до 55 м
Категория 6a **CAT6a**	Определена до 500 МГц	10BASE-T — 10 Мбит/с, 100BASE-TX — 100 Мбит/с, 1000BASE-T — 1 Гбит/с, 10GBASE-T — 10 Гбит/с	4-парный кабель. Планируется использовать его для приложений, работающих на скорости до 40 Гбит/с
Категория 7 **CAT7**	Определена до 600–700 МГц, утверждена только международным стандартом ISO 11801	10GE	4-х парный кабель. Имеет общий экран и экраны вокруг каждой пары. Используется новый «не RJ-45» разъем

Технология использует 8-контактный разъем PJ45 (вилки, розетки), в который вставляются проводники от витых пар. Разъем (вилка) подключается либо к розетке, находящейся в СА, либо — к настенной розетке и СА. К розетке подходит магистральный кабель витой пары и разделывается на контактных площадках. Подключе-

ние СУ от розетки к СА осуществляют с помощью патч-корда (отрезка витой пары с оконцованными на обоих концах вилками) различных длин — 0,5–10 м.

Для соединения многих СУ к моноканалу сети используются концентраторы — хабы (рис. 5.24).

Без них в сети непосредственно можно объединить только два СУ.

Хабы допускают последовательное (иерархическое) включение, но не более чем четыре подряд. Тогда максимальный диаметр сети — 500 м, максимальная длина сети (расстояние между конечными СУ) — 2500 м.

Запрещено петлевидное соединение.

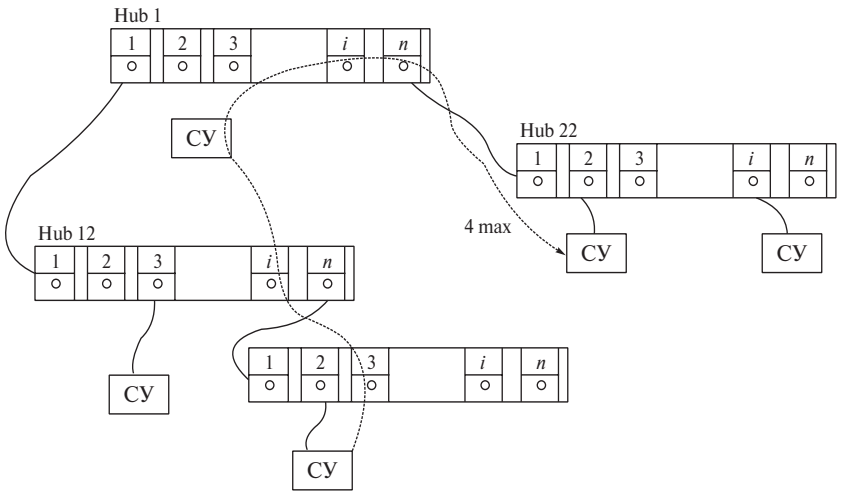


Рис. 5.24. Соединение СУ и хабов

По одной паре проводов можно вести прием, по другой — одновременно передачу информации (полнодуплексный режим). Для этого используется кабель, у которого внутри перевернуты проводники либо один из входов хаба имеет наименование UpLink, в котором уже изменены контакты либо имеются переключатели.

Сетевые адаптеры и хабы технологии Ethernet имеют специальные светодиоды для каждого входа, которые сигнализируют правильность физического соединения СУ и концентраторов (должны всегда гореть, иначе соединение неверное). Проверка правильности соединения витых пар производится с помощью специального сигнала проверки обрыва Normal Link Pulse, который посылается при отсутствии загрузки пары.

Выпускаются также универсальные хабы, которые имеют кроме *n* входов для витой пары еще 1 или 2 входа для коаксиального кабеля — разновидность BNC-разъема для тонкого/толстого Ethernet, осуществляющих переход с одной технологии на другую.

Если у хаба два входа для коаксиальных кабелей, то он является и хабом и репитером одновременно.

Между удаленными СУ не должно быть более четырех репитеров и хабов в сумме.

Максимальное количество СУ в сети может быть по схеме с корневым концентратором (рис. 5.25).

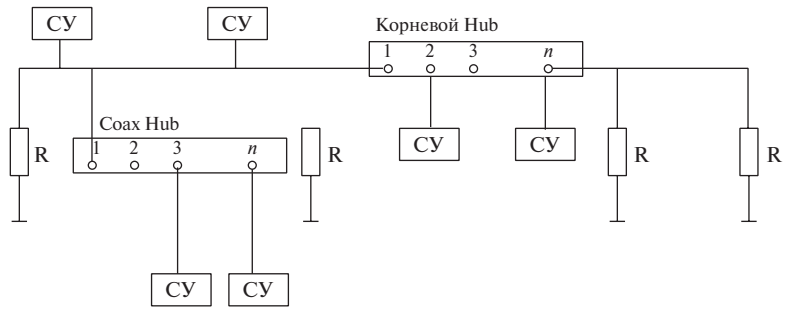


Рис. 5.25. Схема с корневым концентратором

Стандарт 10BASF

Применяется для соединений «точка–точка», например, для соединения двух конкретных распределителей в кабельной сети. Принятое обозначение варианта Ethernet — 100Base-F.

Цена приблизительно такая же, как и медного кабеля, но меньше габариты и масса, полная гальваническая развязка.

Имеет следующие характеристики:

- максимальное число узлов в одном сегменте — 1024;
- максимальная длина сегмента — 2 км;
- максимальная длина между повторителями — 1 км;
- число повторителей — 4 (только каскадное соединение, недопустимы петли);
- максимальная длина сети — 2,5 км (расстояние между крайними СУ).

Оптоволокно значительно дороже, но обладает высокой защищенностью от НСД к информации, так как технически подключиться к оптической среде передачи невозможно без нарушения ее целостности, что легко может быть выявлено. Обычно используют кабель с двумя волокнами для полнодуплексных операций.

Для коммутации с другими типами кабельных систем на концах сегментов кабеля ставят медиаконвертеры МС (преобразователи среды передачи). Универсальный медиаконвертер представлен на рис. 5.26.

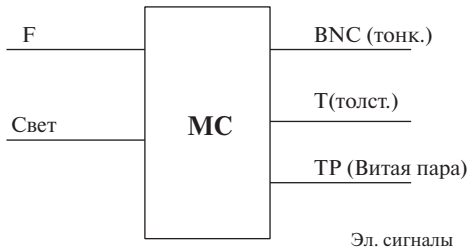


Рис. 5.26. Медиаконвертер

Типовой волоконно-оптический кабель имеет вид, как показано на рис. 5.27.

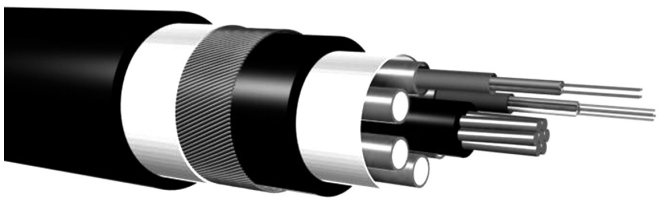


Рис. 5.27. Волоконно-оптический кабель

Действие оптического волокна основано на эффекте полного внутреннего отражения света при переходе из среды с большим коэффициентом преломления в среду с меньшим коэффициентом преломления.

Оптоволоконный кабель состоит из светопроводящего стеклянного сердечника, окруженного стеклянной оболочкой с меньшим коэффициентом преломления.

В зависимости от распределения показателя преломления и от величины диаметра сердечника различают:

- одномодовое волокно;
- многомодовое волокно.

В **многомодовых кабелях (Multi Mode Fiber, MMF)** оптический сигнал, распространяющийся по сердцевине, представлен множеством мод.

Мода описывает режим распространения световых лучей во внутреннем сердечнике кабеля. Варианты оптических кабелей схематично показаны на рис. 5.28.

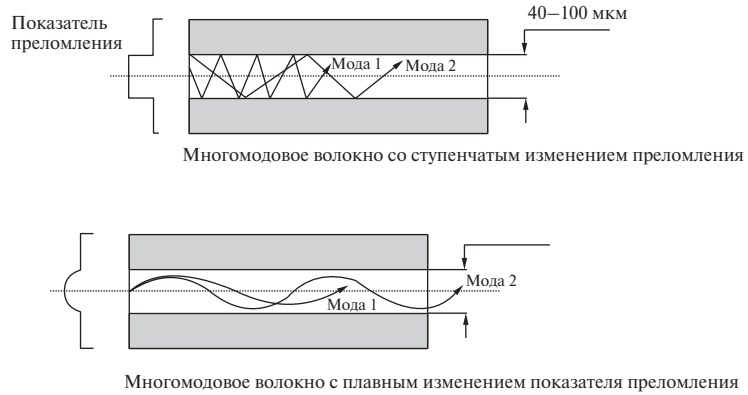


Рис. 5.28. Варианты оптических кабелей

В многомодовых кабелях используются внутренние сердечники с диаметрами 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм — это диаметр центрального проводника, а 125 мкм — диаметр внешнего проводника.

В качестве источников излучения света применяются светодиоды с длиной волны 850 нм.

Максимальная длина многомодового кабеля — до 2 км.

Используется в локальных и домашних сетях небольшой протяженности.

В **одномодовом кабеле (Single Mode Fiber, SMF)** оптический сигнал, распространяющийся по сердцевине, представлен одной модой. Кабель схематично представлен на рис. 5.29.

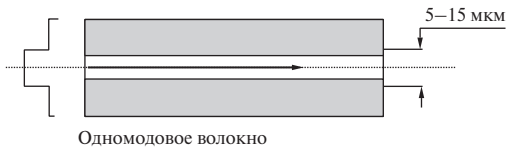


Рис. 5.29. Одномодовый кабель

В одномодовом кабеле используется центральный сердечник очень малого диаметра, соизмеримого с длиной волны света — от 5 до 10 мкм.

В качестве источников излучения света применяются полупроводниковые лазеры с длиной волны 1300 нм, 1550 нм.

Максимальная длина одномодового кабеля — до 100 км.

Используется, как правило, для протяженных линий связи, городских и региональных сетей.

Волоконно-оптические кабели присоединяют к оборудованию разъемами MT-RJ, ST, FC, SC, LC, которые приведены в табл. 5.7.

Таблица 5.7

Разъем ST		Разъем типа ST использует быстро сочленяемое байонетное соединение, которое требует поворота разъема на четверть оборота для осуществления соединения/разъединения
Разъем FC		Разъемы типа FC ориентированы на применение с одномодовым кабелем
Разъем SC		Разъем типа SC широко используется как для одномодового, так и для многомодового волокна. Относится к классу разъемов общего пользования. В разъеме используется механизм сочленения «push-pul». Может объединяться в модуль, состоящий из нескольких разъемов. В этом случае модуль может использоваться для дуплексного соединения (одно волокно которого используется для передачи в прямом, а другое в обратном направлениях)
Разъем LC		Разъем типа LC имеет размеры примерно в два раза меньшие, чем обычные варианты SC, FC, ST, что позволяет реализовать большую плотность при установке на коммутационной панели. Помещен в прочный термостойкий пластмассовый корпус типа push-pull. Фиксируется в розетке защелкой RJ-типа. Может использоваться для дуплексного соединения
Разъем MT-RJ		Разъем типа MT-RJ представляет собой миниатюрный дуплексный разъем

MC может трансформироваться в комбинированный хаб, у которого есть один *N* вход и несколько TP-портов.

До этого рассматривались средства коммутации Ethernet, которые действовали в пределах одной и той же кабельной системы, рассматриваемой как единая шина со своей зоной конфликтов и своим адресом. Кроме хабов в Ethernet в качестве средств коммутации используются специальные устройства — коммутаторы SW (Switch — переключатели).

Коммутатор, в отличие от концентратора, имеет память, которая используется для промежуточного запоминания передаваемых и принимаемых пакетов и, кроме того, в этой памяти по мере работы сети запоминаются адреса сетевых адаптеров по каждому порту (по каким ветвям сети находится станция и в какой порт для нее направляется пакет, в то время как хаб направляет пакет по всем линиям).

Если хаб на *n* портов соединяет два СУ, то SW может соединить *n*/2 портов (пар абонентов между собой), т.е. пропускная способность SW в *n*/2 раз превышает пропускную способность хаба. SW дороже, но эффективнее, так как они разрывают кабельную систему таким образом, что на каждом порте SW — своя кабельная система и зона фиксации коллизии заканчивается на входе порта (каждый порт — отдельный МК).

Последовательное применение коммутаторов позволяет удлинять Ethernet до бесконечности, но предельные расстояния между соседними SW остаются типичными для применяемых технологий, например для витой пары — 100 м.

Для однодуплексной передачи пропускная способность SW определяется: VSW = *n*V/2.

5.4.3. Технология построения сетей Fast Ethernet

Fast Ethernet (FE) — общее название для набора стандартов передачи данных в компьютерных сетях по технологии Ethernet со скоростью до 100 Мбит/с в отличие от исходных 10 Мбит/с. Иногда обозначается как 100BASE-X, где X подразумевает варианты реализации (например, 100BASE-TX, 100BASE-FX). Варианты для работы по витой паре имеют общее обозначение 100BASE-T.

В 1992 г. ряд производителей сетевого оборудования (такие как 3Com, SynOptics и др.) образовали Fast Ethernet Alliance для создания новой спецификации, которая объединила бы отдельные наработки различных компаний в области кабельной передачи данных.

Вместе с тем в институте IEEE была начата работа по стандартизации новой технологии. Созданная для этого исследовательская группа с конца 1992 по конец 1993 г. изучила множество 100-мегабитных решений, предложенных различными производителями, а также высокоскоростную технологию, предложенную компаниями Hewlett-Packard и AT&T.

26 октября 1995 г. официально был принят стандарт IEEE 802.3u, который явился дополнением к уже существующему IEEE 802.3.

В семействе Fast Ethernet различают технологии (стандарт IEEE 802.3u) 1995 г.:

- 100Base-T4 использует четыре неэкранированные витые пары 3, 4, 5-й категории;
- 100Base-TX использует две неэкранированные витые пары TP 5-й категории;
- 100Base-FX использует многомодовый оптоволоконный кабель (2 волокна).

Коаксиальные кабели в данной технологии не применяются.

Информационная скорость — 100 Мбит/с.

Семейство стандартов представлено в табл. 5.8.

Таблица 5.8

Стандарт	Тип кабеля	Максимальная длина сегмента, м
100BASE-TX	Кабель на основе витой пары категории 5 (для приема и передачи используется две пары проводников). Кодирование 4B/5B MLT-3	100
100BASE-FX	Многомодовый оптический кабель (используется два многомодовых волокна). Кодирование 4B/5BNRZI	412 (полудуплекс) 2000 (дуплекс)
100BASE-BX10	Одноволоконный одномодовый оптический кабель (длина волны — 1310 нм восходящий поток, 1550 нм нисходящий). Используется технология WDM для передачи по одному одномодовому волокну	10 000
100BASE-LX10	Одномодовый оптический кабель (длина волны — 1310 нм). Используются два одномодовых волокна	10 000

В Fast Ethernet применен случайный метод доступа МДКН/ОК.

При использовании TP предельные расстояния между СУ и хабами — 100 м, максимальное число хабов между СУ — один, но можно поставить второй при условии, что он отстоит от первого не более чем на 50 м. Таким образом, между двумя наиболее удаленными СУ предельное расстояние составляет 250 м.

При использовании в качестве среды передачи оптоволокна и применении хабов оно увеличивается до 412 м (полудуплекс) и до 2 км (дуплекс) между коммутаторами (при их наличии).

Варианты реализации

Технология 100BASE-TX

100BASE-TX обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из двух витых пар 5-й категории. Обычно передача данных в каждом направлении ведется по одной витой паре, обеспечивая до 100 Мбит/с общей пропускной способности в дуплексе. Длина линии связи ограничена 100 м, но по одному стандартному кабелю, имеющему четыре пары, можно организовать два 100-мегабитных канала связи.

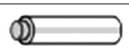
Назначение контактов разъема MDI/MDI-X (TIA/EIA-568-B/A) кабеля UTP 100Base-TX показано в табл. 5.9.

Технология 100Base-T4

100BASE-T4 обеспечивает передачу данных со скоростью до 100 Мбит/с по кабелю, состоящему из четырех витых пар 3-й категории.

Технология 100Base-T4 может использовать старую низкокачественную 8-проводную кабельную систему (от обычного Ethernet). В этом случае необходимо наличие двух трансиверов и двух репитеров. Разводка — та же. Могут использоваться комбинированные коммутаторы, которые позволяют соединять кабельные системы

Таблица 5.9

Контакт	Сигнал	Цвет			
		MDI (TIA/EIA-568-B)		MDI-X (T1A/EIA-568-A)	
1	Передача +		Белый/оранжевый		Белый/зеленый
2	Передача –		Оранжевый		Зеленый
3	Прием +		Белый/зеленый		Белый/оранжевый
4	Не используется		Синий		Синий
5	Не используется		Белый/синий		Белый/синий
6	Прием –		Зеленый		Оранжевый
7	Не используется		Белый/коричневый		Белый/коричневый
8	Не используется		Коричневый		Коричневый

10Мбит/с с системами 100 Мбит/с (SW100/10), причем различают SW, у которых на каждом порту фиксированная скорость передачи и SW с настраиваемой скоростью передачи для каждого порта.

Применение коммутаторов позволяет теоретически до бесконечности увеличивать длину сети Ethernet, а применение хабов — иметь СУ, удаленные на 200–250 м в пределах одной кабельной системы.

Типовая структура сети Fast Ethernet имеет вид дерева, в корнях могут быть использованы более быстрые технологии, в листьях — более медленные.

Технология 100BASE-FX

100BASE-FX использует волоконно-оптический кабель и обеспечивает связь излучением с длиной волны 1310 нм по двум жилам — для приема (RX) и для передачи (TX). Длина сегмента сети может достигать 400 м в полудуплексном режиме (с гарантией обнаружения коллизий) и 2 км в полнодуплексном при использовании многомодового волокна. Работа на бóльших расстояниях возможна при использовании одномодового волокна. 100BASE-FX несовместим с 10BASE-FL (10-мегабитным вариантом).

Технология 100BASE-SX

100BASE-SX — удешевленная альтернатива 100BASE-FX с использованием многомодового волокна и недорогой оптики. 100BASE-SX может работать на расстояниях до 300 м. Используется та же длина волны, что и в 10BASE-FL. Это обеспечивает, в отличие от 100BASE-FX, обратную совместимость с 10BASE-FL. Благодаря использованию более коротких волн (850 нм) и работы на небольших расстояниях, 100BASE-SX требует менее дорогих оптических компонентов (светодиоды вместо лазеров). Это делает данный стандарт привлекательным для тех, кто модернизирует сеть 10BASE-FL и кому не нужна работа на больших расстояниях.

Технология 100BASE-BX

100BASE-BX — вариант для работы по одному оптоволокну (в отличие от 100BASE-FX, где используется пара волокон). Используется одномодовое волокно и специальный мультиплексор, который разбивает сигнал на передающие и принимающие волны.

Технология 100BASE-LX

100BASE-LX обеспечивает передачу данных со скоростью до 100 Мбит/с через оптический кабель по одному одномодовому волокну на длине волны 1310 нм. Максимальная длина сегмента — 15 км в режиме полного дуплекса.

100BASE-LX10 отличается от 100BASE-LX максимальной длиной сегмента — 10 км.

100BASE-LX WDM отличается от 100BASE-LX тем, что допускается использование двух длин волн — 1310 нм и 1550 нм. Интерфейсные модули маркируются либо цифрами (длина волны), либо одной латинской буквой A (1310 нм) или B (1550 нм). В паре могут работать только парные интерфейсы: с одной стороны — передатчик на 1310 нм, а с другой — на 1550 нм.

Сравнение основных характеристик технологий 100BASE приведено в табл. 5.10.

Таблица 5.10

Физический интерфейс	100Base-FX	100Base-TX	100Base-T4
Порт устройства	Dupiex SC	RJ-45	RJ-45
Среда передачи	Оптическое волокно	Витая пара UTP Cat 5 (5e)	Витая пара UTP Cat 3, 4, 5
Сигнальная схема	4B/5B	4B/5B	8B/6T
Битовое кодирование	NRZI	MLT-3	
Число витых пар/волокон	2 волокна		4 витые пары
Протяженность сегмента	До 412 м (ММВ) до 2 км (дуплекс, ММВ) до 100 км (ОМВ)	До 100 м	До 100 м

Fast Ethernet используется: для построения скоростных ЛВС (последовательно включается не более двух хабов), для объединения низкоскоростных подсетей 10Base-T в единую скоростную сеть и для подключения серверов на расстояниях до 200 м. В последнем случае серверы соединяются с клиентскими узлами через шину 100 Мбит/с и коммутатор, называемый также конвертером или переключателем скорости 100/10. К конвертеру с другой стороны подключено несколько шин 10 Мбит/с, на которые нагружены остальные узлы. Практически можно использовать до 250 узлов, теоретически — до 1024. Подсетями могут быть как Fast Ethernet, так и обычные Ethernet с 10 Мбит/с, включенные через преобразователь скорости (рис. 5.30).

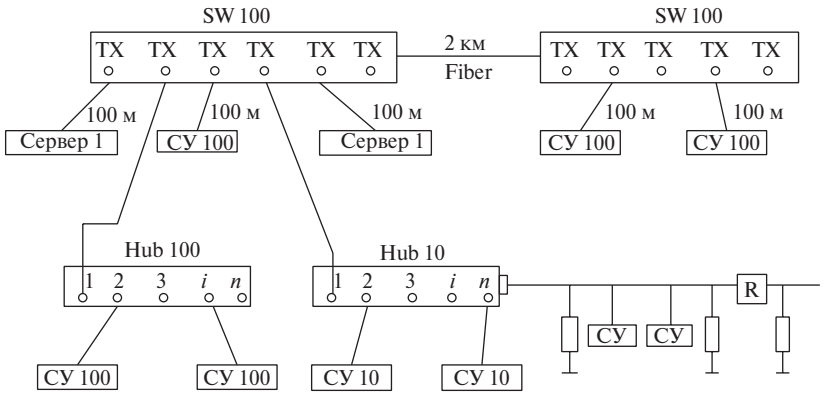


Рис. 5.30. Сеть Fast Ethernet

5.4.4. Технология построения сетей Giga Ethernet

Гигабитные скорости 1 Гбит/с в сети Ethernet достигнуты в варианте Gigabit Ethernet.

Gigabit Ethernet (GE, GbE или 1 GigE) в компьютерных сетях — термин, описывающий различные технологии передачи Ethernet-кадров со скоростью 1 гигабит в секунду, определяемые рядом стандартов группы IEEE 802.3. Используется для построения проводных локальных сетей с 1999 г., постепенно вытесняя Fast Ethernet благодаря значительно более высокой скорости передачи данных. При этом необходимые кабели и часть сетевого оборудования мало отличаются от используемых в предыдущих стандартах, широко распространены и обладают низкой стоимостью.

Ранее в стандарте описывались полудуплексные гигабитные соединения с использованием сетевых концентраторов, но эта спецификация больше не обновляется, и сейчас используется исключительно полнодуплексный режим с соединением через коммутаторы.

Технология Gigabit Ethernet (так же, как и технология Fast Ethernet) используется для построения скоростных ЛВС, но чаще (из-за небольшой протяженности и высокой стоимости оборудования — 5–10 тыс. долл. за коммутатор) используется для связи мощнейших серверов в пределах одного помещения.

Обеспечивается максимальная совместимость с предыдущими технологиями по формату кадров, кабельному хозяйству, полудуплекс/дуплекс протоколы.

Ethernet стал результатом исследований, проведенных Xerox PARC в начале 1970-х гг., и затем развился в популярный протокол

физического и канального уровней OSI. Fast Ethernet увеличил скорость передачи данных с 10 до 100 Мбит/с, Gigabit Ethernet — следующий шаг, на котором скорость увеличилась до 1000 Мбит/с. Первоначально стандарт Gigabit Ethernet был опубликован IEEE в июне 1998 г. как IEEE 802.3z и предполагал использование только оптоволоконного кабеля. Другое широко распространенное название 802.3z — 1000BASE-X, где -X может означать -CX, -SX, -LX или (не описанный в стандарте) -ZX (см. Fast Ethernet).

IEEE 802.3ab, ратифицированный в 1999 г., определяет стандарт гигабитной передачи данных по неэкранированной витой паре (UTP) категорий 5, 5e и 6 и известен как 1000BASE-T. После ратификации 802.3ab гигабитный Ethernet стал прикладной технологией, так как организации могли использовать уже существующую кабельную инфраструктуру.

IEEE 802.3ah, ратифицированный в 2004 г., добавил еще два гигабитных стандарта для оптоволокна: 1000BASE-LX10 (уже широко использовавшийся поставщиками услуг в качестве дополнительной опции) и 1000BASE-BX10. Они являлись частью более обширной группы протоколов (см. Ethernet in the First Mile).

Первоначально гигабитный Ethernet использовался только для опорных сетей с высокой пропускной способностью (к примеру, в высокоскоростных кампусных сетях). В 2000 г. Power Mac G4 и PowerBook G4 компании Apple стали первыми персональными компьютерами на массовом рынке, предоставлявшими возможность 1000BASE-T соединения. Вскоре это стало встроенной особенностью и во многих других компьютерах.

Всего существует пять стандартов физического уровня для гигабитного Ethernet, использующих оптоволоконный кабель (1000BASE-X), витую пару (1000BASE-T) или экранированный сбалансированный медный кабель (1000BASE-CX).

Стандарт IEEE 802.3z включает в себя 1000BASE-SX для передачи сигнала по многомодовому оптоволокну, 1000BASE-LX — по одномодовому оптоволокну и почти вышедший из употребления 1000BASE-CX — по экранированному сбалансированному медному кабелю. Эти стандарты используют кодирование 8b/10b, которое повышает скорость передачи линии на 25%, с 1000 Мбит/с до 1250 Мбит/с. Символы затем отправляются с использованием кода NRZ.

IEEE 802.3ab, в котором описан широко распространенный тип интерфейса 1000BASE-T, использует другую схему кодирования, чтобы поддерживать скорость передачи символов на как можно более низком уровне для отправки данных по витой паре.

IEEE 802.3ap определяет работу Ethernet на электронных объединительных платах при различных скоростях.

Ethernet in the First Mile позднее добавил стандарты 1000BASE-LX10 и -BX10. Семейство стандартов представлено в табл. 5.11.

Таблица 5.11

Стандарт	Тип кабеля	Максимальная длина сегмента, м
1000BASE-T	Кабель на основе витой пары категории 5, 5e, для передачи используются 4 пары проводников. Кодирование PAM5	100
1000BASE-SX	Многомодовый оптический кабель 62.5/125 микрон/ 50/125 микрон (длина волны 850 нм). Кодирование 8B/10BNRZ	550
1000BASE-LX	Одномодовый оптический кабель (длина волны 1310 нм). Многомодовый оптический кабель (длина волны 1310 нм). Кодирование 8B/10B NRZ	5 000 550
1000BASE-LX10	Одномодовый оптический кабель (длина волны 1310 нм). Многомодовый оптический кабель (длина волны 1310 нм). Используются два одномодовых или многомодовых волокна	10 000 550
1000BASE-BX10	Одноволоконный одномодовый оптический кабель (длина волны: 1310 нм восходящий поток, 1490 нм нисходящий). Используется технология WDM для передачи по одному одномодовому волокну	10 000
1000BASE-ZX	Одномодовый оптический кабель (длина волны 1550 нм) – не входит в стандарт, но применяется в отрасли	100 000
1000BASE-LH (Long Haul)	Одномодовый оптический кабель	100 000

Гигабитная скорость достигается благодаря следующим решениям (стандарт IEEE 802.3z).

В качестве среды передачи данных используются:

- витые пары — технология Giga Ethernet 1000Base-CX. Максимальная удаленность СУ — 10-25 м;
- оптоволокно с длиной волны 850 нм — технология Giga Ethernet 1000Base-SX, расстояния до 550 м;
- оптоволокно с длиной волны 1300 нм — технология Giga Ethernet 1000Base-LX, расстояния до 550 м.

При использовании коммутаторов с оптическими портами расстояние между смежными SW может быть до 500 м.

Сеть имеет иерархическую структуру.

Участки (отдельные компьютеры или подсети) по 10 Мб/с подключаются к портам переключателей (switches) скорости 10/100, их выходы по 100 Мб/с, в свою очередь, подключаются к портам переключателей 100/1000.

В сегментах сети, имеющих 1000 Мб/с, используются:

- передача данных по ВОЛС или параллельно по всем четырем витым парам;
- 5-уровневое представление данных (+2, +1, 0, –1, –2 В), за один такт передается 2,322 бит информации;
- кодирование 8b/10b.

В результате в каждой витой паре из четырех имеем 250 Мб/с, при частоте сигналов 125 МГц. Для обработки сигналов В СА используются DSP-процессоры.

Структура сети, использующая все скорости передачи, показана на рис. 5.31.

Типовая структура сети Fast Ethernet имеет вид дерева, в корнях могут быть использованы более быстрые технологии, в листьях — более медленные (рис. 5.30).

Распределение нагрузки между SW должно соответствовать информационным потокам, поэтому для нормального функционирования необходимо рассчитать пропускную способность каждого SW.

Большинство сетевых адаптеров Fast Ethernet имеют функции автоматического определения скорости и вида взаимодействия с устройством, к которому они подключены (SW, Hub или другой компьютер).

Настройка выполняется с помощью сигнала NLP (Normal Link Pulse). Кроме скорости проверяется вид связи (полудуплексная или полнодуплексная) и по возможности выбирается полнодуплексная.

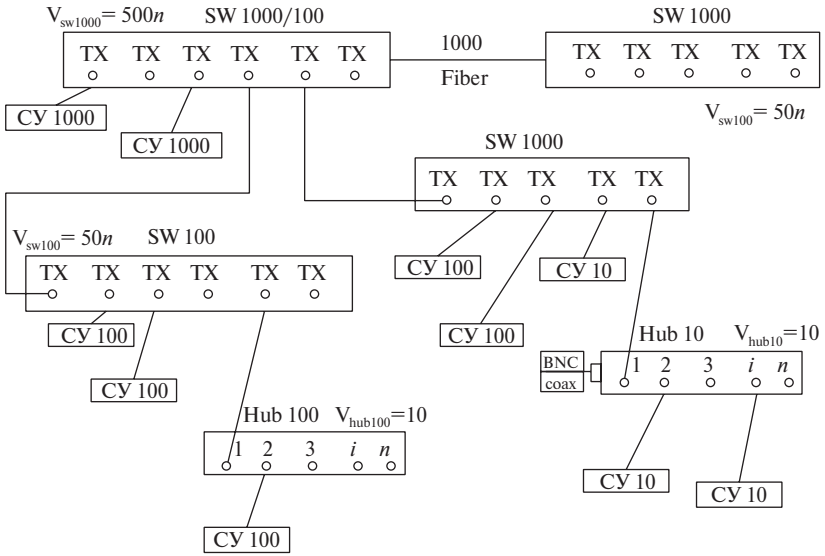


Рис. 5.31. Типовая структура сети Fast Ethernet

5.4.5. 10 Gigabit EtherNet

Стандарт 10-гигабитного Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время он описывается поправкой IEEE 802.3ae.

10GBASE-CX4 — технология 10-гигабитного Ethernet для коротких расстояний (до 15 м), используется медный кабель CX4 и коннекторы InfiniBand.

10GBASE-SR — технология 10-гигабитного Ethernet для коротких расстояний (до 26 или 82 м, в зависимости от типа кабеля), используется многомодовое волокно. Он также поддерживает расстояния до 300 м с использованием нового многомодового волокна (2000 МГц/км).

10GBASE-LX4 — использует уплотнение по длине волны для поддержки расстояний от 240 до 300 м по многомодовому волокну. Также поддерживает расстояния до 10 км при использовании одномодового волокна.

10GBASE-LR и 10GBASE-ER — эти стандарты поддерживают расстояния до 10 и 40 км соответственно.

10GBASE-SW, 10GBASE-LW и 10GBASE-EW — эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.

10GBASE-T, IEEE 802.3an-2006 — принят в июне 2006 г. после четырех лет разработки. Использует витую пару категории 6 (максимальное расстояние — 55 м) и 6a (максимальное расстояние — 100 м).

10GBASE-KR — технология 10-гигабитного Ethernet для кросс-плат (backplane/midplane) модульных коммутаторов/маршрутизаторов и серверов (Modular/Blade).

Семейство стандартов 10 Gigabit EtherNet представлено в табл. 5.12.

Таблица 5.12

Стандарт	Тип кабеля	Максимальная длина сегмента, м
10GBASE-CX4	Экранированный сбалансированный медный кабель. Используется медный кабель CX4 и разъем InfiniBand	15
10GBASE-SR	Многомодовый оптический кабель (длина волны 850 нм). Кодирование 64B/66B	300
10GBASE-LR	Одномодовый оптический кабель (длина волны 1310 нм). Кодирование 64B/66B	10 000
10GBASE-ER	Одномодовый оптический кабель (длина волны 1550 нм). Кодирование 64B/66B	40 000
10GBASE-LX4	Одномодовый оптический кабель. Многомодовый оптический кабель (использует WDM на длине волны около 1310 нм). Кодирование 8B/10B	10 000 от 240 до 300 (в зависимости от полосы пропускания)
10GBASE-T	Кабель на основе витой пары категории 6a (при использовании кабеля категории 6 длина сегмента уменьшается до 50 м). Для передачи используются 4 пары проводников. Кодирование Tomlinson-Harashimaprecoded (THP) — версия PAM с 16 дискретными уровнями	100

Стандарты семейства 10 Gigabit Ethernet на MAC-подуровне поддерживают работу только в полнодуплексном режиме.

5.4.6. 40 и 100 Gigabit EtherNet

40-гигабитный Ethernet (40GbE) и 100-гигабитный Ethernet (100GbE) — стандарты Ethernet, разработанные рабочей группой «IEEEP802.3ba Ethernet Task Force» в период с ноября 2007 г. по июнь 2010 г.

Семейство стандартов представлено в табл. 5.13.

Таблица 5.13

Стандарт 802.3ba		Тип кабеля	Максимальная длина сегмента, м
40GBASE-KR4		По объединительной плате (backplane). Кодирование 64B/66B	1
40GBASE-CR4	100GBASE-CR10	Сбалансированный медный кабель. Кодирование 64B/66B	7
40GBASE-SR4	100GBASE-SR10	4 волокна (40GBASE-SR4) или 10 волокон (100GBASE-SR10) многомодового оптического кабеля 50/125 микрон (длина волны 850 нм). Кодирование 64B/66B	100
40GBASE-LR4	100GBASE-LR4	Одномодовый оптический кабель. Кодирование 64B/66B. Используется технология WDM (4 параллельных потока бит)	10 000
	100GBASE-ER4	Одномодовый оптический кабель. Кодирование 64B/66B. Используется технология WDM (4 параллельных потока бит)	40 000
Стандарт 802.3bg			
40GBASE-FR		Одномодовый оптический кабель	2 000

Эти стандарты являются следующим этапом развития группы стандартов Ethernet, имевших до 2010 г. наибольшую скорость в 10 Гбит/с. В стандарте IEEE Std 802.3ba-2010 устанавливается скорость передачи данных в 40 и 100 Гбит/с при совместном использовании нескольких линий связи (lane) на 10 либо 25 Гбит/с.

В стандартах 40/100-гигабитного Ethernet содержится описание нескольких различных стандартов физического уровня (PHY). Сетевые устройства могут использовать различные типы PHY путем использования сменных PHY-модулей. Модули, использующие оптическое волокно, стандартизированы в 802.3ba в различных multi-source agreements, MSA (соглашения между различными производителями). Один из стандартизованных модулей, поддерживающий и 40- и 100-гигабитный Ethernet, — это CFP MSA (англ. C form-factor pluggable), который может использоваться для расстояний 100 м и более. Модули QSFP и CXP обеспечивают работу на меньших дистанциях.

Стандарт 802.3ba поддерживает только полнодуплексный режим работы.

При разработке PHY-части стандарта ставились цели:

- сохранить формат кадров Ethernet стандарта 802.3, использующих формат 802.3 MAC;
- сохранить минимальные и максимальные размеры кадра (FrameSize), совпадающие с текущей редакцией стандарта 802.3;
- обеспечить в точке сопряжения интерфейса MAC/PLS[10] с уровнем ошибок (Bit error ratio) не выше 10 –12 (т.е. не более 1 ошибки в среднем на каждые 1012 бит);
- обеспечение соответствующей поддержки оптических транспортных сетей (англ. Optical transport network, OTN);
- скорость передачи данных на уровне MAC в 40 и 100 Гбит/с;
- разработка вариантов уровня PHY для работы через одномодовое оптическое волокно (SMF), многомодовое оптическое волокно OM3 (MMF), кабели с медными проводниками и через объединительные платы (backplane).

Задача передачи сигнала со скоростями 40 и 100 Гбит/с по оптическому кабелю OM3 на 100 м (40GBASE-SR4 и 100GBASE-SR10) была решена использованием волны около 850 нм, сходной с таковой в стандарте 10GBASE-SR.

Передача сигнала со скоростью 40 Гбит/с по печатным платам на расстояния до 10 км (40GBASE-KR4) реализуется использованием четырех линий стандарта 10GBASE-KR.

Работа на расстояниях 10 и 40 км реализуется с использованием четырех разных длин волн (около 1310 нм), используются оптические элементы со скоростью передачи данных 25 Гбит/с (для 100GBASE-LR4 и 100GBASE-ER4) и 10 Гбит/с (для 40GBASE-LR4).

В отличие от ситуации конца 1990-х гг., когда отсутствие скоростных интерфейсов магистральных маршрутизаторов сдерживало развитие всей сети Интернет, увеличение транспортных скоростей с 10 до 100 Гбит/с в 2010-х гг. в основном мотивировалось экономическими соображениями, как-то: сокращение числа требуемых волн в магист-

ральных оптических сетях, снижение стоимости интерконнектов в больших центрах обработки данных и точках обмена трафиком, а также снижение потерь емкости за счет разбалансировки трафика в параллельных группах 10-гигабитных каналов. При этом многие магистральные операторы связи стремились перейти непосредственно от использования SONET/SDH на 10 Гбит/с, минуя промежуточную фазу в 40 Гбит/с, к 100-гигабитным Ethernet-интерфейсам и выиграть в стоимости за счет ожидаемого быстрого снижения стоимости последних.

Немаловажную роль в ожидаемом снижении цен сыграл отказ от разработки отдельных канальных схем для SONET/SDH и Ethernet. Де-факто 100-гигабитный Ethernet отныне становился единственным фреймовым форматом на вершине оптической иерархии скоростей (ODU4), что гарантирует параллельное снижение цен при росте производства 100-гигабитных интерфейсов как для магистральных, так и для локальных сетей. Следующим уровнем иерархии должен стать формат ODU5, эксклюзивно планируемый к применению в 400-гигабитных Ethernet-сетях.

При разработке 100-гигабитных систем индустрии предстояло преодолеть следующие технологические проблемы:

- разработать схемы модуляции и кодирования сигнала, позволяющие передавать 100-гигабитные потоки на достаточную дальность в оптическом С-диапазоне (1530—1565 нм);
- разработать новые оптические источники и приемники вкупе с оборудованием оптической коррекции (усилители, компенсаторы дисперсии, селективные фильтры и т.д.);
- разработать электронные линейные карты, Ethernet-MAC-чипы и сетевые процессоры для потоковой обработки пакетных данных на скорости 100 Гбит/с.

В целом, решение этих проблем потребовало значительных инвестиций в интеллектуальную собственность, что способствовало затягиванию выхода конечных продуктов на рынок. Несмотря на то что большинство производителей оптического и электронного оборудования заявили о поддержке 100-гигабитных систем в течение 2009—2010 гг. и регулярно испытывали системы разной степени готовности, широкое внедрение 100-гигабитного Ethernet началось лишь в 2011 г.

Оптический транспорт с поддержкой 100-гигабитного Ethernet

Поскольку передача оптического сигнала в условиях нелинейной среды (оптическое волокно) является принципиально аналоговой проблемой, прогресс в этой области замедляется, причем значительно в большей степени, чем снижающийся прогресс в литографии цифровых электронных схем (описываемый эмпирическим законом Мура). Как результат, несмотря на то что 10-гигабитные оптические интерфейсы и транспортные системы существовали с середины 1990-х гг., первые успешные попытки передачи 100-гигабитных потоков в оптических сетях произошли более чем через 15 лет. Кроме того, первые магистральные 100-гигабитные системы были подвержены ряду серьезных ограничений, в том числе связанных с высокой стоимостью за счет использования уникальных лазерных систем, а также значительным энерго-габаритным требованиям, что исключало выпуск трансиверов в компактных форматах (таких как SFP+), раннее разработанных для 1-, 2,5- и 10-гигабитных сигналов.

По состоянию на середину 2011 г. как минимум пять компаний поставляли покупателям системы оптического транспорта, совместимые с канальной скоростью ODU4 (104,794 Гбит/с), в том числе Ciena (решение бывшей Nortel Networks), MRV, Alcatel-Lucent, ADVA Optical Networking. Последней к списку присоединилась компания Huawei, объявившая о начале поставок корейской компании KPN в июне 2011 г. Ожидается, что до конца 2011 г. такие системы будут доступны от всех ведущих производителей оптического оборудования.

Совершенствование оптических транспортных систем для передачи 100-гигабитного Ethernet будет неизбежно происходить в сторону уменьшения их стоимости, при этом могут использоваться следующие перспективные технологии: совместная передача сигнала двумя 50-гигабитными лазерами меньшей стоимости в одной выделенной полосе спектра, широкое использование цифровой обработки сигнала (DSP) для коррекции нелинейностей, уменьшение числа оптоэлектронных (OEO) преобразований в транспортной системе за счет поддержки внешних источников сигнала (foreign lambdas) и т.д.

Первые пакетные маршрутизаторы и коммутаторы с поддержкой 100-гигабитного Ethernet

Наличие линейных оптических 100-гигабитных систем передачи данных позволяет сократить число требуемых длин волн в DWDM-системах и увеличить объем передаваемых данных по существующей кабельной инфраструктуре. Тем не менее, использование 100-гигабитного оптического транспорта для передачи параллельных 10-гигабитных потоков данных снижает эффективность статистического мультиплексирования в пакетных сетях, а также требует 10×10-гига-

битных мукспондеров для согласования форматов. По этой причине магистральные операторы проявляют заинтересованность в переходе на поддержку 100-гигабитного Ethernet непосредственно на интерфейсе маршрутизатора (пакетного коммутатора).

Сложность в разработке чипсета для поддержки 100-гигабитного Ethernet заключается в необходимости обеспечения высокой производительности при равномерной загрузке интерфейса вне зависимости от параметров входящего трафика и отсутствии перестановок пакетов внутри одного IP/MPLS-потока — последнее требование делает распараллеливание одного полнодуплексного 100-гигабитного интерфейса между несколькими (двумя или четырьмя) отдельными сетевыми процессорами технически сложным. Дополнительные трудности создает дизайн линейных карт — за счет возросших требований к размерам и охлаждению 100-гигабитной оптики и в условиях дефицита на рынке 100-гигабитных трансиверов фирмы-пионеры 100-гигабитного сетевого оборудования были вынуждены вести самостоятельные либо совместные оптоэлектронные разработки для того, чтобы уложиться в жесткие линейные и энергетические ограничения современных сетевых устройств. Ожидается, что по мере выхода на свободный рынок коммерческих электронных и оптических компонентов 100-гигабитных решений список поставщиков таких систем будет расти, а цены будут активно снижаться.

Значительный объем начальных инвестиций в запуск 100-гигабитного Ethernet-продукта объясняет как начальный фокус в сторону оборудования высшей ценовой категории (операторского класса), так и желание производителей «досрочно рапортовать» о запуске продуктов до начала серийного производства, по результатам инженерных либо технологических испытаний. Поэтому в приведенном ниже историческом списке первых поставщиков 100-гигабитного Ethernet-решения указаны как даты начального объявления IP/MPLS-продуктов, так и официальные даты поставок (с учетом доступности информации).

Стандарт 100Gigabit на рынке сетевого оборудования

Alcatel-Lucent

Компания Alcatel-Lucent впервые анонсировала 100-гигабитные интерфейсы стандарта 802.3ba для маршрутизаторов 7450 ESS/7750 SR в июне 2009 г.; в июне–сентябре 2010 г. были проведены публичные тесты и демонстрации. Однако в презентации президента оптического отделения компании Джеймса Уатта (апрель 2011 г.) 100-гигабитный Ethernet упоминался все еще лишь в контексте демонстрации клиентам (T-Systems, Portugal Telecom, 360Networks). Пресс-релиз компании 18 июня 2011 г. был вновь ограничен результатами полевых испытаний.

Возможным объяснением столь длительной задержки является архитектура пакетных продуктов Alcatel-Lucent, изначально ориентированных на оказание услуг на границе сети (VPLS, PPPoE, развитая структура очередей).

Фактически Alcatel-Lucent производит всего одно базовое семейство маршрутизаторов (Alcatel 7750), приобретенное с компанией Timetra Networks. В 2011 г. единственной серийно выпускаемой элементной базой для семейства являлся сетевой процессор собственной разработки FP2 с полнодуплексной производительностью в 50 Гбит/с. В соответствии с документацией фирмы, два чипсета FP2 могут также быть установлены в оппозитной, полудуплексной 100-гигабитной конфигурации, позволяющей реализовать интерфейс 100-гигабитного Ethernet без балансировки по потокам между чипами. Однако такая аппаратная конфигурация чревата дисбалансом нагрузки ввиду того, что количество входных операций (ingress lookup), как правило, превышает количество требуемых выходных операций (egress lookup), что может быть недостаточно для стабильной работы решения в реальной сети.

В перспективе Alcatel-Lucent планирует перевести платформу 7750 на объявленный в мае 2011 г. 400-гигабитный чипсет FP3, который, возможно, и станет первым реальным 100-гигабитным продуктом компании на обновленной платформе 7750.

Brocade

Фирма Brocade объявила о поддержке 100-гигабитного Ethernet на унаследованной от поглощения Foundry Networks платформе MLXe в сентябре 2010 г. Тем не менее, уже в июне 2011 г. Brocade смогла анонсировать первый коммерческий запуск своей 100-гигабитной технологии на площадке AMS-IX в Амстердаме, таким образом став одной из первых фирм, получивших доход на 100-гигабитном рынке.

Линейка скоростных маршрутизаторов MLXe использует сетевые процессоры и оптику сторонних разработчиков; платформа поддерживает минимум услуг как в пакетном (базовый IP/MPLS-коммутатор) так и в оптическом (разнообразие трансиверов) диапазоне. Brocade позиционировал свой первый 100-гигабитный Ethetnet-продукт для MLXe (двухпортовую линейную карту) в на-

чальном ценовом сегменте, с дополнительной лицензией на использование второго порта.

Cisco

Корпорация Cisco совместно с Comcast еще в 2008 г. объявили об успешных испытаниях 100-гигабитного Ethernet по существующей оптической инфраструктуре между городами Филадельфия (штат Пенсильвания) и Маклин (штат Вирджиния). Использовались маршрутизаторы Cisco CRS-1 и оптические каналы DWDM. Тем не менее, эта демонстрация не воспроизводила полностью полнодуплексный Ethernet-канал на 100 Гбит/с, поскольку маршрутизатор CRS-1 поддерживает скорость до 40 Гбит/с на слот. Очевидно, что в тесте 2008 г. нагрузка интерфейса не могла превысить половины от расчетной скорости.

Технически первой платформой Cisco, способной обеспечить работу 100-гигабитных Ethernet-интерфейсов, стал маршрутизатор CRS-3 с одним чипсетом на линейную карту и скоростью в 140 Гбит/с на слот. По этой причине первые настоящие испытания 100-гигабитного Ethernet-оборудования производства Cisco состоялись лишь в 2010 г., а первые коммерческие клиенты (AT&T и Comcast) были объявлены в апреле 2011 г. В июле 2011 г. Cisco также проводила демонстрации 100-гигабитных интерфейсов на маршрутизаторах границы ядра (ASR9000) без анонсирования даты поставок.

Huawei

Huawei представила «первую в индустрии» разработку 100-гигабитного интерфейса для маршрутизатора в октябре 2008 г. Следующим шагом фирмы стал анонс законченной системы для передачи 100 Гбит/с в сентябре 2009 г. Система включала в себя оптический транспорт OSN6800/8800 и 100-гигабитные линейные карты маршрутизаторов NE5000e на основе чипсета собственной разработки «Solar 2.0 PFE2A chip» и оптики в форм-факторе CFP. В 2010 г. это же решение было детализировано как использующее карты LPU-100F на основе двух чипсетов Solar 2.0 в оппозитной конфигурации. Тем не менее, в пресс-релизе компании о получении контракта на строительство IP/MPLS-сети для российской компании «Мегафон» в октябре 2010 г. Huawei отчитался лишь о поставке 40-гигабитных систем NE5000e, «с возможностью масштабирования до 100 Гбит» на слот.

В апреле 2011 г. компания выпустила новый анонс линейной карты для NE5000e на том же чипсете Solar 2.0 — две 100-гигабитные

карты LPU-200[33]. В описании сопутствующего решения приводились цифры по поставкам 20G/40G версии чипсета (120 тыс. комплектов Solar 1.0) но не были приведены цифры по поставкам Solar 2.0. Также в пресс-релизе о тестировании 100-гигабитного оборудования в России за август 2011 г. Huawei сообщил о коммерческой установке DWDM-систем на 100 Гбит/с в KPN и China Telecom, но не привел ни одного покупателя 100-гигабитных решений на базе NE5000e.

Помимо задержек с реализацией чипсета для поддержки 100 Гбит/с, позиции Huawei могут также ослабляться установленной базой NE5000e, большинство экземпляров которой несовместимы с новыми картами со скоростями 100 и 200 Гбит/с на слот. Таким образом, несмотря на весьма раннее анонсирование 100-гигабитных продуктов, вероятность получения компанией Huawei прибыли на 100-гигабитном рынке в 2011 г. невелика.

Juniper Networks

Juniper заявил о поддержке 100-гигабитного Ethernet на платформе T1600 в июне 2009 г. К тому времени платформа T1600 поставлялась уже два года и поддерживала работу 100-гигабитных линейных карт (конфигурации 10×10-гигабитных портов). Установленные в ноябре 2010 г. в маршрутизаторах T1600 академической сети Internet2 100-гигабитные Ethernet-модули позволили Juniper позиционировать себя как ведущего поставщика серийных 100-гигабитных продуктов. В том же 2010 г. компания показала работу 100-гигабитных Ethernet-интерфейсов от ядра до границы сети между платформами T1600 и MX3D.

В марте 2011 г. компания начала поставки 100-гигабитных решений оператору связи Verizon). Судя по отчетам пользователей, в тот же период времени Juniper производил поставки и менее крупным клиентам (к примеру, Janet UK) и на середину 2011 г. уже располагал существенной 100-гигабитной клиентской базой. Обратной стороной лидерства на 100-гигабитном рынке для Juniper, по-видимому, стал выбор архитектуры относительно низкой плотности (один 100-гигабитный интерфейс на слот, работающий через два параллельных 50-гигабитных чипсета с равномерным делением нагрузки). К концу 2011 г. Juniper подготовил начало коммерческой эксплуатации сразу двух новых магистральных продуктов с поддержкой 100 Гбит/с — обновленной T-серии (T4000) со скоростью 240 Гбит/с на слот и нового MPLS-коммутатора PTX со скоростью 480 Гбит/с на слот.

Рынок 100-гигабитных решений для маршрутизаторов в целом повторил ситуацию с запуском 10-гигабитных интерфейсов в начале 2000-х гг. — де-факто, пионером поставок выступила компания Juniper, на несколько месяцев опередившая Cisco, своего крупнейшего соперника. Далее к поставкам подключилось новое сетевое отделение компании Brocade, при этом остальные участники рынка закрепиться в первой волне не смогли.

5.5. Сети 100VGAnyLAN

Сеть 100VG-AnyLAN (стандарт IEEE 802.12) имеет следующие характеристики:

- скорость передачи информации — 100 Мбит/с;
- метод доступа к моноканалу — метод приоритетных запросов DPP (Demand Priority Protocol);
- поддержка форматов кадра, принятых в Ethernet и Token Ring;
- физические линии — витая пара или оптоволокно;
- топология — звезда, но возможно каскадное включение хабов (не более 3-х уровней каскадирования);
- максимальное число центров звезд — 2 (2 уровня: 1 — корневой, 2 — вторичный);
- ограничения по протяженности сети — Li + Lj < = 250 м;
- предельная удаленность при использовании двух уровней — 375 м;
- кодирование данных 5B/6B.

Технологию построения мультисетей 100 VG-AnyLAN (Ethernet & Token Ring) со скоростью 100 Мбит/с иногда связывают с развитием технологии Ethernet 10 Base и ставят на один уровень с технологией Fast Ethernet 100 Base. Однако технология 100 VG отличается от классической технологии Ethernet 10 Base в значительно большей мере, чем Fast Ethernet 100 Base. Главные отличия:

- метод доступа к МК — DPP обеспечивает более справедливое распределение пропусконой способности ЛВС, по сравнению со случайным методом доступа МДКН/ОК. Этот метод поддерживает приоритетный доступ для синхронных приложений;
- кадры передаются в ЛВС не всем СУ, а лишь только СУ приемника;
- в сети есть выделенный арбитр доступа к разделяемой среде — концентратор, в отличие от других ЛВС, где используется распределенный между СУ алгоритм доступа;

- поддержка кадров технологий Ethernet и Token Ring (в названии технологии приставка AnyLAN);
- нет коллизий, поэтому можно передавать данные по всем парам проводов;
- одновременная передача данных 25 Мбит/с по четырем парам UTP категории 3 (в сумме 100 Мбит/с).

Для кодирования информации применяется код без возвращения к нулю (NRZ), в котором единица представляется высоким уровнем напряжения, нуль — низким уровнем.

При разработке этой сети считалось, что она будет дальнейшим развитием обычного Ethernet и будет соединять в себе достоинства сетей Ethernet и Token Ring. От старых сетей Ethernet при использовании данной технологии может использоваться старая кабельная система низкого качества на витой паре. Возможность применения витой пары объясняется тем, что задействованы все 8 проводов, и производится не манчестерское кодирование, а кодирование 5 бит в 6 битах без возврата к 0 (5B/6B NRZ).

В качестве центров коммутации используются концентраторы 100VG Any LAN. При этом имеется корневой (центральный) концентратор и соединенные с ним СУ и подчиненные концентраторы.

Допускается три уровня каскадирования.

Каждый концентратор и СУ должен быть настроен либо на кадры Ethernet, либо на кадры Token Ring (одновременная циркуляция обоих типов кадров не допускается).

Технология 100 VG-AnyLAN поддерживает несколько спецификаций физического уровня:

1) четыре неэкранированные витые пары (UTP) категорий 3, 4, 5;
2) два неэкранированные витые пары (UTP) категории 5;
3) экранированные витые пары (STP) категории 1;
4) два многомодовых оптоволокна.

По каждой из четырех пар передается информация со скоростью 30Мб/с $\rightarrow$ 30Мб/с $\times$ 4 = 120Мб/с. Но так как в этой технологии используется кодирование 5B/6B, то итоговая пропускная способность сети равна 120 $\times$ (5/6) = 100Мб/с. Поэтому для четырех пар достигается 4-кратное увеличение пропускной способности при использовании частоты 25 МГц, то же и для двух экранированных пар, так как здесь вдвое выше допустимая частота 50 МГц.

Преимущества:

- использование детерминированного метода доступа к моноканалу (устойчива к помехам);
- повышенная безотказность сети;

- возможность использования кабелей от старого Ethernet (3-й категории);
- множество хороших технических решений по реализации технологии.

Недостатки:

- более дорогое оборудование;
- небольшая протяженность;
- отсутствует FullDuplex'ный режим, т.е. та станция, которая в данный момент передает пакет данных, не может ничего принять от другой станции и наоборот;
- повышенная сложность по сравнению со ставшей традиционной технологией Fast Ethernet 100 Base.

Принцип информационного взаимодействия технологии 100VG Any LAN

Концентратор циклически выполняет опрос *n*-го количества портов.

Опрос СУ выполняется поочередно по портам корневого хаба с учетом приоритетов (два уровня приоритета). Если к порту подключен хаб низшего уровня, то он ждет окончания опроса портов хаба высшего уровня. Если узел ждет получения полномочий более 300 мс, то его приоритет повышается.

Каждый СУ, в отличие от метода опроса, сам определяет, в какой момент ему посылать данные. Если такие данные готовы для передачи, то СУ посылает сигнал запроса (низкочастотный сигнал) на концентратор с указанием приоритета кадра данных. Этот запрос фиксируется концентратором в очереди портов (от 4 до 32), если сеть занята. Очередь обрабатывается в соответствии с порядком поступления запросов и их приоритетами. Если станция-приемник свободна в данный момент и очередь данного запроса подошла, то концентратор подтверждает получение запроса и ждет от СУ прихода данных. После получения данных концентратор декодирует Апр и далее ретранслирует данные только СУ-приемнику или только вторичному концентратору, к которому подключен приемник. При этом опрос концентратором верхнего уровня приостанавливается до завершения опроса концентратором нижнего уровня.

СУ, подключенные к концентраторам различного уровня иерархии, не имеют преимущества по доступу к разделяемой среде, так как это решение о предоставлении доступа к среде принимается после проведения всеми концентраторами опроса всех своих портов.

Сетевая технология поддерживает структурированную систему приоритетов при обработке запросов от СУ.

Внутри концентратора существуют две очереди:

- с высшим приоритетом (мультимедиа данные);
- с низшим приоритетом — обычные данные (файловая служба, служба печати и др.).

Очередь запросов низшего приоритета обрабатывается в том случае, когда очередь высшего приоритета пуста.

В данной технологии используются механизмы динамических и статических приоритетов. Динамический приоритет — это когда приоритет заявки меняется во времени. Если время ожидания заявки СУ в очереди с низким приоритетом больше определенного порогового значения, то она переходит на другой уровень (повышается приоритет).

Механизм определения концентратором порта СУ-приемника.

Во всех других технологиях кадр передается всем СУ В ЛВС. СУ-приемник, распознав свой адрес в кадре, копирует кадр в буфер. При этом концентратор «узнает» MAC-адрес СУ в момент ее физического подключения к ЛВС. В процедуре физического подключения для технологии Ethernet 10 Base устанавливается связность кабеля (Link test), для FDDI — тип порта, для Fast Ethernet 100 Base — скорость работы порта (процедура автопереговоров), то для технологии 100VG Any LAN концентратор определяет MAC-адрес. СУ запоминает его в таблице MAC-адресов (аналогично таблицам адресов мостов/коммутаторов). Отличие только в том, что у концентратора 100VG Any LAN нет внутреннего буфера для хранения кадров. Поэтому, приняв только один кадр, концентратор сразу направляет его в порт СУ-приемника и, пока этот кадр не будет принят СУ-приемником, прием других кадров не ведет. При этом эффект разделяемой среды сохраняется. Улучшается безопасность сети, так как кадры не попадают на «чужие» порты и их труднее перехватить.

5.6. Технология FDDI/CDDI (кольцевая сеть на оптоволокне/коаксиальном кабеле)

FDDI (англ. Fiber Distributed Data Interface — волоконно-оптический распределенный интерфейс передачи данных) — стандарт передачи данных в локальной сети, протянутой на расстоянии до 200 км. Стандарт основан на протоколе Token Ring. Кроме большой территории сеть FDDI способна поддерживать несколько тысяч пользователей.

Стандарт был разработан в середине 1980-х гг. Национальным американским институтом стандартов (ANSI). В этот период быстродействующие АРМ проектировщика уже начинали требовать максимального напряжения возможностей существующих локальных сетей (LAN) (в основном Ethernet и Token Ring). Необходимо было создать новую LAN, которая могла бы легко поддерживать эти АРМ и их новые прикладные распределенные системы. Все большее внимание начинает уделяться надежности, так как администраторы систем стали переносить критические по назначению прикладные задачи из больших компьютеров в сети. FDDI была создана для того, чтобы удовлетворить эти потребности. После завершения работы над FDDI, ANSI представила его на рассмотрение в ISO. ISO разработала международный вариант FDDI, который полностью совместим с вариантом стандарта, разработанным ANSI. Хотя реализации FDDI сегодня не столь распространены, как Ethernet или Token Ring, FDDI приобрела значительное число своих последователей, которое увеличивается по мере уменьшения стоимости интерфейса FDDI. FDDI часто используется как основа технологий, а также как средство для соединения быстродействующих компьютеров, находящихся в локальной области.

Стандарт FDDI определяет 100 Мбит/с. LAN с двойным кольцом и передачей маркера, которая использует в качестве среды передачи волоконно-оптический кабель. Он определяет физический уровень и часть канального уровня, которая отвечает за доступ к носителю; поэтому его взаимоотношения с эталонной моделью OSI примерно аналогичны тем, которые характеризуют IEEE 802.3 и IEEE 802.5.

Хотя она работает на более высоких скоростях, FDDI во многом похожа на Token Ring. Обе сети имеют одинаковые характеристики, включая топологию (кольцевая сеть), технику доступа к носителю (передача маркера), характеристики надежности (например, сигнализация-beaconing) и др.

Двойное кольцо

Одной из наиболее важных характеристик FDDI является то, что она использует световод в качестве передающей среды. Световод обеспечивает ряд преимуществ по сравнению с традиционной медной проводкой, включая защиту данных (оптоволокно не излучает электрические сигналы, которые можно перехватывать), надежность (оптоволокно устойчиво к электрическим помехам) и скорость (потенциальная пропускная способность световода намного выше, чем у медного кабеля).

При обрывах оптоволокна возможно частичное (при двух обрывах) или полное (при одном обрыве) восстановление связности сети.

FDDI — это первая технология ЛВС (1986–1988 гг.), в которой в качестве среды передачи используется волоконно-оптический кабель. Технология FDDI во многом основывается на технологии Token Ring (рис. 5.32).

Технология Fiber Distributed Data Interface имеет характеристики:

- метод доступа — специфический вариант маркерного метода доступа (Token Ring, но с другой реализацией стандарта IEEE 802.5);
- максимальное расстояние между соседними станциями — не более 2 км; многомодовый ВОЛС, для UTP — 100 м;
- топология — ЛВС кольцевой структуры;
- среда передачи — ВОЛС, UTP cat 5e;
- скорость передачи данных — 100 Мбит/с;
- максимальное число узлов в кольце — 500 с двойным подключением;
- максимальный диаметр двойного кольца — 100 км (одинарного —200 км).

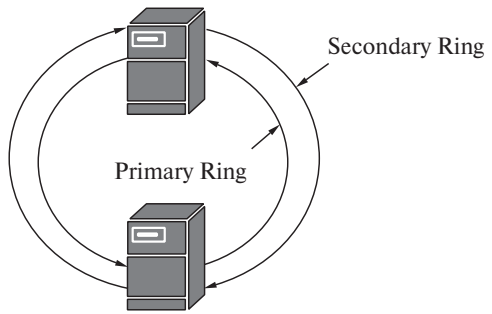


Рис. 5.32. Кольца ВОЛС в сети FDDI

Основная область применения сетей FDDI — опорная (магистральная) сеть, связывающая подсети отдельных подразделений предприятий. Средняя цена на один узел составляет приблизительно 3000 долл.

Сеть FDDI обычно используется как объединяющая в единую сеть много отдельных подсетей ЛВС. Например, при организации информационной системы крупного предприятия целесообразно иметь ЛВС типа Ethernet или Token Ring в помещениях отдельных проектных подразделений, а связь между подразделениями осуществлять через сеть FDDI. Скорость 10 Мбит/с для ЛВС типа Ethernet или Token Ring недостаточна для многих современных применений

сетей. Поэтому разрабатываются технологии и конкретные реализации высокоскоростных ЛВС.

В основном варианте сети применено двойное кольцо на ВОЛС с длиной волны 1300 нм. Кольцо выполняется в виде двух оптоволоконных жил, которые передают информацию в двух противоположных направлениях (таким образом, фактическая пропускная способность — 200 Мбит/с).

Станции можно подключать к одному из колец или к обоим сразу. Два кольца ВОЛС используются одновременно. Использование конкретным узлом обоих колец позволяет для этого узла иметь суммарную пропускную способность в 200 Мбит/с. Другое возможное использование второго кольца — обход поврежденного участка (рис. 5.33).

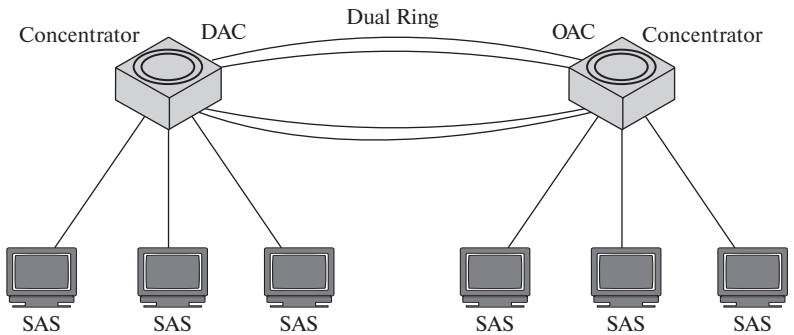


Рис. 5.33. Использование двух колец ВОЛС

FDDI устанавливает применение двойных кольцевых сетей. Трафик по этим кольцам движется в противоположных направлениях. В физическом выражении кольцо состоит из двух или более двухточечных соединений между смежными станциями. Одно из двух колец FDDI называется первичным кольцом, другое — вторичным кольцом. Первичное кольцо используется для передачи данных, в то время как вторичное кольцо обычно является дублирующим.

«Станции Класса B» или «станции, подключаемые к одному кольцу» (SAS) подсоединены к одной кольцевой сети; «станции класса A» или «станции, подключаемые к двум кольцам» (DAS) подсоединены к обеим кольцевым сетям. SAS подключены к первичному кольцу через «концентратор», который обеспечивает связи для множества SAS. Концентратор отвечает за то, чтобы отказ или отключение питания в любой из SAS не прерывали кольцо. Это особенно необходимо, когда к кольцу подключен

PC или аналогичные устройства, у которых питание часто включается и выключается.

В обычном режиме данные передаются только по всем СУ и всем участкам кабеля первичного (Primary) кольца — режим Thru (сквозной или транзитный). В случае обрыва кабеля или выхода из строя СУ задействуется вторичное (Secondary) кольцо, с замыканием которого с первичным восстанавливается кольцевой режим работы ЛВС (Wrap).

Технология FDDI имеет процедуры определения неисправностей в сети (аналогичные технологии Token Ring) и ее реконфигурирования путем передачи данных по резервному кольцу. При этом может полностью восстанавливаться работоспособность сети в случае возникновения единичных отказов ее элементов. В случае множественных отказов сеть распадается на несколько несвязанных сетей.

FDDI поддерживает распределение полосы пропускания сети в масштабе реального времени, что является идеальным для ряда различных типов прикладных задач. FDDI обеспечивает эту поддержку путем обозначения двух типов трафика: синхронного и асинхронного. Синхронный трафик может потреблять часть общей полосы пропускания сети FDDI, равную 100 Mb/сек; остальную часть может потреблять асинхронный трафик. Синхронная полоса пропускания выделяется тем станциям, которым необходима постоянная возможность передачи. Например, наличие такой возможности помогает при передаче голоса и видеоинформации. Другие станции используют остальную часть полосы пропускания асинхронно. Спецификация SMT для сети FDDI определяет схему распределенных заявок на выделение полосы пропускания FDDI.

Распределение асинхронной полосы пропускания производится с использованием восьмиуровневой схемы приоритетов. Каждой станции присваивается определенный уровень приоритета пользования асинхронной полосой пропускания. FDDI также разрешает длительные диалоги, когда станции могут временно использовать всю асинхронную полосу пропускания. Механизм приоритетов FDDI может фактически блокировать станции, которые не могут пользоваться синхронной полосой пропускания и имеют слишком низкий приоритет пользования асинхронной полосой пропускания.

В FDDI используются оригинальные код и метод доступа.

Применяется код типа NRZ (без возвращения к нулю), в котором изменение полярности в очередном такте времени воспринимается как 1, отсутствие изменения полярности как 0. Чтобы код был само-

синхронизирующимся, после каждых четырех битов передатчик вырабатывает синхронизирующий перепад.

Такое специальное манчестерское кодирование носит название 4b/5b. Запись 4b/5b означает код, в котором для самосинхронизации при передаче 4 бит двоичного кода используется 5 бит так, что не может быть более двух нулей подряд или после 4 бит добавляется еще один обязательный перепад, что и используется в FDDI. При таком коде несколько усложняются блоки кодирования и декодирования, но зато повышается скорость передачи по линии связи, так как почти вдвое уменьшается максимальная частота переключения по сравнению с манчестерским кодом.

Кольца в технологии FDDI рассматриваются как общая разделяемая среда, для которой определен детерминированный маркерный метод доступа (аналогичный методам доступа в сетях Token Ring).

В соответствии с методом доступа в сетях FDDI по кольцу циркулирует пакет, состоящий из маркера и информационных кадров. Любая станция, готовая к передаче, распознав проходящий через нее пакет, вписывает свой кадр в конец пакета. Она же ликвидирует его после того, как кадр вернется к ней после оборота по кольцу и при условии, что он был правильно воспринят получателем. Если обмен происходит без сбоев, то кадр, возвращающийся к станции-отправителю, оказывается в пакете уже первым, так как все предшествующие кадры должны быть ликвидированы раньше.

Формат кадра FDDI

Форматы блока данных FDDI (рис. 5.34) аналогичны форматам Token Ring.

PA	SD	FC	DA	SA	PDU	FCS	ED/FS
16 бит	8 бит	8 бит	48 бит	48 бит	до 4478x8 бит	32 бита	16 бит

Рис. 5.34. Формат кадра FDDI

Preamble (PA) — заголовок подготавливает каждую станцию для приема прибывающего блока данных.

Start Delimitter (SD) — ограничитель начала указывает на начало блока данных. Он содержит сигнальные структуры, которые отличают его от остальной части блока данных.

Frame control (FC) — поле управления блоком данных указывает на размер адресных полей, на вид данных, содержащихся в блоке (синхронная или асинхронная информация), и на другую управляющую информацию.

Destination address (DA), Source address (SA) — так же, как у Ethernet и Token Ring, размер адресов равен 6 байтам. Поле адреса назначения может содержать односоставный (единственный), многосоставный (групповой) или широковещательный (все станции) адрес, в то время как адрес источника идентифицирует только одну станцию, отправившую блок данных.

Protocol data unit (PDU) — информационное поле содержит либо информацию, предназначенную для протокола высшего уровня, либо управляющую информацию.

Frame check sequence (FCS) — так же, как у Token Ring и Ethernet, поле проверочной последовательности блока данных (FCS) заполняется величиной «проверки избыточности цикла» (CRC), зависящей от содержания блока данных, которую вычисляет станция-источник. Станция пункта назначения пересчитывает эту величину, чтобы определить наличие возможного повреждения блока данных при транзите. Если повреждение имеется, то блок данных отбрасывается.

End delimiter (ED) — ограничитель конца содержит неинформационные символы, которые означают конец блока данных.

Frame status (FS) — поле состояния блока данных позволяет станции источника определять, не появилась ли ошибка и был ли блок данных признан и скопирован принимающей станцией.

Отличия маркерного метода доступа FDDI от Token Ring:

- для асинхронного трафика (не критичен к небольшим задержкам в передаче кадров) время удержания маркера в сети — величина переменная и зависит от загрузки сети: при небольшой загрузке оно увеличивается, а при перегрузках уменьшается — вплоть до 0;
- для синхронного трафика время удержания маркера в сети по-прежнему — величина постоянная;
- отсутствует механизм приоритетов кадров;
- трафик делится на два уровня (синхронный и асинхронный) в отличие от восьми уровней.

На MAC-уровне пересылка кадров в сетях FDDI совпадает с пересылкой кадров в сетях Token Ring. Фомат MAC- адресов полностью соответствует стандарту IEEE 802.

Отличительной особенностью технологии FDDI является наличие уровня управления станцией SMT (Station Manegment). Этот уровень выполняет все функции управления и мониторинга всех

уровней протокольного стека. Так как в управлении сетью принимают участие все СУ, то они обмениваются кадрами SMT.

Структура протоколов технологии FDDI показана в табл. 5.14.

Таблица 5.14

<table>
<tr><td>7</td><td>Прикладной</td><td colspan="4" rowspan="5">LLC 802.2</td></tr>
<tr><td>6</td><td>Представительский</td></tr>
<tr><td>5</td><td>Сеансовый</td></tr>
<tr><td>4</td><td>Транспортный</td></tr>
<tr><td>3</td><td>Сетевой</td></tr>
<tr><td>2</td><td>Канальный</td><td></td><td>MAC</td><td></td><td rowspan="3">SMT</td></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Физический</td><td rowspan="2"></td><td>PHY</td><td></td></tr>
<tr><td>PMD</td><td></td></tr>
</table>

Достоинства:

- высокая скорость передачи данных;
- высокая отказоустойчивость по сравнению с другими технологиями ЛВС (за счет стандартных процедур восстановления после отказа — повреждение кабеля, ошибка в работе СУ или концентратора, большой уровень помех в МК);
- максимально эффективное использование пропускной способности МК ЛВС как для асинхронного, так и для синхронного (чувствительного к задержкам) трафика сети;
- высокие показатели гарантированной доставки за счет маркерного метода доступа;
- маркерный метод доступа для асинхронного трафика адаптивен к загрузке сети и хорошо регулирует временные перегрузки.

Недостатки:

- сложность масштабирования (подключения/отключения СУ) ЛВС;
- невысокая безопасность передачи информации.

5.7. Сравнение различных сетевых технологий

Сравнение различных сетевых технологий представлено в табл. 5.15.

Таблица 5.15

Параметр	PolyNet (Cambridge Ring)	ArcNet	Token Ring	Ethernet 10 Base	Fast Ethernet 100 Base	Giga Ethernet 1000 Base	100 VG-AnyLAN	FDDI
Топология	Кольцо	Шина	Звезда/кольцо	Шина/звезда			Шина/звезда	Двойное кольцо деревьев
Скорость	10	2,5, 25	4, 16	10	100	1000	100	100
Среда передачи	COAX 50	COAX 75, 93, 100 UTP	COAX, UTP, STP	COAX 50, UTP 3,4,5, STP	UTP 3,4,5, STP, FO	UTP 5, STP, FO	UTP 3,4,5, STP, FO	UTP 5, STP, FO
Метод доступа к МК	Метод зазора (кольцевых слотов) ISO/DIS 8802/7	Маркерный метод доступа (Token Bus) ieee 802.4	Маркер в шине и маркер в кольце ieee 802.5	Случайный метод доступа с контролем несущей и обнаружением коллизии МДКН/ОК (CSMA/CD) стандарт IEEE 802.			Метод приоритетных запросов	Маркерный метод доступа IEEE 802.5
Длина кадра	42, 58, 74, 82 бит	516 байт	1–8 Кбайт	72–1526 байт				28–4528 байт
Максимальное число СУ в сети	256	254	96/260	COAX 30 COAX 100 UTP 1024 FO 1024				500

Окончание табл. 5.17

Параметр	PolyNet (Cambridge Ring)	ArcNet	Token Ring	Ethernet 10 Base	Fast Ethernet 100 Base	Giga Ethernet 1000 Base	100 VG-AnyLAN	FDDI
Структуризация ЛВС	Репитер	Хаб 9 последовательно	Концентратор MAU (до 12 портов) 12/3 MAU в кольце	Репитеры, концентраторы, коммутаторы, маршрутизаторы. Допустимо 5 сегментов сети (2 ненагруженных). Каскадно не более 4 концентраторов			Каскадно не более 2 концентраторов	
Максимальная длина сети (без мостов)	400 м	COAX 60–70 м	COAX 150/380 м	COAX 185 м COAX 500 м UTP 2,5 км FO 2 км	UTP 250 м FO 412 м	UTP 10–100 м FO 25–550 м	250 м	
Максимальная длина сети (с мостами)		COAX 6 км	COAX 150/380 м	COAX 1 км COAX 2,5 км UTP 2,5 км FO 2,5 км	UTP 500 м FO 1 км	UTP 500 м FO 1 км	375 м	200 км
Максимальное расстояние между СУ		COAX 70 м для 8 СУ	COAX 45/100 м					2 км

5.8. Контрольные вопросы

1. **Какая спецификация Ethernet рекомендована в качестве магистральной (backbone) технологии?**
   а) 10BASE-T;
   б) 100BASE-TX;
   в) 100BASE-FX;
   г) 1000BASE-LX.
2. **Что описывает технологию Gigabit Ethernet? (Выберите два ответа.)**
   а) функционирует со скоростью 100 Мбит/с;
   б) обычно используется в качестве магистральной (backbone) среды;
   в) требуется экранированная витая пара;
   г) используется оптическая (или медная) среда передачи;
   д) обычно используется в качестве среды между рабочими станциями.
3. **Какой уровень OSI модели делает различие между Ethernet, Fast Ethernet и Gigabit Ethernet?**
   а) physical layer;
   б) data link layer;
   в) network layer;
   г) transport layer.
4. **Как 1000BASE-T использует пары кабеля UTP для обмена данными?**
   а) две пары использует для передачи и две пары для приема;
   б) одна пара — для передачи, одна для приема, и две пары — двунаправленные;
   в) все четыре пары используются для передачи и приема одновременно;
   г) две пары используют спецификацию 10BASE-T и две пары — 100BASE-TX.
5. **Какая спецификация использует UTP? (Выберите два ответа.)**
   а) 10Base-T;
   б) 10Base-5;
   в) 100Base-FX;
   г) 100Base-TX;
   д) 100Base-5-T;
   е) 10Base-FB.
6. **Каково максимальное расстояние передачи данных при использовании 1000Base-T?**
   а) 90 м;
   б) 100 м;
   в) 500 м;
   г) 2000 м;
   д) 5000 м;
   е) 40 000 м.

7. **Спецификация 100Base-FX предусматривает работу по двум волокнам оптического кабеля:**
   а) многомодового кабеля только в полудуплексном режиме;
   б) многомодового кабеля в полудуплексном или полнодуплексном режиме;
   в) одномодового кабеля в полнодуплексном режиме;
   г) одномодового кабеля в полудуплексном или полнодуплексном режиме.
8. **В какой технологии не используется метод доступа CSMA/CD в полудуплексном режиме?**
   а) Ethernet;
   б) FastEthernet;
   в) GigabitEthernet;
   г) 10 GigabitEthernet;
   д) во всех.
9. **Технология 10GbE регламентируется стандартом:**
   а) 802.3;
   б) 802.3u;
   в) 802.3z;
   г) 802.3ab;
   д) 802.3ae.
10. **Технология Gigabit Ethernet регламентируется стандартом: (Дать 2 ответа.)**
    а) 802.3;
    б) 802.3u;
    в) 802.3z;
    г) 802.3ab;
    д) 802.3ae.
11. **Технология Fast Ethernet регламентируется стандартом: (Дать 2 ответа.)**
    а) 802.3;
    б) 802.3u;
    в) 802.3z;
    г) 802.3ab;
    д) 802.3ae.
12. **Связь на расстояние до 40 км обеспечивает спецификация:**
    а) 1000 Base-LX;
    б) 10GBase-ER;
    в) 1000Base-SX;
    г) 10GBase-LX4;
    д) 100Base-FX.
13. **Что представляет собой устройство множественного доступа MSAU?**
14. **Нарисовать структуру и описать функционирование ЛВС TokenRing на основе одного и нескольких MSAU.**
15. **В чем отличие физической топологии ЛВС TokenRing от логической?**
16. **Нарисовать и пояснить структуру ЛВС FDDI.**
17. **Пояснить на рисунке принцип реорганизации ЛВС FDDI при обрыве в кабеле и при отказе рабочей станции.**

Раздел 6
СЕМЕЙСТВО ПРОТОКОЛОВ TCP/IP

6.1. Общие сведения о семействе TCP/IP

Протоколы TCP/IP являются основными протоколами сети Интернет, они поддерживаются операционными системами Unix и Windows NT.

Эти протоколы берут свое начало от одной из первых территориальных сетей ARPANET. Они получили широкое распространение благодаря реализации в ОС Unix и в сети Интернет и в настоящее время оформлены в виде стандартов RFC (Requests For Comments) организацией IETF (Internet Engineering Task Force).

TCP/IP — сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. В модели предполагается прохождение информации через четыре уровня, каждый из которых описывается правилом (протоколом передачи). Наборы правил, решающих задачу по передаче данных, составляют стек протоколов передачи данных, на которых базируется Интернет. Название TCP/IP происходит из двух важнейших протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые первыми были разработаны и описаны в данном стандарте. Также изредка упоминается как модель DOD в связи с историческим происхождением от сети ARPANET из 1970-х гг. (под управлением DARPA, Министерства обороны США).

Набор интернет-протоколов — это концептуальная модель и набор коммуникационных протоколов, используемых в Интернете и подобных компьютерных сетях. Он широко известен как TCP/IP, поскольку базовые протоколы в пакете — это протокол управления передачей (TCP) и интернет-протокол (IP). Его иногда называют моделью Министерства обороны (МО), поскольку разработка сетевого метода финансировалась Министерством обороны Соединенных Штатов через DARPA.

Набор интернет-протоколов обеспечивает сквозную передачу данных, определяющую, как данные должны пакетироваться, обрабатываться, передаваться, маршрутизироваться и приниматься. Эта функциональность организована в четыре слоя абстракции, которые

классифицируют все связанные протоколы в соответствии с объемом задействованных сетей. От самого низкого до самого высокого уровня — это уровень связи, содержащий методы связи для данных, которые остаются в пределах одного сегмента сети (ссылка); интернет-уровень, обеспечивающий межсетевое взаимодействие между независимыми сетями; транспортный уровень, обрабатывающий связь между хостами; и прикладной уровень, который обеспечивает обмен данными между процессами для приложений.

Технические стандарты, определяющие набор протоколов Интернета и многие из его составляющих протоколов, поддерживаются Целевой группой по разработке Интернета (IETF). Набор интернет-протоколов предшествует модели OSI, более всеобъемлющей базовой базой для общих сетевых систем.

Стек протоколов TCP/IP был создан на основе NCP (Network Control Protocol) группой разработчиков под руководством Винтона Серфа в 1972 г. В июле 1976 г. Винт Серф и Боб Кан впервые продемонстрировали передачу данных с использованием TCP по трем различным сетям. Пакет прошел по следующему маршруту: Сан-Франциско — Лондон — Университет Южной Калифорнии. В конце своего путешествия пакет проделал 150 тыс. км, не потеряв ни одного бита. В 1978 г. Серф, Джон Постел и Дэнни Кохэн решили выделить в TCP две отдельные функции: TCP и IP (англ. Internet Protocol — межсетевой протокол). TCP был ответственен за разбивку сообщения на датаграммы (англ. datagram) и соединение их в конечном пункте отправки. IP отвечал за передачу (с контролем получения) отдельных датаграмм. Вот так родился современный протокол Интернета. А 1 января 1983 г. ARPANET перешла на новый протокол. Этот день принято считать официальной датой рождения Интернета.

Стек протоколов TCP/IP включает в себя четыре уровня:

- прикладной уровень (application layer);
- транспортный уровень (transport layer);
- сетевой уровень (межсетевой) (Internet layer);
- канальный уровень (link layer).

Протоколы этих уровней полностью реализуют функциональные возможности модели OSI. На стеке протоколов TCP/IP построено все взаимодействие пользователей в IP-сетях. Стек является независимым от физической среды передачи данных, благодаря чему, в частности, обеспечивается полностью прозрачное взаимодействие между проводными и беспроводными сетями.

Распределение протоколов по уровням модели TCP/IP

Распределение протоколов по уровням модели TCP/IP представлено в табл. 6.1.

Таблица 6.1

Прикладной (Application layer)	Например, HTTP, RTSP, FTP, DNS
Транспортный (Transport layer)	Например, TCP, UDP, SCTP, DCCP (RIP, протоколы маршрутизации, подобные OSPF, что работают поверх IP, являются частью сетевого уровня)
Сетевой (Межсетевой) (Internet layer)	Для TCP/IP это IP (вспомогательные протоколы, вроде ICMP и IGMP, работают поверх IP, но тоже относятся к сетевому уровню; протокол ARP является самостоятельным вспомогательным протоколом, работающим поверх канального уровня)
Канальный (Link layer)	Ethernet, IEEE 802.11WLAN, SLIP, Token Ring, ATM и MPLS, физическая среда и принципы кодирования информации, T1, E1

Прикладной уровень

На прикладном уровне (Application layer) работает большинство сетевых приложений.

Эти программы имеют свои собственные протоколы обмена информацией, например, интернет-браузер для протокола HTTP, ftp-клиент для протокола FTP (передача файлов), почтовая программа для протокола SMTP (электронная почта), SSH (безопасное соединение с удаленной машиной), DNS (преобразование символьных имен в IP-адреса) и многие другие.

В массе своей эти протоколы работают поверх TCP или UDP и привязаны к определенному порту, например:

HTTP на TCP-порт 80 или 8080;

- FTP на TCP-порт 20 (для передачи данных) и 21 (для управляющих команд);
- SSH на TCP-порт 22;
- запросы DNS на порт UDP (реже TCP) 53;
- обновление маршрутов по протоколу RIP на UDP-порт 520.

Эти порты определены Агентством по выделению имен и уникальных параметров протоколов (IANA).

К этому уровню относятся: Echo, Finger, Gopher, HTTP, HTTPS, IMAP, IMAPS, IRC, NNTP, NTP, POP3, POPS, QOTD, RTSP, SNMP, SSH, Telnet, XDMCP.

Транспортный уровень

Протоколы транспортного уровня (Transport layer) могут решать проблему негарантированной доставки сообщений («дошло ли сообщение до адресата?»), а также гарантировать правильную последовательность прихода данных. В стеке TCP/IP транспортные протоколы определяют, для какого именно приложения предназначены эти данные.

Протоколы автоматической маршрутизации, логически представленные на этом уровне (поскольку работают поверх IP), на самом деле являются частью протоколов сетевого уровня; например OSPF (IP идентификатор 89).

TCP (IP идентификатор 6) — «гарантированный» транспортный механизм с предварительным установлением соединения, предоставляющий приложению надежный поток данных, дающий уверенность в безошибочности получаемых данных, перезапрашивающий данные в случае потери и устраняющий дублирование данных. TCP позволяет регулировать нагрузку на сеть, а также уменьшать время ожидания данных при передаче на большие расстояния. Более того, TCP гарантирует, что полученные данные были отправлены точно в такой же последовательности. В этом его главное отличие от UDP.

UDP (IP идентификатор 17) протокол передачи датаграмм без установления соединения. Также его называют протоколом «ненадежной» передачи, в смысле невозможности удостовериться в доставке сообщения адресату, а также возможного перемешивания пакетов. В приложениях, требующих гарантированной передачи данных, используется протокол TCP.

UDP обычно используется в таких приложениях, как потоковое видео и компьютерные игры, где допускается потеря пакетов, а повторный запрос затруднен или не оправдан, либо в приложениях вида запрос–ответ (например, запросы к DNS), где создание соединения занимает больше ресурсов, чем повторная отправка.

И TCP, и UDP используют для определения протокола верхнего уровня число, называемое портом.

Сетевой уровень

Межсетевой уровень (Internet layer) изначально разработан для передачи данных из одной сети в другую. На этом уровне работают маршрутизаторы, которые перенаправляют пакеты в нужную сеть путем расчета адреса сети по маске сети. Примерами такого протокола является X.25 и IPC в сети ARPANET.

С развитием концепции глобальной сети в уровень были внесены дополнительные возможности по передаче из любой сети в любую сеть, независимо от протоколов нижнего уровня, а также возможность запрашивать данные от удаленной стороны, например в протоколе ICMP (используется для передачи диагностической информации IP-соединения) и IGMP (используется для управления multicast-потоками).

ICMP и IGMP расположены над IP и должны попасть на следующий — транспортный — уровень, но функционально являются протоколами сетевого уровня, и поэтому их невозможно вписать в модель OSI.

Пакеты сетевого протокола IP могут содержать код, указывающий, какой именно протокол следующего уровня нужно использовать, чтобы извлечь данные из пакета. Это число — уникальный IP-номер протокола. ICMP и IGMP имеют номера соответственно 1 и 2.

К этому уровню относятся: DVMRP, ICMP, IGMP, MARS, PIM, RIP, RIP2, RSVP.

Канальный уровень

Канальный уровень (Link layer) описывает способ кодирования данных для передачи пакета данных на физическом уровне (т.е. специальные последовательности бит, определяющих начало и конец пакета данных, а также обеспечивающие помехоустойчивость). Ethernet, например, в полях заголовка пакета содержит указание того, какой машине или машинам в сети предназначен этот пакет.

Примеры протоколов канального уровня — Ethernet, IEEE 802.11 WLAN, SLIP, Token Ring, ATM и MPLS.

PPP не совсем вписывается в такое определение, поэтому обычно описывается в виде пары протоколов HDLC/SDLC.

MPLS занимает промежуточное положение между канальным и сетевым уровнем, и, строго говоря, его нельзя отнести ни к одному из них.

Канальный уровень иногда разделяют на два подуровня — LLC и MAC.

Кроме того, канальный уровень описывает среду передачи данных (будь то коаксиальный кабель, витая пара, оптическое волокно или радиоканал), физические характеристики такой среды и принцип передачи данных (разделение каналов, модуляцию, амплитуду сигналов, частоту сигналов, способ синхронизации передачи, время ожидания ответа и максимальное расстояние).

При проектировании стека протоколов на канальном уровне рассматривают помехоустойчивое кодирование, позволяющее обнаруживать и исправлять ошибки в данных вследствие воздействия шумов и помех на канал связи.

Сравнение с моделью OSI

Три верхних уровня в модели OSI, т.е. уровень приложения, уровень представления и уровень сеанса, отдельно не различаются в модели TCP/IP, которая имеет только прикладной уровень над транспортным уровнем. Хотя некоторые чистые приложения протокола OSI, такие как X.400, также объединяют их, нет требования, чтобы стек протокола TCP/IP накладывал монолитную архитектуру над транспортным уровнем. Например, протокол NFS-приложений работает через протокол представления данных External Data Representation (XDR), который, в свою очередь, работает по протоколу Remote Procedure Call (RPC). RPC обеспечивает надежную передачу данных, поэтому он может безопасно использовать транспорт UDP с максимальным усилием.

Различные авторы интерпретировали модель TCP/IP по-разному и не согласны с тем, что уровень связи или вся модель TCP/IP охватывает проблемы уровня OSI уровня 1 (физический уровень) или предполагается, что аппаратный уровень ниже уровня канала.

Несколько авторов попытались включить слои 1 и 2 модели OSI в модель TCP/IP, поскольку они обычно упоминаются в современных стандартах (например, IEEE и ITU). Это часто приводит к модели с пятью слоями, где уровень связи или уровень доступа к сети разделяются на слои 1 и 2 модели OSI.

Усилия по разработке протокола IETF не касаются строгого расслоения. Некоторые из его протоколов могут не соответствовать чисто модели OSI, хотя RFC иногда ссылаются на нее и часто используют старые номера уровня OSI. IETF неоднократно заявлял, что разработка интернет-протокола и архитектуры не должна соответствовать требованиям OSI. В RFC 3439, адресованном интернет-архитектуре, содержится раздел, озаглавленный «Слой, считающийся вредным».

Например, считается, что уровни сеанса и представления пакета OSI включены в прикладной уровень пакета TCP/IP. Функциональность уровня сеанса можно найти в протоколах, таких как HTTP и SMTP, и более очевидна в таких протоколах, как Telnet и протокол инициации сеанса (SIP). Функциональность уровня сеанса также

реализована с нумерацией портов протоколов TCP и UDP, которые охватывают транспортный уровень в наборе TCP/IP. Функции уровня представления реализуются в приложениях TCP/IP со стандартом MIME при обмене данными.

Конфликты очевидны также в оригинальной модели OSI, ISO 7498, когда не рассматриваются приложения к этой модели, например ISO 7498/4 Management Framework или ISO 8648 Internal Organization of the Network layer (IONL). Когда рассматриваются документы IONL и Management Framework, ICMP и IGMP определяются как протоколы управления уровнем для сетевого уровня. Аналогичным образом IONL предоставляет структуру для «зависимых от подсетей объектов конвергенции», таких как ARP и RARP.

Протоколы IETF могут быть инкапсулированы рекурсивно, о чем свидетельствуют протоколы туннелирования, такие как Инкапсуляция общей маршрутизации (GRE). GRE использует тот же механизм, который OSI использует для туннелирования на сетевом уровне. Существуют разногласия в том, как вписать модель TCP/IP в модель OSI, поскольку уровни в этих моделях не совпадают.

К тому же модель OSI не использует дополнительный уровень — «Internetworking» — между канальным и сетевым уровнями. Примером спорного протокола может быть ARP или STP.

Традиционно протоколы TCP/IP вписываются в модель OSI следующим образом (табл. 6.2).

Таблица 6.2

Распределение протоколов по уровням модели OSI

	TCP/IP	OSI	
7	Прикладной	Прикладной	Например, HTTP, SMTP, SNMP, FTP, Telnet, SSH, SCP, SMB, NFS, RTSP, BGP
6		Представительский	Например, XDR, AFP, TLS, SSL
5		Сеансовый	Например, ISO 8327 / CCITT X.225, RPC, NetBIOS, PPTP, L2TP, ASP
4	Транспортный	Транспортный	Например, TCP, UDP, SCTP, SPX, ATP, DCCP, GRE
3	Сетевой	Сетевой	Например, IP, ICMP, IGMP, CLNP, OSPF, RIP, IPX, DDP, ARP

Окончание табл. 6.2

	TCP/IP	OSI	
2	Канальный	Канальный	Например, Ethernet, Token ring, HDLC, PPP, X.25, Frame relay, ISDN, ATM, SPB, MPLS
1		Физический	Например, электрические провода, радиосвязь, волоконно-оптические провода, инфракрасное излучение

Обычно в стеке TCP/IP верхние три уровня модели OSI (прикладной, представительский и сеансовый) объединяют в один — прикладной. Поскольку в таком стеке не предусматривается унифицированный протокол передачи данных, функции по определению типа данных передаются приложению.

6.2. Протоколы физического/канального (MAC) уровня протокольного стека TCP/IP

На канальном и физическом уровне используются либо протоколы локальных сетей, либо модемные протоколы (в порядке их исторического появления):

- SLIP (Serial Line IP). Имеет очень большие накладные расходы (на 1 информационный байт приходится 40 байт служебной информации). Обеспечивает передачу отдельного байта в сети и рассчитан на один виртуальный канал;
- CLIP (Compressed Line IP). Позволяет передавать 1 байт полезной информации, обрамленный тремя служебными байтами. Поддерживает до 16 виртуальных TCP-соединений.

  Протоколы SLIP и CLIP относятся к асинхронным протоколам;
- PPP (Point To Point Protocol). Обеспечивает мультиплексированное соединение, коррекцию ошибок, динамическое определение IP-адреса (он назначается другим СУ). Поддерживаются и синхронный и асинхронный способы передачи.

На двух нижних уровнях используются одни и те же стандартизированные протоколы Ethernet(802.3), FDDI, TokenRing(802.5), Fast Ethernet, SLIP,100VG-AnyLAN, ATM, PPP, X.25, LAP-B(-D) и др. и физические каналы (коаксиал, экр./неэкр. витая пара, оптоволокно, радиоволны, ИК и др.). Это позволяет использовать унифицированное сетевое оборудование.

6.3. Сетевой протокол IP в стеке протоколов TCP/IP

Internet Protocol (IP, досл. «межсетевой протокол») — маршрутизируемый протокол сетевого уровня стека TCP/IP. Именно IP стал тем протоколом, который объединил отдельные компьютерные сети во всемирную сеть Интернет. Неотъемлемой частью протокола является адресация сети.

IP объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети через произвольное число промежуточных узлов (маршрутизаторов). Он классифицируется как протокол сетевого уровня по сетевой модели OSI. IP не гарантирует надежной доставки пакета до адресата — в частности, пакеты могут прийти не в том порядке, в котором были отправлены, продублироваться (приходят две копии одного пакета), оказаться поврежденными (обычно поврежденные пакеты уничтожаются) или не прийти вовсе. Гарантию безошибочной доставки пакетов дают некоторые протоколы более высокого уровня — транспортного уровня сетевой модели OSI, например TCP, которые используют IP в качестве транспорта.

Протокол IP — это дейтаграммный сетевой протокол без установления соединения.

Его функции:

- фрагментация и сборка пакетов при прохождении через промежуточные сети, имеющие другие протоколы;
- маршрутизация;
- проверка контрольной суммы заголовка пакета (правильность передачи всего пакета проверяется на транспортном уровне, т.е. с помощью TCP, в оконечном узле);
- управление потоком — сброс дейтаграмм при превышении заданного времени жизни.

При доставке IP-пакета он проходит через разные каналы доставки. Возможно возникновение ситуации, когда размер пакета превысит возможности узла системы связи. В этом случае протокол предусматривает возможность дробления пакета на уровне IP в процессе доставки. Соответственно, к конечному получателю пакет придет в виде нескольких пакетов, которые необходимо собрать в один перед дальнейшим анализом. Возможность дробления пакета с последующей сборкой называется IP-фрагментацией.

В протоколе предусмотрена возможность запрещения фрагментации конкретного пакета. Если такой пакет нельзя передать через сегмент связи целиком, то он уничтожается, а отправителю направляется ICMP-сообщение о проблеме.

В современной сети Интернет используется IP четвертой версии, также известный как IPv4. В протоколе IP этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 4 октета (4 байта). При этом компьютеры в подсетях объединяются общими начальными битами адреса. Количество этих бит, общее для данной подсети, называется маской подсети (ранее использовалось деление пространства адресов по классам — A, B, C; класс сети определялся диапазоном значений старшего октета и определял число адресуемых узлов в данной сети, сейчас используется бесклассовая адресация).

В настоящее время вводится в эксплуатацию шестая версия протокола — IPv6, которая позволяет адресовать значительно большее количество узлов, чем IPv4. Эта версия отличается повышенной разрядностью адреса, встроенной возможностью шифрования и некоторыми другими особенностями. Переход с IPv4 на IPv6 связан с трудоемкой работой операторов связи и производителей программного обеспечения и не может быть выполнен одномоментно. К осени 2013 г. в Интернете присутствовало более 14 тыс. сетей, работающих по протоколу IPv6. Для сравнения: к середине 2010 г. в адресном пространстве IPv4 присутствовало более 320 тыс. сетей, но в IPv6 сети гораздо более крупные, нежели в IPv4.

6.3.1. IPv4

IPv4 (англ. Internet Protocol version 4) — четвертая версия интернет-протокола (IP). Первая широко используемая версия. Протокол описан в RFC 791 (сентябрь 1981 г.), заменившем RFC 760 (январь 1980 г.).

IPv4 использует 32-битные (четырехбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (232) возможными уникальными адресами.

Традиционной формой записи IPv4 адреса является запись в виде четырех десятичных чисел (от 0 до 255), разделенных точками, как показано в табл. 6.3. Через дробь указывается длина маски подсети.

Таблица 6.3

Форма записи	Пример	Преобразование из десятичной нотации с точками
Десятичная с точками	192.0.2.235	—
Шестнадцатеричная с точками	0xC0.0x00.0x02.0xEB	Каждый октет преобразуется в шестнадцатеричную форму

Окончание табл. 6.3

Форма записи	Пример	Преобразование из десятичной нотации с точками
Восьмеричная с точками	0300.0000.0002.0353	Каждый октет преобразуется в восьмеричную форму
Шестнадцатеричная	0xC00002EB	Конкатенация октетов из шестнадцатеричной нотации с точками
Десятичная	3221226219	32-битное число в десятичной форме
Восьмеричная	030000001353	32-битное число в восьмеричной форме

Некоторые адреса IPv4 зарезервированы для специальных целей и не предназначены для глобальной маршрутизации. Список подсетей специального назначения определен RFC 6890, некоторые из них показаны в табл. 6.4.

Таблица 6.4

Подсети IPv4

Подсеть	Назначение	Маршрутизация
0.0.0.0/8	Адреса источников пакетов «этой» («своей») сети	Запрещена
0.0.0.0/32	В сокетах с состоянием «listening» обозначает любые IP отправителя или любые сети получателя на текущем хосте. Может посылаться в сеть только в качестве адреса источника, если хосту еще не назначен IP-адрес (обычно по протоколу DHCP). Не может быть использован как адрес назначения в сети. В маршрутизаторах Cisco при попытке отправить пакет на адрес 0.0.0.0 он будет отправлен на широковещательный адрес наименьшей подсоединенной подсети (connected в таблице маршрутизации)	Запрещена

Продолжение табл. 6.4

Подсеть	Назначение	Маршрутизация
10.0.0.0/8	Для использования в частных сетях	Только в частных сетях
100.64.0.0/10	Shared Address Space. RFC 6598. Для использования в сетях сервис-провайдера	
127.0.0.0/8	Подсеть для коммуникаций внутри хоста (см. localhost). Используется сетевая подсистема, но в действительности такие пакеты не проходят через сетевую карту. Если пакет с таким адресом назначения был получен из сети, то должен быть отброшен	Запрещена
169.254.0.0/16	Канальные адреса. Подсеть используется для автоматического назначения IP операционной системой в случае, если настроено получение адреса по DHCP, но ни один сервер не отвечает	Только в частных сетях
172.16.0.0/12	Для использования в частных сетях	Только в частных сетях
192.0.0.0/24	IETF Protocol Assignments	
192.0.0.0/29	Dual-Stack Lite (DS-Lite). RFC 6333. IPv6 transition mechanisms	
192.0.0.170/32	NAT64	
192.0.0.171/32	DNS64	
192.0.2.0/24[7]	Для примеров в документации	Запрещена
192.88.99.0/24[1]	Используются для рассылки ближайшему узлу. RFC 3068	Глобально разрешена
192.88.99.1/32	Применяется в качестве ретранслятора при инкапсуляции IPv6 в IPv4 (6to4). Иными словами, этот IP не уникален. Его анонсируют многие компании. Пакет на этот адрес пойдет до ближайшего хоста с этим IP, который распакует пакет и отправит его дальше по IPv6 маршрутизации	Глобально разрешена

Окончание табл. 6.4

Подсеть	Назначение	Маршрутизация
192.168.0.0/16[4]	Для использования в частных сетях	Только в частных сетях
198.51.100.0/24[7]	Для примеров в документации	Запрещена
198.18.0.0/15[9]	Для стендов тестирования производительности	Только для тестов
203.0.113.0/24[7]	Для примеров в документации	Запрещена
224.0.0.0/4[10]	Используются для многоадресной рассылки. Полный актуальный список зарезервированных блоков на сайте IANA. Разъяснения по зарезервированным мультикастовым подсетям RFC 5771	Глобально разрешена только для подсетей 233.0.0.0/8 и 234.0.0.0/8
240.0.0.0/4	Зарезервировано для использования в будущем. Существует мнение, что эта подсеть больше никогда не будет использована, так как есть множество оборудования, не способного посылать пакеты в эту сеть	Запрещена
255.255.255.255/32	Ограниченный широковещательный адрес. Чаще всего используется как адрес назначения при поиске DHCP серверов	Запрещена
Все остальные	Распределяются региональными интернет-регистраторами. Могут быть провайдеро-независимыми (Provider-independent address space)	Глобально разрешена

Структура дейтаграммы в IP

Заголовок пакета IP содержит 14 полей, из которых 13 являются обязательными, структура пакета показана на рис. 6.1. Четырнадцатое поле предназначено для необязательных опций. Поля используют порядок байтов от старшего к младшему, старшие биты идут первыми. Первый бит имеет номер 0. Таким образом, например, поле с версией находится в четырех старших битах первого байта. При передаче многооктетных значений старший октет передается первым.

Отступ	Октет	0								1								2								3			
Октет	Бит	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
0	0	Версия				Размер заголовка				Differentiated Services Code Point						Explicit Congestion Notification		Размер пакета (полный)															
4	32	Идентификатор																Флаги				Смещение фрагмента											
8	64	Время жизни								Протокол								Контрольная сумма заголовка															
12	96	IP-адрес источника																															
16	128	IP-адрес назначения																															
20	160	Опции (если размер заголовка > 5)																															
20 или 24+	160 или 192+	Данные																															

Рис. 6.1. Структура пакета IPv4

Версия

Первым полем заголовка пакета является версия протокола размером в четыре бита. Для IPv4 это 4.

Размер заголовка (Internet Header Length)

Следующие четыре бита содержат размер заголовка пакета в 32-битных словах. Поскольку число опций не постоянно, указание размера важно для отделения заголовка от данных. Минимальное значение равно 5 ($5 \times 32 = 160$ бит, 20 байт), максимальное — 15 (60 байт).

Differentiated Services Code Point (DSCP)

Изначально называлось «тип обслуживания» (Type of Service, ToS), в настоящее время определяется RFC 2474 как «Differentiated Services». Используется для разделения трафика на классы обслуживания, например для установки чувствительному к задержкам трафику, такому как VoIP, большего приоритета.

Указатель перегрузки (Explicit Congestion Notification, ECN)

Предупреждение о перегрузке сети без потери пакетов. Является необязательной функцией и используется, только если оба хоста ее поддерживают.

Размер пакета

16-битный полный размер пакета в байтах, включая заголовок и данные. Минимальный размер равен 20 байтам (заголовок без данных), максимальный — 65 535 байт. Хосты должны поддерживать передачу пакетов размером до 576 байт, но современные реализации обычно поддерживают гораздо больший размер. Пакеты большего размера, чем поддерживает канал связи, фрагментируются.

Идентификатор

Преимущественно используется для идентификации фрагментов пакета, если он был фрагментирован. Существуют эксперименты по его использованию для других целей, таких как добавление информации о трассировке пакета для упрощения отслеживания пути пакета с подделанным адресом источника.

Флаги

Поле размером три бита, содержащее флаги контроля над фрагментацией. Биты, от старшего к младшему, означают:

0: Зарезервирован, должен быть равен 0.

1: Не фрагментировать.

2: У пакета еще есть фрагменты.

Если установлен флаг «не фрагментировать», то в случае необходимости фрагментации такой пакет будет уничтожен. Может использоваться для передачи данных хостам, не имеющим достаточных ресурсов для обработки фрагментированных пакетов.

Флаг «есть фрагменты» должен быть установлен в 1 у всех фрагментов пакета, кроме последнего. У нефрагментированных устанавливается в 0 — такой пакет считается собственным последним фрагментом.

Смещение фрагмента

Поле размером в 13 бит указывает смещение поля данных текущего фрагмента относительно начала поля данных первого фрагментированного пакета в блоках по 8 байт. Позволяет $(213 - 1) \times 8 = 65\,528$ байт смещения. При учете размера заголовка итоговое смещение может превысить максимальный размер пакета ($65\,528 + 20 = 65\,548$ байт). Первый фрагмент в последовательности имеет нулевое смещение.

«Время жизни» (Time to Live, TTL) пакета

Определяет максимальное количество маршрутизаторов на пути следования пакета. Наличие этого параметра не позволяет пакету бесконечно ходить по сети. Каждый маршрутизатор при обработке пакета должен уменьшить значение TTL на единицу. Пакеты, время жизни которых стало равно нулю, уничтожаются, а отправителю посылается сообщение ICMP Time Exceeded. На отправке пакетов с разным временем жизни основана трассировка их пути прохождения (traceroute). Максимальное значение TTL = 255. Обычное начальное значение TTL = 64 (зависит от ОС).

Протокол

Указывает, данные какого протокола IP содержит пакет (например, TCP или ICMP). Присвоенные номера протоколов можно найти на сайте IANA.

Контрольная сумма заголовка

16-битная контрольная сумма, используемая для проверки целостности заголовка. Каждый хост или маршрутизатор сравнивает контрольную сумму заголовка со значением этого поля и отбрасывает пакет, если они не совпадают. Целостность данных IP не проверяет — она проверяется протоколами более высоких уровней (такими, как TCP или UDP), которые тоже используют контрольные суммы.

Поскольку TTL уменьшается на каждом шаге прохождения пакета, сумма тоже должна вычисляться на каждом шаге. Метод пересчета контрольной суммы определен в RFC 1071.

Адрес источника

32-битный адрес отправителя пакета. Может не совпадать с настоящим адресом отправителя из-за трансляции адресов.

Адрес назначения

32-битный адрес получателя пакета. Также может меняться при трансляции адресов.

Опции

За адресом назначения может следовать поле дополнительных опций, но оно используется редко. Размер заголовка в этом случае должен быть достаточным, чтобы вместить все опции (с учетом дополнения до целого числа 32-битных слов). Присвоенные номера опций размещаются на сайте IANA.

Время жизни может измеряться как в единицах времени T, так и в хопах P (числом пройденных маршрутизаторов). В первом случае контроль ведется по записанному в заголовке значению T, которое уменьшается на единицу каждую секунду. Во втором случае каждый маршрутизатор уменьшает число P, записанное в поле «Время жизни», на единицу. При $T = 0$ или при $P = 0$ дейтаграмма сбрасывается.

Поле «Тип протокола» определяет структуру данных в дейтаграмме. Примерами протоколов могут служить UDP, SNA, IGP и т.п.

6.3.2. IPv6

IPv6 (англ. Internet Protocol version 6) — новая версия интернет-протокола (IP), призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Интернете, за счет использования длины адреса 128 бит вместо 32. Протокол был разработан IETF.

В настоящее время протокол IPv6 уже используется в нескольких тысячах сетей по всему миру (более 14 000 сетей на осень 2013 г.), но пока еще не получил столь широкого распространения в Интернете, как IPv4. На конец 2012 г. доля IPv6 в сетевом трафике составляла около 1%. К концу 2013 г. ожидался рост до 3%. В России коммерческое использование операторами связи невелико (не более 1% трафика). DNS-серверы многих российских регистраторов доменов и провайдеров хостинга используют IPv6.

После того как адресное пространство в IPv4 закончится, два стека протоколов — IPv6 и IPv4 — будут использоваться параллельно (англ. dual stack), с постепенным увеличением доли трафика IPv6, по сравнению с IPv4. Такая ситуация станет возможной из-за наличия огромного количества устройств, в том числе устаревших, не поддерживающих IPv6 и требующих специального преобразования для работы с устройствами, использующими только IPv6.

В конце 1980-х гг. стала очевидна необходимость разработки способов сохранения адресного пространства Интернета. В начале 1990-х гг., несмотря на внедрение бесклассовой адресации, стало ясно, что этого недостаточно для предотвращения исчерпания адресов и необходимы дальнейшие изменения инфраструктуры Интернета. К началу 1992 г. появилось несколько предложений, и к концу 1992 г. IETF объявила конкурс для рабочих групп на создание интернет-протокола следующего поколения (англ. IP Next Generation — IPng). 25 июля 1994 г. IETF утвердила модель IPng, с образованием нескольких рабочих групп IPng. К 1996 г. была выпущена серия RFC, определяющих интернет-протокол версии 6, начиная с RFC 1883.

IETF назначила новому протоколу версию 6, так как версия 5 была ранее назначена экспериментальному протоколу, предназначенному для передачи видео и аудио.

Перевод на IPv6 начал осуществляться внутри Google с 2008 г. Тестирование IPv6 признано успешным. 6 июня 2012 г. состоялся Всемирный запуск IPv6. Интернет-провайдеры включат IPv6 как минимум для 1% своих пользователей (уже подписались AT&T, Comcast, Free Telecom, Internode, KDDI, Time Warner Cable, XS4ALL). Производители сетевого оборудования активируют IPv6 в качестве настроек по умолчанию в маршрутизаторах (Cisco, D-Link). Веб-компании включат IPv6 на своих основных сайтах (Google, Facebook, Microsoft Bing, Yahoo), а некоторые переводят на IPv6 также корпоративные сети. В спецификации стандарта мобильных сетей LTE указана обязательная поддержка протокола IPv6.

Сравнение с IPv4

Иногда утверждается, что новый протокол может обеспечить до 5·1028 адресов на каждого жителя Земли. Такое большое адресное пространство было введено ради иерархичности адресов (это упрощает маршрутизацию). Тем не менее, увеличенное пространство адресов сделает NAT необязательным. Классическое применение IPv6 (по сети /64 на абонента; используется только unicast-адресация) обеспечит возможность использования более 300 млн IP-адресов на каждого жителя Земли.

Из IPv6 убраны функции, усложняющие работу маршрутизаторов: маршрутизаторы больше не должны фрагментировать пакет, вместо этого пакет отбрасывается с ICMP-уведомлением о превышении MTU и указанием величины MTU следующего канала, в который этому пакету не удалось войти. В IPv4 размер MTU в ICMP-пакете не указывался и отправителю требовалось осуществлять подбор MTU техникой Path MTU discovery. Для лучшей работы протоколов, требовательных к потерям, минимальный MTU поднят до 1280 байт. Фрагментация поддерживается как опция (информация о фрагментации пакетов вынесена из основного заголовка в расширенные) и возможна только по инициативе передающей стороны.

- Из IP-заголовка исключена контрольная сумма. С учетом того, что канальные (Ethernet) и транспортные (TCP и UDP) протоколы имеют свои контрольные суммы, еще одна контрольная сумма на уровне IP воспринимается как излишняя. Кроме того, модификация поля hop limit (или TTL в IPv4) на каждом маршрутизаторе в IPv4 приводила к необходимости ее постоянного перерасчета.

Несмотря на больший по сравнению с предыдущей версией протокола размер адреса IPv6 (16 байтов вместо 4), заголовок пакета удлинился всего лишь вдвое: с 20 до 40 байт.

Улучшения IPv6 по сравнению с IPv4:

- в сверхскоростных сетях возможна поддержка огромных пакетов (джамбограмм) — до 4 гигабайт;
- Time to Live переименовано в Hop Limit;
- появились метки потоков и классы трафика;
- появилось многоадресное вещание.

Автоконфигурация (Stateless address autoconfiguration — SLAAC)

При инициализации сетевого интерфейса ему назначается локальный IPv6-адрес, состоящий из префикса fe80::/10 и идентификатора интерфейса, размещенного в младшей части адреса. В каче-

стве идентификатора интерфейса часто используется 64-битный расширенный уникальный идентификатор EUI-64, часто ассоциируемый с MAC-адресом. Локальный адрес действителен только в пределах сетевого сегмента канального уровня и используется для обмена информационными ICMPv6-пакетами.

Для настройки других адресов узел может запросить информацию о настройках сети у маршрутизаторов, отправив ICMPv6-сообщение «Router Solicitation» на групповой адрес маршрутизаторов. Маршрутизаторы, получившие это сообщение, отвечают ICMPv6-сообщением «Router Advertisement», в котором может содержаться информация о сетевом префиксе, адресе шлюза, адресах рекурсивных DNS-серверов, MTU и множестве других параметров. Объединяя сетевой префикс и идентификатор интерфейса, узел получает новый адрес. Для защиты персональных данных идентификатор интерфейса может быть заменен на псевдослучайное число.

Для большего административного контроля может быть использован DHCPv6, позволяющий администратору маршрутизатора назначать узлу конкретный адрес.

Для провайдеров может использоваться функция делегирования префиксов клиенту, что позволяет клиенту просто переходить от провайдера к провайдеру, без изменения каких-либо настроек.

Метки потоков

Введение в протоколе IPv6 поля «Метка потока» позволяет значительно упростить процедуру маршрутизации однородного потока пакетов. Поток — это последовательность пакетов, посылаемых отправителем определенному адресату. При этом предполагается, что все пакеты данного потока должны быть подвергнуты определенной обработке. Характер данной обработки задается дополнительными заголовками.

Допускается существование нескольких потоков между отправителем и получателем. Метка потока присваивается узлом-отправителем путем генерации псевдослучайного 20-битного числа. Все пакеты одного потока должны иметь одинаковые заголовки, обрабатываемые маршрутизатором.

При получении первого пакета с меткой потока маршрутизатор анализирует дополнительные заголовки, выполняет предписанные этими заголовками функции и запоминает результаты обработки (адрес следующего узла, опции заголовка переходов, перемещение адресов в заголовке маршрутизации и т.д.) в локальном кэше. Ключом для такой записи является комбинация адреса источника

и метки потока. Последующие пакеты с той же комбинацией адреса источника и метки потока обрабатываются с учетом информации кэша без детального анализа всех полей заголовка.

Время жизни записи в кэше составляет не более 6 секунд, даже если пакеты этого потока продолжают поступать. При обнулении записи в кэше и получении следующего пакета потока пакет обрабатывается в обычном режиме, и для него происходит новое формирование записи в кэше. Следует отметить, что указанное время жизни потока может быть явно определено узлом-отправителем с помощью протокола управления или опций заголовка переходов и может превышать 6 секунд.

Обеспечение безопасности в протоколе IPv6 осуществляется с использованием протокола IPsec, поддержка которого является обязательной для данной версии протокола.

Основы адресации IPv6

Существуют различные типы адресов IPv6: одноадресные (Unicast), групповые (Anycast) и многоадресные (Multicast).

Адреса типа Unicast хорошо всем известны. Пакет, посланный на такой адрес, достигает в точности интерфейса, который этому адресу соответствует.

Адреса типа Anycast синтаксически неотличимы от адресов Unicast, но они адресуют группу интерфейсов. Пакет, направленный такому адресу, попадет в ближайший (согласно метрике маршрутизатора) интерфейс. Адреса Anycast могут использоваться только маршрутизаторами.

Адреса типа Multicast идентифицируют группу интерфейсов. Пакет, посланный на такой адрес, достигнет всех интерфейсов, привязанных к группе многоадресного вещания.

Широковещательные адреса IPv4 (обычно xxx.xxx.xxx.255) выражаются адресами многоадресного вещания IPv6. Крайние адреса подсети IPv6 (например, xxxx:xxxx:xxxx:xxxx:0:0:0:0 и xxxx:xxxx:xxxx:xxxx:ffff:ffff:ffff:ffff для подсети /64) являются полноправными адресами и могут использоваться наравне с остальными.

Группы цифр в адресе разделяются двоеточиями (например, fe80:0:0:0:200:f8ff:fe21:67cf). Незначащие старшие нули в группах могут быть опущены. Большое количество нулевых групп может быть пропущено с помощью двойного двоеточия (fe80::200:f8ff:fe21:67cf). Такой пропуск должен быть единственным в адресе.

Типы Unicast-адресов

Глобальные

Соответствуют публичным IPv4-адресам. Могут находиться в любом не занятом диапазоне. В настоящее время региональные интернет-регистраторы распределяют блок адресов 2000::/3 (с 2000:: по 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF).

Link-Local

Соответствуют автосконфигурированным с помощью протокола APIPA IPv4 адресам. Начинаются с FE80:. Используются:

- в качестве исходного адреса для Router Solicitation(RS) и Router Advertisement(RA) сообщений, для обнаружения маршрутизаторов;
- для обнаружения соседей (эквивалент ARP для IPv4);
- как next-hop-адрес для маршрутов.

Unique-Local

RFC 4193 соответствуют внутренним IP-адресам, которыми в версии IPv4 являлись 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Начинаются с цифр FCxx: и FDxx:.

Типы Multicast-адресов

Адреса мультикаст бывают двух типов:

Назначенные (Assigned multicast) — специальные адреса, назначение которых предопределено. Это зарезервированные для определенных групп устройств мультикастовые адреса. Отправляемый на такой адрес пакет будет получен всеми устройствами, входящими в группу.

Запрошенные (Solicited multicast) — остальные адреса, которые устройства могут использовать для прикладных задач. Адрес этого типа автоматически появляется, когда на некотором интерфейсе появляется юникастовый адрес. Адрес формируется из сети FF02:0:0:0:0:1:FF00::/104, оставшиеся 24 бита — такие же, как у настроенного юникастового адреса.

Формат пакета IPv6

IPv6-пакет — блок информации, форматированный для передачи через компьютерные сети, поддерживающие протокол IPv6.

Пакеты состоят из управляющей информации, необходимой для доставки пакета адресату и полезных данных, которые требуется переслать. Управляющая информация делится на содержащуюся в основном фиксированном заголовке, и содержащуюся в одном из необязательных дополнительных заголовков. Полезные данные — это, как правило, дейтаграмма или фрагмент протокола более высокого транспортного уровня, но могут быть и данные сетевого уровня (например ICMPv6), или же канального уровня (например OSPF).

IPv6-пакеты обычно передаются с помощью протоколов канального уровня, таких как Ethernet, который инкапсулирует каждый пакет в кадр. IPv6-пакет может быть также передан с помощью туннельного протокола более высокого уровня, например, с помощью 6to4 или Teredo.

В отличие от IPv4, маршрутизаторы не фрагментируют IPv6-пакеты в ситуациях, когда пакет больше MTU подключения и узлам настоятельно рекомендуется реализовать механизм Path MTU discovery для определения размера MTU пути. Иначе им придется использовать минимально допустимый в IPv6-сетях MTU, равный 1280 октетам. Конечные узлы могут фрагментировать пакет перед отправкой, если он больше, чем MTU пути.

Фиксированный заголовок IPv6-пакета состоит из 40 октетов (320 бит) и имеет следующий формат (рис. 6.2):

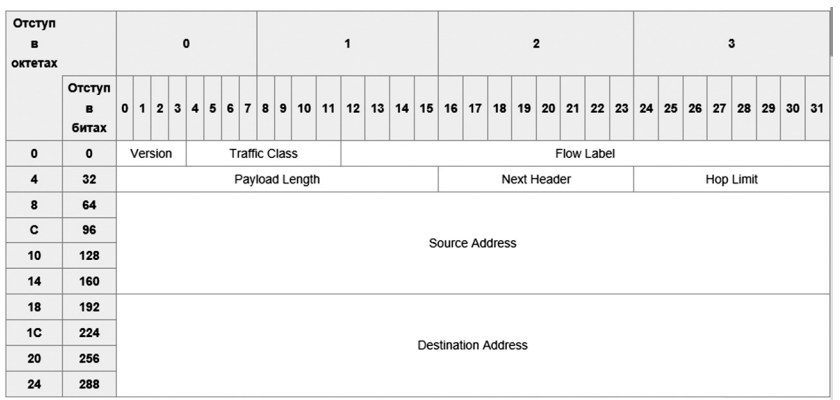


Рис. 6.2. Заголовок IPv6-пакета

Описание полей:

Version: версия протокола; для IPv6 это значение равно 6 (значение в битах — 0110).

Traffic Class: приоритет пакета (8 бит). Это поле состоит из двух значений. Старшие 6 бит используются DSCP для классификации пакетов. Оставшиеся два бита используются ECN для контроля перегрузки.

Flow Label: метка потока.

Payload Length: размер данных в октетах (16 бит), не включая данный заголовок, но включая все расширенные заголовки.

Next Header: задает тип расширенного заголовка (англ. IPv6 extension), который идет следующим. В последнем расширенном заголовке поле Next Header задает тип транспортного протокола (TCP, UDP и т.д.).

Hop Limit: аналог поля time to live в IPv4 (8 бит).

Source Address u Destination Address: адрес отправителя и получателя соответственно; по 128 бит.

С целью повышения производительности и с расчетом на то, что современные технологии канального и транспортного уровней обеспечивают достаточный уровень обнаружения ошибок, заголовок не имеет контрольной суммы.

Расширенные заголовки содержат дополнительную информацию и размещены между фиксированным заголовком и заголовком протокола более высокого уровня. Тип первого расширенного заголовка указывается в поле Next Header фиксированного заголовка, а каждый расширенный заголовок имеет аналогичное поле, в котором хранится тип следующего расширенного заголовка. В поле Next Header последнего заголовка находится тип протокола более высокого уровня, находящегося в качестве полезных данных.

Каждый расширенный заголовок должен иметь размер в октетах, кратный 8. Некоторые заголовки необходимо расширить до нужного размера.

Расширенные заголовки должны быть обработаны только конечным узлом, за исключением заголовка Hop-By-Hop Options, который должен быть обработан каждым промежуточным узлом на пути пакета, включая отправителя и получателя. Если расширенных заголовков в пакете несколько, то рекомендуется отсортировать их, как указано в таблице ниже. Отметим, что все расширенные заголовки являются необязательными и не должны появиться в пакете более одного раза, за исключением заголовка Destination Options, который может появиться дважды.

Если узел не может обработать какой-то расширенный заголовок, то он должен отбросить пакет и отправить сообщение Parameter Problem (ICMPv6 тип 4, код 1). Если в поле Next Header расширенного заголовка будет 0, то узел должен сделать то же самое.

За фиксированным и расширенными заголовками находятся полезные данные протокола транспортного уровня, например TCP-сегмент или UDP-дейтаграмма. Поле Next Header последнего IPv6-заголовка указывает тип полезных данных, хранимых в пакете.

Поле фиксированного заголовка Payload Length имеет размер 16 бит, поэтому максимально возможный размер полезных данных и расширенных заголовков равен 65 535 октетам. Максимальный размер фрейма многих протоколов канального уровня гораздо меньше.

Джамбограммы

IPv6-пакет может нести больше данных с помощью опции jumbo payload в расширенном заголовке Hop-By-Hop Options [7]. Эта опция позволяет обмениваться пакетами с размером полезных данных на 1 байт меньшим, чем 4 ГиБ (232 – 1 = 4 294 967 295 байт). Пакет с таким содержимым называют джамбограммой.

Так как протоколы TCP и UDP оба имеют поля длины, ограниченные 16 битами, для поддержки джамбограмм требуется реализация модифицированных протоколов транспортного уровня. Джамбограммы могут работать только на подключениях с MTU, большим чем 65 583 октетов (более 65 535 октетов для полезных данных, 40 октетов для фиксированного заголовка и 8 октетов для расширенного заголовка Hop-By-Hop Options).

Фрагментация

IPv6-пакеты никогда не фрагментируются маршрутизаторами. Пакеты, чей размер превышает MTU сетевого подключения, уничтожаются и отправителю посылается сообщение Packet too Big (ICMPv6 тип 2). Подобное поведение в IPv4 происходит, если установлен бит Don't Fragment.

Ожидается, что конечные IPv6-узлы выполнят Path MTU discovery для определения максимально допустимого размера отправляемых пакетов, и протокол более высокого уровня ограничит размер пакета. Однако если протокол более высокого уровня не в состоянии сделать этого, отправитель может использовать расширенный заголовок Fragment для выполнения фрагментации IPv6-пакетов. Все протоколы, передающие через себя IPv6-пакеты, должны иметь MTU, равный или больший 1280 октетов. Протоколы, не способные передать пакет длиной 1280 октетов одним блоком, должны произвести фрагментацию и сборку самостоятельно, не затрагивая уровень IPv6.

Пакет, содержащий фрагмент оригинального (большого) пакета, состоит из двух частей: нефрагментируемая часть оригинального пакета, одинаковая для всех фрагментов, и фрагментируемая часть, идентифицируемая по смещению фрагмента.

Нефрагментируемая часть пакета состоит из фиксированного заголовка и расширенных заголовков оригинального пакета (опционально).

Значение поля Next Header последнего заголовка нефрагментируемой части должно быть равным 44, обозначающее, что следующим заголовком будет Fragment. В заголовке Fragment поле Next Header должно быть равно типу первого заголовка фрагментируемой части. После заголовка Fragment следует фрагмент оригинального пакета. Размер каждого фрагмента фрагментируемой части должен быть кратен 8, исключение составляет последний фрагмент.

Принимающий узел, собрав все фрагменты, отбрасывает расширенный заголовок Fragments и размещает фрагменты по смещениям, указанным в поле Fragment Offset, умноженным на 8. Пакеты, содержащие фрагменты, не обязаны приходить в правильном порядке, и они будут переставлены принимающим узлом, если потребуется.

Если спустя 60 секунд после получения первого фрагмента были собраны не все фрагменты, то сборка оригинального пакета отменяется и все полученные фрагменты отбрасываются. Если при этом получен первый фрагмент (с полем Fragmant Offset, равным нулю), то отправителю фрагментированного пакета посылается сообщение Fragment Reassembly Time Exceeded (ICMPv6 тип 3 код 1).

Максимальный размер оригинального пакета не должен превышать 65 535 октетов, а если после сборки оригинальный пакет оказывается больше, то он должен быть отброшен.

Зарезервированные адреса IPv6

Как и предыдущая версия протокола, IPv6 также имеет ряд резервных адресов, которые представлены в табл. 6.5.

Таблица 6.5

IPv6-адрес	Длина префикса (биты)	Описание	Заметки
::	128	—	см. 0.0.0.0 в IPv4
::1	128	loopback-адрес	см. 127.0.0.1 в IPv4
::xx.xx.xx.xx	96	встроенный IPv4	Нижние 32 бита — это адрес IPv4. Также называется *IPv4 совместимым IPv6-адресом*. Устарел и больше не используется

Окончание табл. 6.5

IPv6-адрес	Длина префикса (биты)	Описание	Заметки
::ffff:xx.xx.xx.xx	96	Адрес IPv4, отображенный на IPv6	Нижние 32 бита — это адрес IPv4 для хостов, не поддерживающих IPv6
64:ff9b::	96	NAT64 (англ.)	Зарезервирован для доступа из подсети IPv6 к публичной сети IPv4 через механизм трансляции NAT64
2001::	32	Teredo	Зарезервирован для туннелей Teredo в RFC 4380
2001:db8::	32	Документирование	Зарезервирован для примеров в документации в RFC 3849
2002::	16	6to4	Зарезервирован для туннелей 6to4 в RFC 3056
fe80:: — febf::	10	link-local	Аналог 169.254.0.0/16 в IPv4
fec0:: — feff::	10	site-local	Помечен как устаревший в RFC 3879 (Аналог внутренних сетей 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16)
fc00::	7	Unique Local Unicast	Пришел на смену Site-Local RFC 4193
ff00::	8	multicast	

6.4. Протоколы UDP и TCP транспортного уровня стека TCP/IP

Стек протоколов TCP/IP содержит два основных протокола транспортного уровня:

- UDP (User Datagram Protocol) — обеспечивает дэйтаграммный способ;

- TCP (Transmission Control Protocol) — протокол управления передачей через виртуальное соединение.

При написании программ, работающих через TCP/IP часто возникает вопрос выбора протокола: TCP или UDP? TCP больше подходит для соединений «много-к-одному», а UDP — «один-к-одному», однако ничего не мешает использовать и UDP для соединений «много-к-одному», а TCP — для «один-к-одному».Если необходимо использование широковещательной или групповой адресации (т.е. «один-ко-многим»), то тут поможет только UDP. В большинстве остальных случаев предпочтительнее использовать TCP за некоторым исключением. Во-первых, UDP работает быстрее TCP из-за меньшего количества передаваемой служебной информации. Фактически, кроме заголовка UDP-дейтаграммы, вся передаваемая служебная информация определяется приложением. Однако из-за отсутствия средств управления потоком данных в глобальной сети протокол UDP может показать меньшую, чем TCP, производительность из-за большого разброса характеристик самой сети. Чтобы повысить производительность, необходимо программно реализовать алгоритмы управления потоком данных, что повышает сложность программного обеспечения и по количеству передаваемой служебной информации приближает UDP к TCP.

Таким образом, UDP гарантированно работает быстрее TCP в локальных сетях, а в глобальных — его поведение неоднозначно. UDP часто применяется для передачи потоковых данных, связанных с реальным временем. Он используется, к примеру, в RealPlayer для передачи потока данных звука и видео. И конечно же, используется в играх. Протокол UDP часто используется в сетевых устройствах, таких как маршрутизатор, из-за простоты реализации. При этом часто используются протоколы SNMP (Simple Network Management Protocol — простой протокол управления сетью) для управления и опроса состояния и TFTP (Trivial File Transfer Protocol — тривиальный протокол передачи файлов) для загрузки необходимых данных.

6.4.1. Протокол TCP

Transmission Control Protocol (TCP, протокол управления передачей) — один из основных протоколов передачи данных Интернета, предназначенный для управления передачей данных. Сети и подсети, в которых совместно используются протоколы TCP и IP, называются сетями TCP/IP.

В стеке протоколов IP, TCP выполняет функции протокола транспортного уровня модели OSI.

Механизм TCP предоставляет поток данных с предварительной установкой соединения, осуществляет повторный запрос данных в случае потери данных и устраняет дублирование при получении двух копий одного пакета, гарантируя тем самым, в отличие от UDP, целостность передаваемых данных и уведомление отправителя о результатах передачи.

Реализации TCP обычно встроены в ядра ОС. Существуют реализации TCP, работающие в пространстве пользователя.

Когда осуществляется передача от компьютера к компьютеру через Интернет, TCP работает на верхнем уровне между двумя конечными системами, например, браузером и веб-сервером. TCP осуществляет надежную передачу потока байтов от одной программы на некотором компьютере к другой программе на другом компьютере (например, программы для электронной почты, для обмена файлами). TCP контролирует длину сообщения, скорость обмена сообщениями, сетевой трафик.

TCP — это один из самых широко используемых протоколов транспортного уровня. IP не предполагает установление соединения. Он просто передает дейтаграмму от узла к узлу, а при каком-либо нарушении она просто отбрасывается, о чем отправитель уведомляется ICMP-сообщением. Проверка принятых данных и повторная передача данных, не дошедших до получателя, ложится на TCP. Он следит за доставкой данных протоколом IP.

Главная функция TCP заключается в доставке сообщений без потерь. Для этого предварительно устанавливается соединение между приложением-отправителем и приложением-получателем, осуществляя надежную доставку дейтаграмм. Именно TCP производит повторную передачу искаженного или утерянного пакета.

TCP — дуплексный транспортный протокол с установлением соединения. Его функции:

- упаковка и распаковка пакетов на концах транспортного соединения;
- установление виртуального канала путем обмена запросом и согласием на соединение;
- управление потоком — получатель при подтверждении правильности передачи сообщает размер окна, т.е. диапазон номеров пакетов, которые получатель готов принять; помещение срочных данных между специальными указателями, т.е. возможность управлять скоростью передачи.

TCP регламентирует передачу данных с прикладного уровня на уровень межсетевого взаимодействия и обратно. TCP должен отве-

чать за соблюдение приоритетов и защиту данных, за завершение приложения на более высоком уровне, ожидающего дейтаграммы, за обработку ошибок нижних уровней, за ведение таблиц состояний для всех потоков как в самом TCP, так и на других уровнях. Выделение всех этих функций в отдельный уровень освобождает разработчиков прикладных программ от решения задач управления потоком и обеспечения надежности передачи данных. Без TCP перечисленные функции пришлось бы реализовывать в каждой прикладной программе.

TCP является протоколом, ориентированным на соединение, обеспечивая сквозную передачу данных от машины-отправителя машине-получателю. Поскольку в нем применяется соединение, адресат, получивший дейтаграмму, должен уведомить отправителя об этом. Обычно используется термин «виртуальный канал», чтобы указать, что машина-отправитель и машина-получатель обмениваются сообщениями, большинство из которых являются подтверждениями о получении или кодами ошибок.

Протокол TCP, в отличие от UDP, ориентирован на потоковую (stream, а не datagram) передачу данных. Это означает, что прикладной уровень добавляет посылаемые данные в очередь, а средствами протокола TCP производится разбиение потока данных на дейтаграммы и сборка их во входную очередь на принимающей стороне.

Говорят, что протокол TCP является «надежным», так как обеспечивает отслеживание потерь дейтаграмм и их повторную передачу. Кроме того, протокол TCP содержит средства управления потоком данных, что означает динамическую подстройку параметров передачи под канал связи. Протокол TCP использует понятие соединения (connection), которое должно быть установлено между передающей и принимающей стороной перед тем, как начнется передача данных. Протокол TCP гарантирует доставку данных, пока установлено соединение. В противном случае соединение разрывается. Сторона, которая устанавливает соединение, называется клиентской, а которая ожидает установки соединения — серверной. TCP-сервер может одновременно обслуживать несколько соединений. Передача данных внутри соединения может одновременно происходить в обе стороны, т.е. соединение является дуплексным. Таким образом, по модели OSI/ISO, протокол TCP удовлетворяет требованием протокола транспортного уровня. Кроме того, он может быть отнесен и к протоколам сеансового уровня (session layer) из-за ориентации на соединение. Протокол не может работать с широковещательными адресами.

В TCP имеется программа-демон, которая постоянно готова к работе и при приходе запроса генерирует свою копию для обслуживания создаваемого соединения, а сама программа-родитель ждет новых вызовов.

Схема установления соединения в одноранговых сетях такова: инициатор соединения обращается к своей ОС, которая в ответ выдает номер протокольного порта и посылает сегмент получателю. Тот должен подтвердить получение запроса и послать свой сегмент-запрос на создание обратного соединения (так как соединение дуплексное). Инициатор должен подтвердить создание обратного соединения. Получается трехшаговая процедура (handshake) установления соединения. Во время этих обменов партнеры сообщают номера байтов в потоках данных, с которых начинаются сообщения. На противоположной стороне счетчики устанавливаются в состояние на единицу больше, чем и обеспечивается механизм синхронизации в дейтаграммной передаче, реализуемой на сетевом уровне. После установления соединения начинается обмен. При этом номера протокольных портов включаются в заголовок пакета. Каждое соединение (socket) получает свой идентификатор ISN. Разъединение происходит в обратном порядке.

Примечание: ISN в TCP/IP не используется, но предусмотрен в UNIX, так как может потребоваться в других протоколах.

Схема установления соединения в сетях «клиент–сервер» аналогична (за исключением handshake) и включает посылку клиентом запроса на соединение (команда ACTIVE_OPEN) с указанием адреса сервера, тайм-аута (времени жизни), уровня секретности. Можно сразу же поместить в запрос данные (тогда команда ACTIVE_OPEN_WITH_DATA). Если сервер готов к связи, он отвечает командой согласия (OPEN_RECEIVED), в которой назначает номер соединения. Далее командой SEND посылаются данные, а командой DELIVER подтверждается их получение. Разъединение выполняется обменом командами CLOSE и CLOSING.

Заголовок сегмента TCP

Структура заголовка пакета TCP показана на рис. 6.3.

- Порт источника, Порт назначения

Эти 16-битные поля содержат номера портов — числа, которые определяются по специальному списку.

Порт источника идентифицирует приложение клиента, с которого отправлены пакеты. Ответные данные передаются клиенту на основании этого номера.

Порт назначения идентифицирует порт, на который отправлен пакет.

Бит	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт источника, **Source Port**			Порт назначения, **Destination Port**
32	Порядковый номер, **Sequence Number (SN)**			
64	Номер подтверждения, **Acknowledgment Number (ACK SN)**			
96	Длина заголовка	Зарезервировано	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции (необязательное, но используется практически всегда)			
160/192+	Данные			

Рис. 6.3. Заголовок сегмента TCP

Порядковый номер

Порядковый номер выполняет две задачи:

Если установлен флаг SYN, то это изначальный порядковый номер — ISN (Initial Sequence Number), и первый байт данных, которые будут переданы в следующем пакете, будет иметь номер, равный ISN + 1.

В противном случае, если SYN не установлен, первый байт данных, передаваемый в данном пакете, имеет этот порядковый номер.

Поскольку поток TCP в общем случае может быть длиннее, чем число различных состояний этого поля, то все операции с порядковым номером должны выполняться по модулю 232. Это накладывает практическое ограничение на использование TCP. Если скорость передачи коммуникационной системы такова, чтобы в течение MSL (максимального времени жизни сегмента) произошло переполнение порядкового номера, то в сети может появиться два сегмента с одинаковым номером, относящихся к разным частям потока, и приемник получит некорректные данные.

Номер подтверждения

Acknowledgment Number (ACK SN) (32 бита) — если установлен флаг ACK, то это поле содержит порядковый номер октета, который отправитель данного сегмента желает получить. Это означает, что все предыдущие октеты (с номерами от ISN+1 до ACK-1 включительно) были успешно получены.

Длина заголовка (смещение данных)

Длина заголовка (Data offset) занимает 4 бита и указывает значение длины заголовка, измеренное в 32-битовых словах. Минимальный размер составляет 20 байт (пять 32-битовых слов), а максимальный — 60 байт (пятнадцать 32-битовых слов). Длина заголовка определяет смещение полезных данных относительно начала сегмента. Например, Data offset, равное 1111, говорит о том, что заголовок занимает пятнадцать 32-битных слова (15 строк × 32 бита в каждой строке/8 бит = 60 байт).

Зарезервировано

Зарезервировано (6 бит) для будущего использования и должно устанавливаться в ноль. Из них два (5-й и 6-й) уже определены:

CWR (Congestion Window Reduced) — Поле «Окно перегрузки уменьшено» — флаг установлен отправителем, чтобы указать, что получен пакет с установленным флагом ECE (RFC 3168);

ECE (ECN-Echo) — Поле «Эхо ECN» — указывает, что данный узел способен на ECN (явное уведомление перегрузки) и для указания отправителю о перегрузках в сети (RFC 3168).

Флаги (управляющие биты)

Это поле содержит 6 битовых флагов:

- URG — поле «Указатель важности» задействовано (англ. Urgent pointer field is significant);
- ACK — поле «Номер подтверждения» задействовано (англ. Acknowledgement field is significant);
- PSH — (англ. Push function) инструктирует получателя протолкнуть данные, накопившиеся в приемном буфере, в приложение пользователя;
- RST — оборвать соединения, сбросить буфер (очистка буфера) (англ. Reset the connection);
- SYN — синхронизация номеров последовательности (англ. Synchronize sequence numbers);
- FIN (англ. final, бит) — флаг, будучи установлен, указывает на завершение соединения (англ. FIN bit used for connection termination).

Размер окна

Количество байт данных, начиная с последнего номера подтверждения, которые может принять отправитель данного пакета. Иначе говоря, отправитель пакета располагает для приема данных буфером длиной «размер окна» байт.

Контрольная сумма

Поле контрольной суммы — это 16-битное дополнение к сумме всех 16-битных слов заголовка (включая псевдозаголовок) и данных. Если сегмент, по которому вычисляется контрольная сумма, имеет длину, не кратную 16 битам, то длина сегмента увеличивается до кратной 16, за счет дополнения к нему справа нулевых битов заполнения. Биты заполнения (0) не передаются в сообщении и служат только для расчета контрольной суммы. При расчете контрольной суммы значение самого поля контрольной суммы принимается равным 0.

Указатель важности

16-битовое значение положительного смещения от порядкового номера в данном сегменте. Это поле указывает порядковый номер октета, которым заканчиваются важные (urgent) данные. Поле принимается во внимание только для пакетов с установленным флагом URG. Используется для внеполосных данных.

Опции

Могут применяться в некоторых случаях для расширения протокола. Иногда используются для тестирования. На данный момент в опции практически всегда включают 2 байта NOP (в данном случае 0×01) и 10 байт, задающих timestamps. Вычислить длину поля опции можно через значение поля смещения.

Механизм действия протокола

В отличие от традиционной альтернативы — UDP, который может сразу же начать передачу пакетов, TCP устанавливает соединения, которые должны быть созданы перед передачей данных. TCP-соединение можно разделить на три стадии:

- установка соединения;
- передача данных;
- завершение соединения.

Состояния сеанса TCP

Состояния протокола TCP представлены в табл. 6.6.

Таблица 6.6

Состояния сеанса TCP

CLOSED	Начальное состояние узла. Фактически фиктивное
LISTEN	Сервер ожидает запросов установления соединения от клиента
SYN-SENT	Клиент отправил запрос серверу на установление соединения и ожидает ответа

Окончание табл. 6.6

SYN-RECEIVED	Сервер получил запрос на соединение, отправил ответный запрос и ожидает подтверждения
ESTABLISHED	Соединение установлено, идет передача данных
FIN-WAIT-1	Одна из сторон (назовем ее узел-1) завершает соединение, отправив сегмент с флагом FIN
CLOSE-WAIT	Другая сторона (узел-2) переходит в это состояние, отправив в свою очередь сегмент ACK, и продолжает одностороннюю передачу
FIN-WAIT-2	Узел-1 получает ACK, продолжает чтение и ждет получения сегмента с флагом FIN
LAST-ACK	Узел-2 заканчивает передачу и отправляет сегмент с флагом FIN
TIME-WAIT	Узел-1 получил сегмент с флагом FIN, отправил сегмент с флагом ACK и ждет 2×MSL секунд, перед окончательным закрытием соединения
CLOSING	Обе стороны инициировали закрытие соединения одновременно: после отправки сегмента с флагом FIN узел-1 также получает сегмент FIN, отправляет ACK и находится в ожидании сегмента ACK (подтверждения на свой запрос о разъединении)

Процесс начала сеанса TCP (также называемый «рукопожатие» (англ. handshake)), состоит из трех шагов.

1. Клиент, который намеревается установить соединение, посылает серверу сегмент с номером последовательности и флагом SYN.

Сервер получает сегмент, запоминает номер последовательности и пытается создать сокет (буферы и управляющие структуры памяти) для обслуживания нового клиента.

В случае успеха сервер посылает клиенту сегмент с номером последовательности и флагами SYN и ACK и переходит в состояние SYN-RECEIVED.

В случае неудачи сервер посылает клиенту сегмент с флагом RST.

2. Если клиент получает сегмент с флагом SYN, то он запоминает номер последовательности и посылает сегмент с флагом ACK.

Если клиент одновременно получает и флаг ACK (что обычно и происходит), то он переходит в состояние ESTABLISHED.

Если клиент получает сегмент с флагом RST, то он прекращает попытки соединиться.

Если клиент не получает ответа в течение 10 секунд, то он повторяет процесс соединения заново.

3. Если сервер в состоянии SYN-RECEIVED получает сегмент с флагом ACK, то он переходит в состояние ESTABLISHED.

В противном случае после тайм-аута он закрывает сокет и переходит в состояние CLOSED.

Процесс называется «трехэтапным согласованием» (англ. three way handshake), так как несмотря на то, что возможен процесс установления соединения с использованием четырех сегментов (SYN в сторону сервера, ACK в сторону клиента, SYN в сторону клиента, ACK в сторону сервера), на практике для экономии времени используются три сегмента.

Передача данных

При обмене данными приемник использует номер последовательности, содержащийся в получаемых сегментах, для восстановления их исходного порядка. Приемник уведомляет передающую сторону о номере последовательности, до которой он успешно получил данные, включая его в поле «номер подтверждения». Все получаемые данные, относящиеся к промежутку подтвержденных последовательностей, игнорируются. Если полученный сегмент содержит номер последовательности больший, чем ожидаемый, то данные из сегмента буферизируются, но номер подтвержденной последовательности не изменяется. Если впоследствии будет принят сегмент, относящийся к ожидаемому номеру последовательности, то порядок данных будет автоматически восстановлен исходя из номеров последовательностей в сегментах.

Для того чтобы передающая сторона не отправляла данные интенсивнее, чем их может обработать приемник, TCP содержит средства управления потоком. Для этого используется поле «окно». В сегментах, направляемых от приемника передающей стороне, в поле «окно» указывается текущий размер приемного буфера. Передающая сторона сохраняет размер окна и отправляет данных не более, чем указал приемник. Если приемник указал нулевой размер окна, то передача данных в направлении этого узла не происходит, пока приемник не сообщит о большем размере окна.

В некоторых случаях передающее приложение может явно затребовать протолкнуть данные до некоторой последовательности принимающему приложению, не буферизируя их. Для этого используется флаг PSH. Если в полученном сегменте обнаруживается флаг PSH, то реализация TCP отдает все буферизированные на текущий момент данные принимающему приложению. «Проталкивание» используется, например, в интерактивных приложениях. В сетевых

терминалах нет смысла ожидать ввода пользователя после того, как он закончил набирать команду. Поэтому последний сегмент, содержащий команду, обязан содержать флаг PSH, чтобы приложение на принимающей стороне смогло начать ее выполнение.

Завершение соединения

Завершение соединения можно рассмотреть в три этапа.

- Посылка серверу от клиента флага FIN на завершение соединения.
- Сервер посылает клиенту флаги ответа ACK, FIN, что соединение закрыто.
- После получения этих флагов клиент закрывает соединение и в подтверждение отправляет серверу ACK, что соединение закрыто.

6.4.2. Транспортный протокол UDP в стеке протоколов TCP/IP

В TCP/IP входит также протокол UDP (User Datagram Protocol) — транспортный протокол без установления соединения.

UDP значительно проще TCP, но используется чаще всего для сообщений, умещающихся в один пакет.

Протокол UDP обеспечивает простой обмен дейтаграммами: отправитель посылает набор данных в виде дейтаграммы получателю. При этом говорят, что он является «ненадежным» протоколом. Это означает, что он не содержит средств проверки: дошла ли дейтаграмма до получателя. Эта задача выполняется прикладным уровнем. Дейтаграмма может быть потеряна при программных и аппаратных сбоях на пути ее прохождения, при переполнении входных и выходных очередей стека протоколов. Если получатель отсутствует в сети, то отправитель также не будет уведомлен об этом.

Протокол UDP может использовать широковещательную (broadcast) или множественную (multicast) адресацию, когда одна дейтаграмма направляется нескольким получателям.

Таким образом, по модели OSI/ISO протокол UDP является «не совсем» протоколом транспортного уровня, так как он не обеспечивает гарантированную доставку данных.

После оформления UDP-пакета он передается с помощью средств IP к адресату, который по заголовку IP-пакета определяет тип протокола и передает пакет не агенту TCP, а агенту UDP. Агент определяет номер порта и ставит пакет в очередь к этому порту.

В UDP служебная часть дейтаграммы короче, чем в TCP (8 байт вместо 20), не требуется предварительного установления соединения или подтверждения правильности передачи, как это делается в TCP, что и обеспечивает большую скорость за счет снижения надежности доставки.

UDP — минимальный ориентированный на обработку сообщений протокол транспортного уровня, задокументированный в RFC 768.

UDP не предоставляет никаких гарантий доставки сообщения для вышестоящего протокола и не сохраняет состояния отправленных сообщений. По этой причине UDP иногда называют Unreliable Datagram Protocol (англ. — ненадежный протокол датаграмм).

UDP обеспечивает многоканальную передачу (с помощью номеров портов) и проверку целостности (с помощью контрольных сумм) заголовка и существенных данных. Надежная передача в случае необходимости должна реализовываться пользовательским приложением.

Структура UDP-дейтаграммы представлена на рис. 6.4.

Биты	0 - 15	16 - 31
0-31	Порт отправителя (Source port)	Порт получателя (Destination port)
32-63	Длина датаграммы (Length)	Контрольная сумма (Checksum)
64-...	Данные (Data)	

Рис. 6.4. Структура UDP-дейтаграммы

UDP-дейтаграмма состоит из заголовка и данных. Заголовок содержит следующие поля:

- порт отправителя (16 бит);
- порт получателя (16 бит);
- длина дейтаграммы (16 бит);
- контрольная сумма (16 бит);
- данные.

Порт отправителя может содержать порт отправителя. Сетевой адрес отправителя, по которому можно послать ответ, находится в заголовке IP-дейтаграммы. Если нет необходимости посылать дейтаграммы отправителю, поле содержит нулевое значение.

Длина дейтаграммы. Это поле содержит полную длину дейтаграммы, включая заголовок и данные. Из того, что поле занимает

16 бит, следует, что максимальная длина данных равна 65 535 – 8 = = 65 527 байт. Однако большинство реализаций стека протоколов TCP/IP ограничивают длину данных в дейтаграмме 8192 байтами. Это, скорее всего, связано с тем, что с таким размером данных работает часто используемый протокол NFS (Network File System), который работает поверх протокола UDP. Другие объяснения придумать сложно.

Контрольная сумма охватывает и заголовок и данные. Поле контрольной суммы заполняется отправителем и проверяется получателем. При несовпадении расчитанной и хранимой контрольных сумм, дейтаграмма отбрасывается. В протоколе UDP заполнение и проверка контрольной суммы необязательна. Отключение заполнения и проверки может немного повысить скорость работы протокола, но применимо только в локальных сетях, где контрольная сумма и так проверяется на канальном уровне (например, в Ethernet). В глобальных сетях контрольная сумма на канальном уровне не всегда проверяется (например, при передаче по телефонной линии с использованием протокола SLIP — Serial Line Internet Protocol). В этом случае заполнение и проверка поля контрольной суммы обязательна.

6.5. Другие протоколы в стеке TCP/IP

В состав протокола IP входит ряд частных протоколов. Среди них протоколы ARP, IGP, EGP, относящиеся к маршрутизации на разных иерархических уровнях в архитектуре сети. На одном уровне с IP находится протокол управления ICMP (Internet Control Message Protocol).

Протокол ARP (Address Resolution Protocol). Относится к связям «хост-хост» или «хост-шлюз» в конкретной подсети. Он использует локальные таблицы маршрутизации — ARP-таблицы, устанавливающие соответствие IP-адресов с NPA (Network Point of Attachment) адресами серверов доступа в соответствующих подсетях. В подсетях не нужно рассчитывать кратчайший путь и определять маршрут в разветвленной сети, что, естественно, ускоряет доставку. ARP-таблицы имеются в каждом узле. Если в таблице отправителя нет строки для IP-адреса получателя, то отправитель сначала посылает широковещательный запрос. Если некоторый узел имеет этот IP-адрес, он откликается своим NPA, и отправитель пополняет свою таблицу и отсылает пакет. Иначе отправка пакета произойдет на внешний порт сети.

Узел, которому нужно выполнить отображение IP-адреса на локальный адрес, формирует ARP-запрос, вкладывает его в кадр про-

токола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно.

Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным.

В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес и отправляет его уже направленно, так как в ARP-запросе отправитель указывает свой локальный адрес.

Преобразование адресов выполняется путем поиска в таблице. Эта таблица, называемая ARP-таблицей, хранится в памяти и содержит строки для каждого узла сети. В двух столбцах содержатся IP- и Ethernet-адреса. Если требуется преобразовать IP-адрес в Ethernet-адрес, то ищется запись с соответствующим IP-адресом. Ниже приведен пример упрощенной ARP-таблицы.

Часто считают, что в состав TCP/IP входят также протоколы высоких уровней такие, как:

- SMTP (Simple Mail Transport Protocol) — почтовый протокол, который по классификации ISO можно было бы отнести к прикладному уровню;
- FTP (File Transfer Protocol) — протокол с функциями представительного уровня;
- Telnet — протокол с функциями сеансового уровня.

На нижних уровнях в TCP/IP используется протокол IEEE 802.X или X.25.

6.6. Протоколы управления в стеке TCP/IP

Рост сложности сетей повышает значимость и сложность средств управления сетью.

Среди протоколов управления различают:

1) протоколы, реализующие управляющие функции сетевого уровня;

2) протоколы мониторинга за состоянием сети, относящиеся к более высоким уровням.

В сетях TCP/IP роль первых из них выполняет протокол ICMP, роль вторых — протокол SNMP (Simple Network Management Protocol).

Основные функции ICMP:

- оповещение отправителя с чрезмерным трафиком о необходимости уменьшить интенсивность посылки пакетов; при перегрузке адресат (или промежуточный узел) посылает ICMP-пакеты, указывающие о необходимости сокращения интенсивности входных потоков;
- передача откликов (квитанций) на успешно переданные пакеты;
- контроль времени жизни T дейтаграмм и их ликвидация при превышении T или по причине искажения данных в заголовке;
- оповещение отправителя о недостижимости адресата. Отправление ICMP-пакета с сообщением о невозможности достичь адресата осуществляет маршрутизатор;
- формирование и посылка временных меток (измерение задержки) для контроля Tv — времени доставки пакетов, что нужно для «оконного» управления.

Например, время доставки Tv определяется следующим образом. Отправитель формирует ICMP-запрос с временной меткой и отсылает пакет. Получатель меняет адреса местами и отправляет пакет обратно. Отправитель сравнивает метку с текущим временем и тем самым определяет Tv.

ICMP-пакеты вкладываются в IP-дейтаграммы при доставке.

Протокол SNMP (System Network Management Protocol)

Один из протоколов семейства TCP/IP. Разработан в 1988 г. SNMP протокол верхнего уровня (6–7). Наиболее важными объектами управления являются внешние порты СУ и маршрутизаторы. Каждый управляемый объект имеет свой уникальный идентификатор. Протокол SNMP поддерживается в основе на передаче сообщений не имеющих фиксированного формата и полей.

Основные функции протоколов мониторинга SNMP:

- сбор информации о состоянии сети;
- предоставление этой информации нужным лицам путем посылки ее на соответствующие узлы;
- возможное автоматическое принятие необходимых управляющих мер.

Собственно собираемая информация о состоянии сети хранится в базе данных под названием MIB (Managment Information Base).

Примеры данных в MIB: статистика по числу пакетов и байтов, отправленных или полученных правильно или с ошибками, длины очередей, максимальное число соединений и др.

Все объекты сети InterNet разбить на 10 групп и каждой группе соответствует свое описание в этой управляющее БД — MIB.

1. Система. В MIB хранится название, № версии оборудования ОС, сетевой ОС, время последнего запуска этой системы.

2. Интерфейс, содержащий описание сетевых интерфейсов, число поддерживаемых интерфейсов, тип интерфейса, работающего под управлением IP, размер дейтограмм, скорость обмена, адрес интерфейса и т.д.

3. Обмены.

4. Трансляция адресов.

5. ПО IP.

6. ПО ICMP.

7. ПО TCP. Параметры, алгоритм для повторной пересылки, максимальное число портовых пересылок.

8. ПО UDP.

9. ПО EGP.

10. ПО SNMP. Параметры, число запросов, откликов, число полученных ошибок.

Протокол SNMP реализуется через пять типов команд (каналов) PDU.

Протокол SNMP относится к прикладному уровню в стеке протоколов TCP/IP. Он работает по системе «менеджер–агент». Менеджер (серверная программа SNMP) посылает запросы агентам, агенты (т.е. программы SNMP объектов управления) устанавливаются в контролируемых узлах, они собирают информацию (например, о загрузке, очередях, временах совершения событий) и передают ее серверу для принятия нужных мер. В общем случае агентам можно поручить и обработку событий, и автоматическое реагирование на них. Для этого в агентах имеются триггеры, фиксирующие наступление событий, и средства их обработки. Команды SNMP могут запрашивать значения объектов MIB, посылать ответы, менять значения параметров.

Для посылки команд SNMP используется транспортный протокол UDP.

Одной из проблем управления по SNMP является защита агентов и менеджеров от ложных команд и ответов, которые могут дезорганизовать работу сети. Используется шифрование сообщений, но это снижает скорость реакции сети на происходящие события.

Расширением SNMP являются протоколы RMON (Remote Monitoring) для сетей Ethernet и Token Ring и RMON2 для сетевого уровня. Преимущество RMON заключается в меньшем трафике, так как здесь агенты более самостоятельны и сами выполняют часть необходимых управляющих воздействий на состояние контролируемых ими узлов.

На базе протокола SNMP разработан ряд мощных средств управления, примерами которых могут служить продукт ManageWISE фирмы Novell или система UnicenterTNG фирмы Computer Associates. С их помощью администратор сети может:

1) строить 2D-изображение топологии сети, причем на разных иерархических уровнях, перемещаясь от региональных масштабов до подсетей ЛВС (при интерактивной работе);

2) разделять сеть на домены управления по функциональным, географическим или другим принципам с установлением своей политики управления в каждом домене;

3) разрабатывать нестандартные агенты с помощью имеющихся инструментальных средств.

Дальнейшее развитие подобных систем может идти в направлении связи сетевых ресурсов с проектными или бизнес-процедурами и сетевых событий с событиями в процессе проектирования или управлении предприятиями. Тогда система управления сетью станет комплексной системой управления процессами проектирования и управления предприятием.

6.7. Контрольные вопросы

1. Какая информация содержится в заголовке IP-пакета?
2. Чему равна минимальная и максимальная длина IP-заголовка?
3. Чему равна максимально возможная длина IP-пакета?
4. Какова основная цель перехода с протокола IPv4 на IPv6?
5. Какие особенности присущи протоколу IPv6?
6. Какую длину имеет адрес в протоколе IPv6?
7. Сколько уровней иерархии адресов предусмотрено в протоколе IPv6?
8. Какую длину имеет основной заголовок IPv6?
9. Как называется процесс разбиения длинных пакетов на более короткие в процессе передачи по сети?
10. Что такое MTU?
11. Что используется на транспортном уровне стека TCP/IP в качестве адреса?
12. Сколько портов может быть сформировано для одного прикладного процесса?
13. В чем отличие централизованного способа присвоения порта приложению от локального?
14. Назначение протоколов UDP, TCP и ICMP.
15. В чем отличие протокола UDP от TCP?

Библиографический список

1. *Олифер В.* Компьютерные сети. Принципы, технологии, протоколы [Текст]: учебник для вузов / В. Олифер, Н. Олифер. — 5-е изд. — СПб.: Питер, 2016.
2. *Таненбаум Э.* Компьютерные сети [Текст] / Э. Таненбаум, Д. Уэзеролл. — 5-е изд. — СПб.: Питер, 2016.
3. *Джеймс Ф. Куроуз.* Компьютерные сети. Настольная книга системного администратора [Текст] / Ф. Куроуз Джеймс, В. Росс Кит. — М.: Эксмо, 2016.
4. *Джеймс Ф. Куроуз.* Компьютерные сети. Нисходящий подход [Текст] / Ф. Куроуз Джеймс, В. Росс Кит. — М.: Эксмо, 2016.
5. Lammel Todd CCNA Cisco Certified Network Associate Study Guide, 2011.
6. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 640-822 [Текст] / У. Одом. — М.: Вильямс, 2015.
7. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101, 2017.
8. *Одом У.* Официальное руководство по подготовке к сертификационным экзаменам CCNA ICND 2 200-101. Маршрутизация и коммутация [Текст] / У. Одом. — М.: Вильямс, 2015.
9. *Одом У.* Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-105 [Текст] / У. Одом. — М.: Вильямс, 2017.
10. *Сергеев А.Н.* Основы локальных компьютерных сетей [Текст]: учеб. пособие / А.Н. Сергеев. — СПб.: Лань, 2016.

СОДЕРЖАНИЕ

Учебное издание

Сергей Игоревич Бабаев,
Борис Васильевич Костров,
Михаил Борисович Никифоров

КОМПЬЮТЕРНЫЕ СЕТИ. ЧАСТЬ 3. СТАНДАРТЫ И ПРОТОКОЛЫ

Учебник

Оригинал-макет подготовлен в Издательстве «КУРС»

Подписано в печать 02.07.2018.
Формат 60×90/16. Бумага офсетная. Гарнитура Newton.
Печать цифровая. Усл. печ. л. 11,0.
Тираж 500 экз. Заказ №

ТК 693924-987226-020718

ООО Издательство «КУРС»
127273, Москва, ул. Олонецкая, д. 17А, офис 104.
Тел.: (495) 203-57-83.
E-mail: kursizdat@gmail.com http://www.kursizdat.ru

Отпечатано в АО «Первая Образцовая типография»
Филиал «Чеховский Печатный Двор»
142300, Московская область, г. Чехов, ул. Полиграфистов, д. 1.
Сайт: www.chpd.ru, E-mail: sales@chpd.ru, тел.: 8(499) 270-73-59

Для заметок

Для заметок

Для заметок

Для заметок

Для заметок