Основы сетевых технологий

Учебный курс D-Link

Версия 2.0

Москва 2014

Оглавление

1 Базовые понятия сетевых технологий 6
1.1 История компьютерных сетей 6
1.2 Использование компьютерных сетей 9
1.3 Основные понятия в области компьютерных сетей 9
1.4 Классификация компьютерных сетей 11
1.5 Взаимодействие компьютеров в сети 18

2 Модели сетевого взаимодействия 20
2.1 Модель OSI 20
2.2 Уровни модели OSI 20
2.2.1 Взаимодействие между уровнями 22
2.2.2 Инкапсуляция данных 23
2.2.3 Описание уровней модели OSI 25
2.3 Модель и стек протоколов TCP/IP 27
2.3.1 Описание уровней модели TCP/IP 28

3 Физический уровень модели OSI 30
3.1 Понятие линии и канала связи 30
3.2 Сигналы 34
3.3 Основные характеристики канала связи 37
3.3.1 Полоса пропускания 37
3.3.2 Затухание 38
3.3.3 Помехоустойчивость 39
3.3.4 Пропускная способность 41
3.3.5 Достоверность передачи данных 41
3.4 Методы совместного использования среды передачи канала связи 41
3.4.1 Мультиплексирование с разделением по времени 42
3.4.2 Мультиплексирование с разделением по частоте 45
3.4.3 Мультиплексирование со спектральным разделением 47
3.4.4 Мультиплексирование с кодовым разделением 49
3.4.5 Мультиплексирование и методы множественного доступа 50
3.5 Модуляция и кодирование сигналов 51
3.5.1 Методы аналоговой модуляции 52
3.5.2 Методы импульсной модуляции 53
3.5.3 Методы цифровой модуляции 55
3.5.4 Методы цифрового кодирования 56
3.6 Стандарты кабелей 61
3.6.1 Основные характеристики электрических кабелей 62
3.6.2 Коаксиальный кабель 63
3.6.3 Кабель на основе витой пары 64
3.6.4 Волоконно-оптический (оптоволоконный) кабель 71
3.6.5 Кабельные системы 76
3.6.6 Структурированные кабельные системы 77
3.6.7 Медиаконвертеры 78

3.7 Электрическая проводка 80
3.8 Беспроводная среда передачи 84
3.8.1 Распространение сигналов в беспроводных средах передачи 88

4 Топологии компьютерных сетей 93
4.1 Понятие топологии сети 93
4.2 Сетевое оборудование в топологии 93
4.2.1 Повторители и концентраторы 94
4.2.2 Мосты и коммутаторы 96
4.2.3 Маршрутизаторы 99
4.2.4 Средства управления сетевыми устройствами 103
4.3 Обзор сетевых топологий 107
4.3.1 Топология «шина» 107
4.3.2 Топология «кольцо» 108
4.3.3 Последовательное соединение 109
4.3.4 Топология «звезда» 111
4.3.5 Топология «дерево» 112
4.3.6 Ячеистая топология 113

5 Канальный уровень модели OSI 116
5.1 Методы коммутации 116
5.1.1 Коммутация каналов 116
5.1.2 Коммутация пакетов 118
5.2 Сетевые протоколы и методы коммутации 120
5.3 Протоколы канального уровня 121
5.3.1 Структура кадра данных 121
5.4 Протоколы локальных сетей 122
5.4.1 Протокол LLC 123
5.4.2 Подуровень MAC 124
5.4.3 Понятие MAC-адреса 124
5.4.4 Сетевые адаптеры 127
5.5 Технологии локальных сетей 129
5.5.1 Технология Token Ring 129
5.5.2 Технология FDDI 131
5.6 Технология Ethernet 132
5.6.1 Форматы кадров Ethernet 133
5.6.2 Дуплексный и полудуплексный режимы работы 137
5.6.3 Метод доступа CSMA/CD 137
5.6.4 Коммутируемая сеть Ethernet 142
5.6.5 Управление потоком в полудуплексном и полнодуплексном режимах 144
5.7 Физический уровень технологии Ethernet 145
5.7.1 Спецификации физической среды Ethernet (10 Мбит/с) 148
5.7.2 Спецификации физической среды Fast Ethernet (100 Мбит/с) 149
5.7.3 Автосогласование 150
5.7.4 Спецификации физической среды Gigabit Ethernet (1000 Мбит/с) 151

5.7.5 Спецификации физической среды 10 Gigabit Ethernet (10 Гбит/с) 152
5.7.6 Спецификации физической среды 40 и 100 Gigabit Ethernet 154
(40 и 100 Гбит/с) 154
5.8 Энергоэффективный Ethernet 156
5.9 Сменные интерфейсные модули 157

6 Технологии коммутации 162
6.1 Алгоритм прозрачного моста 162
6.2 Методы коммутации 165
6.3 Конструктивное исполнение коммутаторов 166
6.4 Физическое стекирование коммутаторов 168
6.5 Технологии коммутации и модель OSI 169
6.6 Программное обеспечение коммутаторов 169
6.7 Общие принципы сетевого дизайна 170
6.8 Трехуровневая иерархическая модель сети 170
6.9 Протокол Spanning Tree Protocol (STP) 172
6.9.1 Построение активной топологии связующего дерева 174
6.9.2 Bridge Protocol Data Unit (BPDU) 177
6.9.3 Состояния портов 178
6.9.4 Таймеры STP 180
6.9.5 Изменение топологии 180
6.9.6 Настройка STP 181
6.10 Виртуальные локальные сети (VLAN) 184
6.10.1 Типы VLAN 187
6.10.2 VLAN на основе портов 187
6.11 VLAN на основе стандарта IEEE 802.1Q 189
6.11.1 Некоторые определения IEEE 802.1Q 190
6.11.2 Тег VLAN IEEE 802.1Q 191
6.11.3 Port VLAN ID 192
6.11.4 Продвижение кадров VLAN IEEE 802.1Q 192
6.11.5 Пример настройки VLAN IEEE 802.1Q 196
6.12 Технология Power over Ethernet 202

Обозначения, используемые в книге

В тексте книги используются следующие пиктограммы для обозначения сетевых устройств различных типов:

1 Базовые понятия сетевых технологий

1.1 История компьютерных сетей

Концепция вычислительных сетей является логическим результатом эволюции компьютерных технологий. В 1940-х годах компьютеры были огромными электромеханическими устройствами, которые часто выходили из строя. В 1947 году, с изобретением полупроводниковых транзисторов, появились перспективы создания небольших по размерам, более надежных компьютеров. В 1950-х стали широко использоваться *мэйнфреймы* – мощные и надежные компьютеры универсального назначения, команды программ и данные для которых содержались на *перфокартах.*

Перфокарта – носитель информации, изготавливаемый из тонкого картона, информация на котором представлялась наличием или отсутствием отверстий в определенных позициях.

На основе мэйнфреймов строили *системы пакетной обработки* данных.

Мэйнфреймы представляли собой высокопроизводительные компьютеры общего назначения со значительным объемом оперативной и внешней памяти и предназначались для выполнения интенсивных вычислительных работ. Такие компьютеры были большие, громоздкие и дорогие, часто они занимали по объему комнаты и целые здания.

В конце 50-х годов были изобретены интегральные схемы. В 60-х годах, по мере удешевления процессоров, появились новые способы организации вычислительного процесса. Начали развиваться *интерактивные многотерминальные системы*, работающие в режиме разделения времени, что стало первым шагом на пути создания локальных компьютерных сетей. В таких системах использовались мэйнфреймы с подключенными к ним терминалами, причем терминалы могли быть рассредоточены на территории всего предприятия. Несмотря на то, что подобные многотерминальные системы были похожи на локальные компьютерные сети, подключение к мэйнфреймам удаленных терминалов не являлось сетевым взаимодействием, т. к. терминалы обеспечивали только преобразование формы информации, но не ее обработку. Такие среды строились на основе системной архитектуры IBM (System Network Architecture, SNA) или на основе сетевой архитектуры Digital.

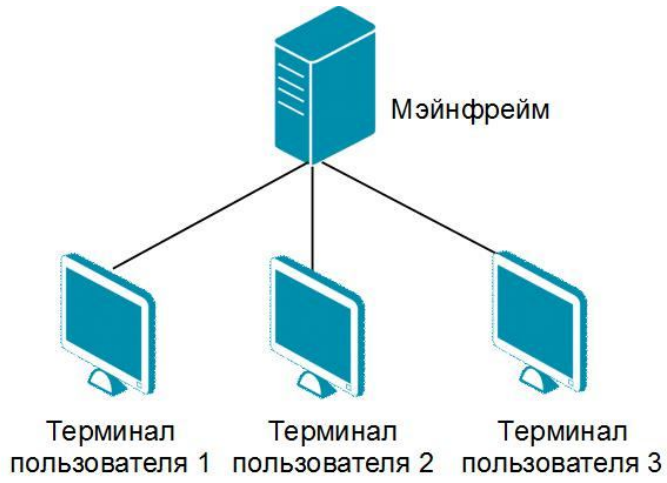


Рис. 1.1 Интерактивная многотерминальная система

В конце 60-х – начале 70-х годов появление *больших интегральных схем (БИС)* привело к созданию мини-компьютеров, которые стали реальными конкурентами мэйнфреймов. В 1978 году компания Apple Computer выпустила персональный компьютер. Через три года появился компьютер, созданный компанией IBM, который был дешевле своего предшественника. Низкая стоимость и большая функциональность привели к широкому использованию персональных компьютеров для дома и бизнеса. Каждый компьютер выполнял свою задачу, таким образом, появилась идея разделения компьютерных ресурсов по всему предприятию, однако при этом каждый компьютер должен оставаться автономно работающим устройством. Очень скоро стала очевидна низкая эффективность такого подхода. Необходимо было найти решение, которое удовлетворяло бы следующим требованиям: устраняло дублирование оборудования и ресурсов, обеспечивало эффективный обмен информацией между устройствами, снимало проблему управления взаимосвязанными устройствами. Предприятия и организации начали объединять свои компьютеры в сеть или расширять существующие сети, причем делали они это с той же скоростью, с которой появлялись новые сетевые технологии. В результате в начале 80-х годов произошел стремительный рост в области объединения компьютеров в сеть. Так появились первые *локальные сети (LAN, Local Area Network)*.

Компьютерная сеть (сеть передачи данных) — группа устройств, объединенных между собой каким-либо способом с целью совместного доступа к ресурсам и обмена информацией.

В середине 80-х годов появились проблемы, связанные с хаотичным развитием локальных сетей. Многие сетевые технологии оказались несовместимыми друг с другом, поскольку у них была разная аппаратная и программная реализация. В результате чего сетям, использующим разные спецификации, было трудно взаимодействовать друг с другом.

Возникла необходимость в стандартизации правил сетевого взаимодействия. Решением этой проблемы стало появление стандартов на локальные вычислительные сети. В 1983 г. Институт инженеров по электротехнике и электронике (IEEE) принял стандарт IEEE 802.3 на технологию *Ethernet*, разработанную Робертом Меткалфом в 1973 г. В 1985 г. был принят стандарт IEEE 802.5 на технологию *Token Ring*, изначально разработанную компанией IBM. В середине 80-х стали популярными технологии *FDDI* (Fiber Distributed Data Interface) и *ARCNET* (Attached Resource Computer NETwork).

Стандартные технологии превратили процесс построения локальных сетей из искусства в рутинную работу. Для создания сети достаточно было приобрести сетевой адаптер соответственного стандарта, например Ethernet, подключить к нему кабель и установить на компьютер соответствующую сетевую операционную систему.

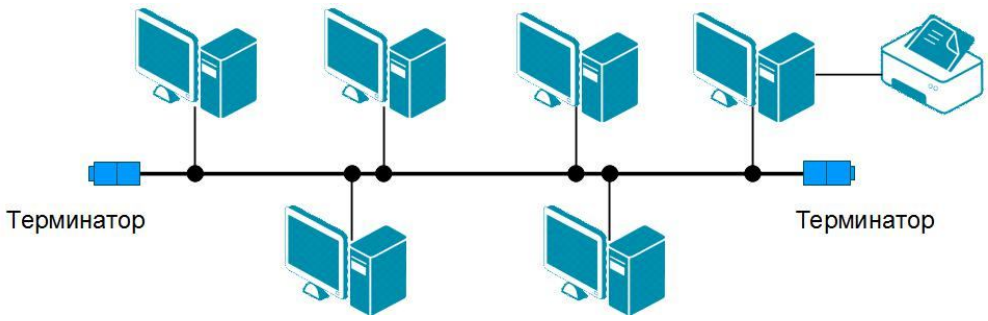


Рис. 1.2 Локальная сеть на основе технологии Ethernet

По мере увеличения числа компьютеров в организациях и на предприятиях, вскоре стало очевидно, что только локальных сетей уже недостаточно. Требовалось найти способ

передачи информации от одной локальной сети к другой, которые находились на больших расстояниях друг от друга. Решение этой проблемы было найдено в создании *глобальных сетей* (*WAN, Wide Area Network*). Началось все с простой задачи – доступа к компьютеру с терминалов, удаленных от него на сотни и тысячи километров. Терминалы объединялись с компьютерами через телефонные сети с помощью модемов. Затем появились системы, в которых наряду с удаленными соединениями типа терминал-компьютер были реализованы и удаленные связи компьютер-компьютер. Компьютеры получили возможность обмениваться данными в автоматическом режиме. С использованием этого механизма, в первых сетях были реализованы службы обмена файлами, синхронизации баз данных, электронной почты и другие службы, ставшие теперь традиционными.

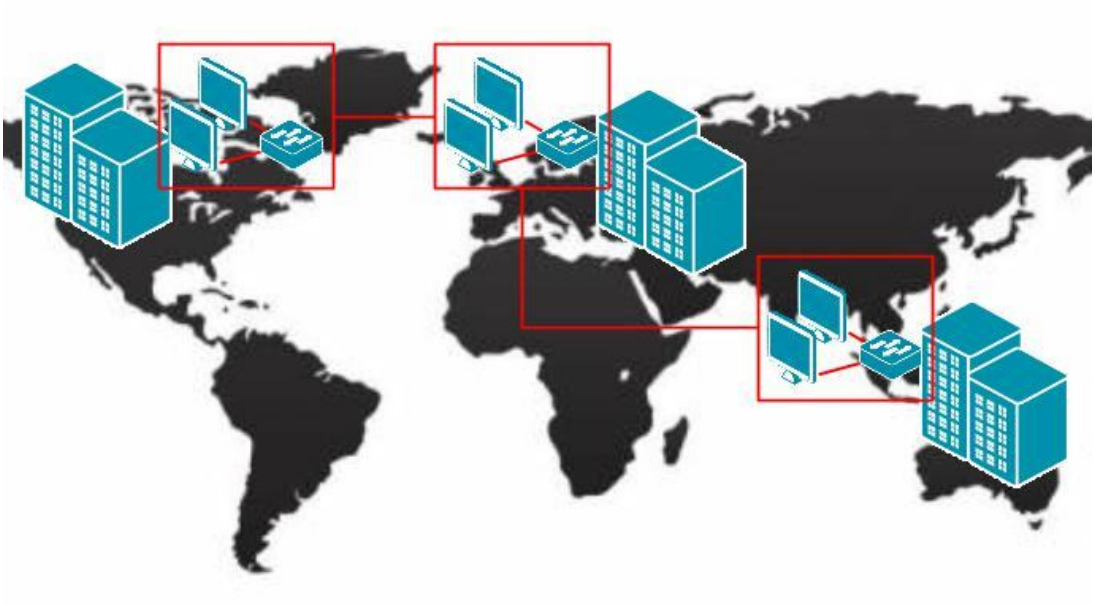


Рис. 1.3 Глобальная сеть

Начиная с 60-х годов и продолжая в 70, 80, 90-х годах, Министерство обороны США проводило работы по созданию большой и надежной глобальной сети. В 1969 году Министерство обороны США посчитало, что на случай войны Америке нужна надежная система передачи информации. Агентство передовых исследовательских проектов (ARPA) предложило разработать для этого компьютерную сеть. Разработка такой сети была поручена Калифорнийскому университету в Лос-Анджелесе, Стэндфордскому исследовательскому центру, Университету штата Юта и Университету штата Калифорния в Санта-Барбаре. Первое испытание технологии произошло 29 октября 1969 года. Сеть состояла из двух терминалов, один из которых находился в Калифорнийском университете, а второй на расстоянии 600 км от него – в Стэндфордском университете.

Компьютерная сеть была названа ARPANET, которая в рамках проекта объединила четыре указанных научных учреждения. Затем сеть ARPANET начала активно увеличиваться и развиваться, ее начали использовать ученые из разных областей науки.

В 1973 году к сети ARPANET были подключены первые иностранные организации из Великобритании и Норвегии, сеть стала международной. Параллельно с ARPANET стали появляться и формироваться другие сети университетов и предприятий.

1 января 1983 года сеть ARPANET была полностью переведена с протокола Network Control Protocol (NCP) на протокол TCP/IP (Transmission Control Protocol/Internet Protocol) и стала первой подсетью будущей сети Интернет. Впоследствии было принято решение о принятии протокола TCP в качестве стандарта Министерства обороны США и о последующем выделении военного сегмента сети MILnet, что сократило сеть ARPANET с 113 до 68 узлов. В это же время произошли другие важные события: протокол TCP/IP вошел

в операционную систему Berkeley Unix (4.2 BSD), что стало толчком для появления целого поколения компьютеров – рабочих Unix-станций.

Стек протоколов TCP/IP создавался продолжительное время в течение нескольких лет. Впервые о TCP/IP было сказано в 1973 году на заседании International Network Working Group, прошедшем в Великобритании, где Роберт Кан и Винт Серф выступили с проектом статьи, которая позже, в мае 1974 года, была опубликована в одном из самых престижных журналов Transactions on Communications, выпускаемом институтом IEEE. В статье, озаглавленной «A Protocol for Packet Network Intercommunication», были изложены основы будущего протокола TCP/IP, в становление которого каждый из соавторов внес свой вклад. Кан был одним из ведущих сотрудников компании BBN, которая изготовила связное оборудование для ARPANET, и самостоятельно подошел к идеям, близким к TCP, а Серф занимался аналогичными задачами в Стэндфордском университете.

Главная идея, предложенная авторами, состояла в том, чтобы перенести обеспечение надежности коммуникаций из сети в подключенные к ней серверы. Идея оказалась отличной и была принята учеными и военными одновременно. После этого протокол начал жить своей жизнью, пока еще под названием TCP. В совершенствовании нового протокола приняли участие многие инженеры и ученые, в итоге к октябрю 1977 года его работу удалось продемонстрировать не только в ARPANET, но и в пакетной радиосети, а также спутниковой сети SATNET.

К разработке протокола присоединились Джонатан Постел и Дэни Коэн, которые вместе с Каном и с Серфом пришли к выводу о необходимости разделения протокола на две части. В результате появились протоколы TCP и IP. Протокол TCP отвечает за разбиение сообщения на сегменты, сборку их на стороне получателя, обнаружение ошибок и восстановление порядка сегментов, если он был нарушен в процессе передачи. Протокол IP, или Internet Protocol, отвечает за маршрутизацию отдельных сообщений. К 1978 году стек протоколов TCP/IP окончательно оформился в том виде, в каком он известен сегодня.

1.2 Использование компьютерных сетей

За последние 15-20 лет миллионы компьютеров в мире были объединены в сети и миллиарды пользователей получили возможность взаимодействовать друг с другом. Сейчас можно с уверенностью сказать, что компьютерные сети стали неотъемлемой частью нашей жизни, а область их применения охватывает буквально все сферы человеческой деятельности. Сети позволяют объединять компьютеры и пользователей этих компьютеров, совместно использовать аппаратные ресурсы и данные большому количеству людей, быстро обмениваться важной информацией, используя, например, электронную почту, ICQ или сервисы социальных сетей. С помощью сетей появилась возможность искать информацию, используя поисковые системы, организовывать видеонаблюдение за удаленными объектами, заниматься электронной коммерцией, получать образование или просто развлекаться, играя, например, с друзьями в сетевые игры или просматривая ролики на YouTube.

1.3 Основные понятия в области компьютерных сетей

Прежде чем приступить к изучению технологий и принципов работы сетей, необходимо познакомиться с основными понятиями, которые будут использоваться в курсе.

Компьютерная сеть (сеть передачи данных) представляет собой совокупность узлов (компьютеров, сетевых принтеров, IP-камер, IP-телефонов, дисковых массивов), объединенных с помощью каналов связи (кабельных или беспроводных) и сетеобразующего телекоммуникационного оборудования (коммутаторов, маршрутизаторов, модемов, точек доступа и т.д.) в единую систему для обмена сообщениями и доступа пользователей к программным, техническим, информационным и организационным ресурсам сети.

Ресурсы – программы, файлы данных, совместно используемые периферийные сетевые устройства (принтеры, дисковые массивы, многофункциональные устройства и т.д.).

Среда передачи (канал связи, линия связи) – физическая среда распространения сигналов (электрических, оптических или электромагнитного излучения) от источника к приемнику.

Компьютерную сеть, как правило, представляют как совокупность *узлов*.

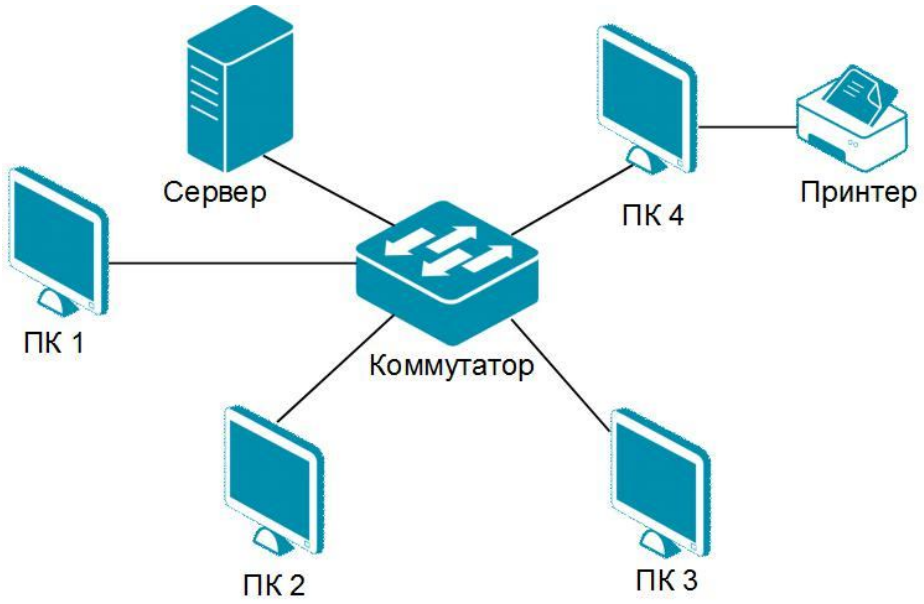


Рис. 1.4 Компьютерная сеть

Узел (абонент, хост) – оконечное устройство (компьютер, сетевой принтер, IP-камера, IP-телефон, дисковый массив), непосредственно подключенное к сетеобразующему телекоммуникационному оборудованию.

Компьютерные сети бывают *одноранговыми*, т.е. такими, где все компьютеры равноправны (каждый компьютер выполняет функции клиента и сервера) и *сети с выделенным сервером (клиент-серверные)*.

Сервер – специально выделенный высокопроизводительный компьютер, оснащенный соответствующим программным обеспечением, централизованно управляющий работой сети и/или предоставляющий другим компьютерам свои ресурсы (файлы данных, накопители, процессорное время и т.д.).

Клиентский компьютер (клиент, рабочая станция) – компьютер пользователя сети, получающий доступ к ресурсам сервера(ов).

Одной из важных характеристик сети является скорость передачи данных. Максимально возможную скорость передачи данных по линии связи характеризует **пропускная способность** *(throughput)*. Пропускная способность измеряется в битах в секунду (бит/с), а также производных единицах, таких как килобит в секунду (Кбит/с), мегабит в секунду (Мбит/с), гигабит в секунду (Гбит/с) и т. д. Обращаем внимание, что в отличие от компьютеров, где данные ассоциируются с потоком *байтов*, в компьютерных сетях данные рассматриваются как поток *битов*.

На максимально возможную скорость передачи информации по линии связи влияет ее **полоса пропускания** *(bandwidth),* которая определяет частотный диапазон сигналов, пропускаемых линией связи без значительных искажений.

При большом количестве компьютеров в сети возникает задача ее **сегментации**, т.е. разделения сети на сегменты с целью уменьшения в них количества узлов, увеличения пропускной способности в расчете на один узел и повышения безопасности.

Сегмент сети – логически или физически обособленная часть сети.

Управляет сетью или ее сегментом *системный администратор*. **Системный администратор (администратор сети)** – должностное лицо, ответственное за работу локальной сети или ее части. В его обязанности входит *администрирование сети*. **Администрирование сети** – решение целого комплекса задач по управлению и настройке компьютеров и сетевого оборудования, управлению доступом пользователей к ресурсам сети, защите данных, установке и модернизации системного и прикладного программного обеспечения, что позволяет поддерживать стабильную работу сети. Управлением сложно структурированных сетей занимаются группы администраторов.

1.4 Классификация компьютерных сетей

Компьютерные сети можно классифицировать следующим образом:

- по территориальному признаку;
- по типу среды передачи;
- по скорости передачи информации;
- по типу функционального взаимодействия;
- по типу сетевой топологии;
- по функциональному назначению;
- по сетевым операционным системам;
- по режиму доступа пользователей;
- по роли в многоуровневой архитектуре сети.

Фундаментальной является *классификация сетей по их территориальному признаку*. В зависимости от расстояния между узлами компьютерные сети можно разделить на *локальные*, *глобальные* и *городские*.

Локальная сеть *(Local Area Network, LAN)* – группа узлов, связанных друг с другом и расположенных на небольшой территории. В общем случае локальная сеть представляет собой коммуникационную систему, принадлежащую одной организации. В качестве примера локальной сети можно привести домашние сети, офисные сети, школьные сети, сети предприятий. Локальные сети характеризуются высокими скоростями передачи данных. Наиболее распространенные технологии локальных сетей – Ethernet и семейство стандартов IEEE 802.11 для беспроводных локальных сетей (Wireless Local Area Network, WLAN).

Небольшие локальные сети, радиус действия которых ограничен несколькими метрами и которые предназначены для объединения устройств, используемых одним человеком (или небольшой группой людей) называются **персональными локальными сетями** (*Personal Area Network, PAN*). Чаще всего этот термин применяется к сетям беспроводной технологии Bluetooth (IEEE 802.15).

Разновидностью локальной сети можно считать сеть кампуса. **Сеть кампуса** *(Campus Area Network, CAN)* представляет собой компьютерную сеть, соединяющую локальные сети на географически ограниченном пространстве, например, университетский городок, корпоративный кампус или военная база. Сеть кампуса больше, чем обычная локальная сеть, но меньше, чем городская сеть. Как правило, в сетях кампусов используются высокоскоростные технологии семейства Ethernet.

Глобальная сеть *(Wide Area Network, WAN)* – компьютерная сеть, охватывающая большие территории и включающая в себя сети городов, стран, континентов. Самой популярной глобальной сетью является сеть Интернет. Глобальные сети предназначены для объединения различных сетей так, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети. Некоторые глобальные сети построены исключительно для определенных организаций и являются частными, другие организованы операторами связи и являются средством подключения домашних локальных сетей или локальных сетей организаций к Интернет. Глобальные сети могут быть созданы на основе выделенных линий (соединение типа «точка-

точка» между двумя компьютерами или локальными сетями) или методов, основанных на коммутации каналов, пакетов или ячеек. Наиболее распространенными протоколами и технологиями глобальных сетей являются SONET/SDH, MPLS, HDLC, PPP, xDSL, GPON, ATM, семейство Ethernet.

Городская сеть или **сеть мегаполиса** *(Metropolitan Area Network, MAN)* – компьютерная сеть, связывающая множество локальных сетей на территории одного города. Городская сеть сочетает в себе признаки как локальной, так и глобальной сети. Для нее характерна большая плотность подключения конечных абонентов, высокоскоростные линии связи и большая протяженность каналов связи. В качестве примера городских сетей можно привести опорную сеть провайдера, сеть кабельного телевидения. В большинстве случаев в городских сетях используются оптические линии связи и технологии семейства Ethernet (т.е. Metro Ethernet). Однако каналы связи между локальными сетями могут быть организованы и без применения кабелей. Разработки, связанные с высокоскоростным беспроводным доступом в Интернет, привели к созданию **беспроводных MAN** *(Wireless Metropolitan Area Networks, WMAN)*, которые описаны в семействе стандартов IEEE 802.16 (коммерческое название WiMAX).

Объединение глобальных, городских и локальных сетей позволяет создавать многоуровневые иерархии, которые представляют собой мощные средства для обработки больших массивов данных и доступа к практически неограниченным информационным ресурсам.

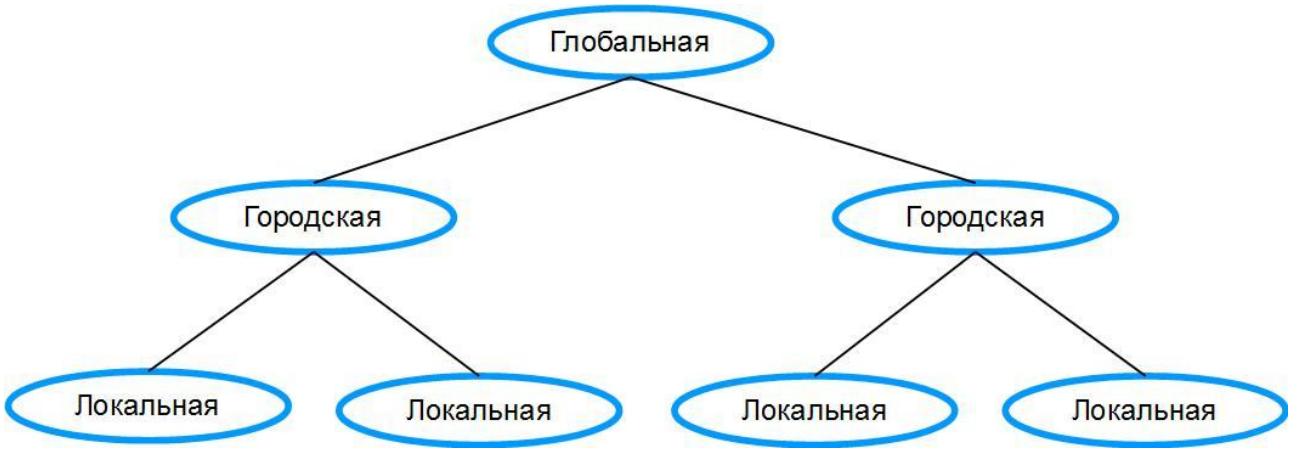


Рис. 1.5 Пример объединения сетей

Локальные сети в качестве компонентов могут входить в городские сети, городские сети – в глобальные. Глобальные сети могут образовывать еще более крупные системы. Самым крупным объединением компьютерных сетей в масштабах планеты является сеть Интернет.

Примером взаимодействия локальных и глобальных сетей является **виртуальная частная сеть** *(Virtual Private Network, VPN)* – сеть организации, получившаяся в результате объединения двух или нескольких территориально распределенных локальных сетей с помощью общедоступных каналов глобальных сетей, например, сети Интернет.

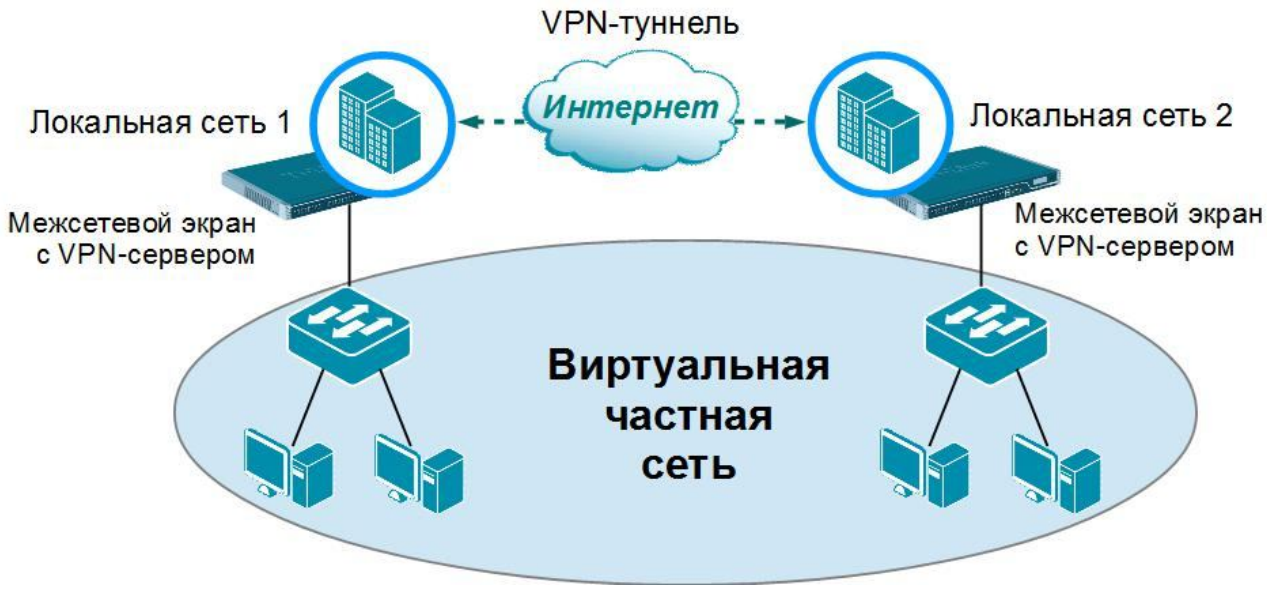


Рис. 1.6 Виртуальная частная сеть

Другими словами, крупную сеть можно описать как структуру, состоящую из множества объединенных друг с другом сетей меньшего размера или их частей. Эта концепция важна для понимания сетевых технологий, т.к. некоторые из них наилучшим образом можно объяснить, рассмотрев большую сеть целиком на верхнем уровне иерархии, а разъяснение других технологий требует детального рассмотрения работы входящих в нее частей.

Здесь необходимо сделать небольшое отступление, чтобы познакомиться с терминами, которые являются важными концепциями проектирования сетей и используются для описания относительного размера сетей и их частей. Наиболее часто используемыми из них являются:

- **Сеть** *(Network)* – общий термин, который не редко используют для обозначения различных понятий. Сеть может быть практически любого размера, от двух устройств до тысяч. Когда сеть большая и состоит из множества соединенных между собой сетей меньших размеров, она уже называется составной сетью (Internetwork). Однако, несмотря на это, часто можно услышать, например, «Корпоративная сеть D-Link», хотя понятно, что она состоит не менее чем из тысячи компьютеров.
- **Подсеть** *(Subnetwork, subnet)*. Этот термин имеет несколько значений. Подсеть – это часть сети или сеть, которая является частью большой составной сети. Также термин «подсеть» имеет специальное значение в контексте IP-адресации.
- **Сегмент** *(Сегмент сети, segment, network segment)*. Этот термин, также как и термин «подсеть», имеет несколько значений. Сегментом можно назвать небольшую часть сети, в некоторых контекстах, под сегментом подразумевают «подсеть» и термины используются взаимозаменяемо. Однако наиболее часто под термином «сегмент» понимают обособленную часть сети, меньшую, чем подсеть. В основном сети проектируют таким образом, чтобы компьютеры, связанные друг с другом или используемые одной группой людей, помещались в один сегмент сети.

  Существует проблема двоякого использования термина «сегмент» в технологии Ethernet. Первые спецификации физического уровня Ethernet использовали коаксиальный кабель, который сам по себе назывался «сегмент». Этот сегмент совместно использовался всеми, подключенными к нему устройствами и получил название «домена коллизий» (collision domain) сети.

  Для каждого физического уровня технологии Ethernet были определены правила, регламентирующие количество устройств в одном сегменте, длину сегмента, способ соединения сегментов друг с другом в зависимости от используемого сетевого

оборудования. Например, такие устройства как повторители и концентраторы увеличивали домен коллизий, в то время как коммутаторы разделяли один большой домен коллизий на несколько меньших. Со временем термины «домен коллизий» и «сегмент» стали взаимозаменяемыми. Таким образом, сегодня в технологии Ethernet термин «сегмент» используется как для обозначения части кабеля, а также для электрически соединенных кабелей, представляющих один домен коллизий.

Еще одно значение термина «сегмент» связано с протоколом TCP. Сегментом называется сообщение, отправляемое этим протоколом.

- **Составная сеть** *(Internetwork, Internet)*. Значение этого термина может иметь общее или конкретное значение, в зависимости от контекста. В некоторых технологиях «internetwork» используется для обозначения большой сетевой структуры, состоящей из множества меньших по размеру сетей. В других – это сеть, выделенная из составной сети на основе способа подключения устройств.

  Например, под сетью часто подразумевают группу узлов, соединенных на канальном уровне модели OSI (Open Systems Interconnection Reference Model) по технологии Ethernet с помощью коммутаторов. Составная сеть формируется, когда эти сети объединяются между собой на третьем уровне модели OSI с помощью маршрутизаторов.

  Исходя из *роли в многоуровневой архитектуре* сети могут подразделяться на:
  - абонентские сети (*susbscriber network*);
  - сети доступа (*access network*);
  - магистральные сети (*backbone, backbone network*).

Абонентские сети представляют собой домашние, офисные или корпоративные локальные сети.

Под *сетями доступа* понимаются местные сети, необходимые для подключения оконечного оборудования абонентских сетей к узлам магистральной сети предприятия или оператора связи.

Под магистральными сетями понимаются территориально-распределенные сети, которые выполняют функции переноса (транспортирования) потоков сообщений из одной сети доступа в другую. Узлы магистральных сетей (коммутаторы, маршрутизаторы) обычно соединяются высокоскоростными и надежными каналами связи (оптическими или спутниковыми).

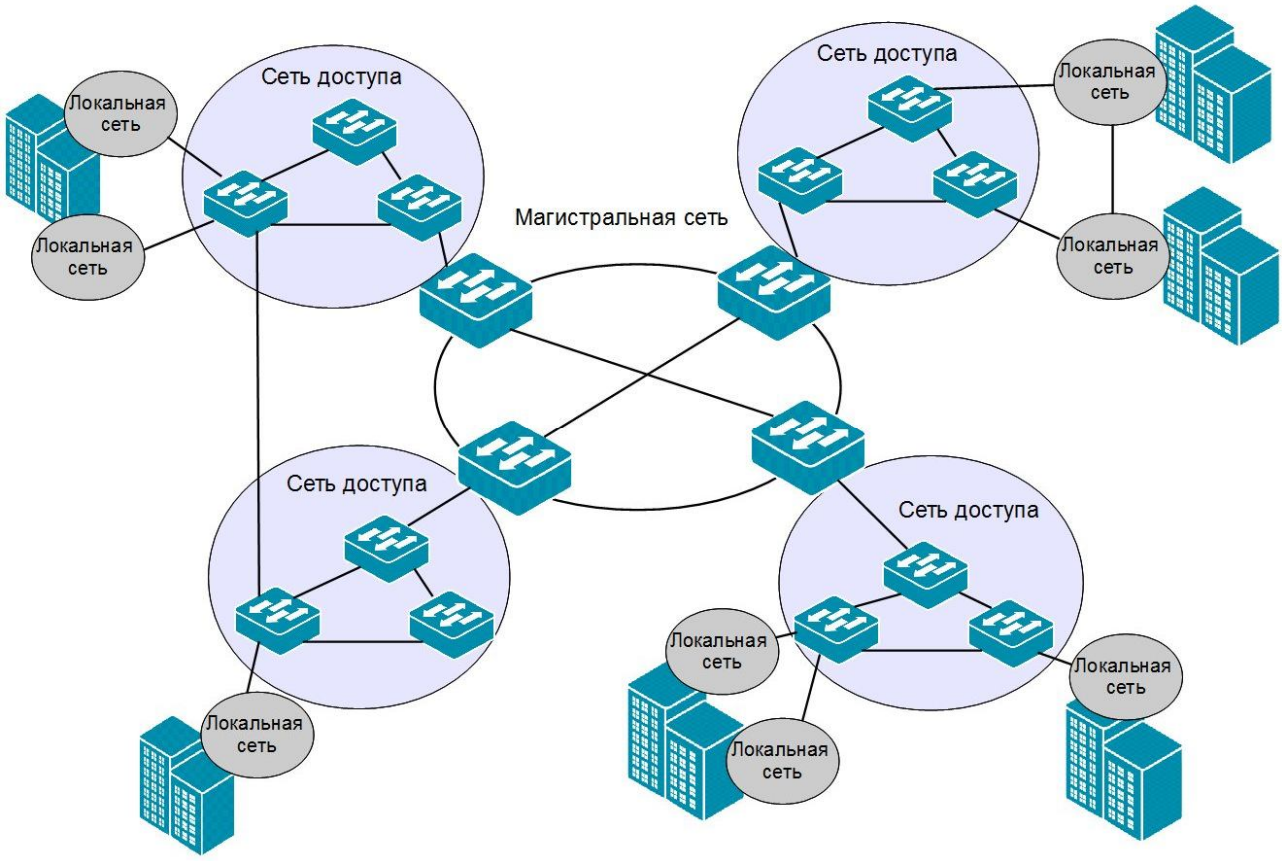


Рис. 1.7 Подключение сетей доступа к магистральной сети

По режиму доступа пользователей все существующие сети делятся на: **сети общего пользования** (*public*) и **частные сети** (*private*). Сеть общего пользования – это сеть, к которой может получить доступ любой пользователь. К сетям связи общего пользования относятся Интернет, телефонные сети общего пользования, сети теле- и радиовещания. К частной сети имеет доступ только ограниченная группа людей, как правило, домашние пользователи, служащие фирм, предприятий. К частным сетям относятся домашние, корпоративные, профессиональные, производственно-технологические сети.

По типу среды передачи компьютерные сети можно разделить на *проводные* и *беспроводные*.

Проводные сети для передачи данных используют электрические кабели (коаксиальные, витая пара) или волоконно-оптические кабели.

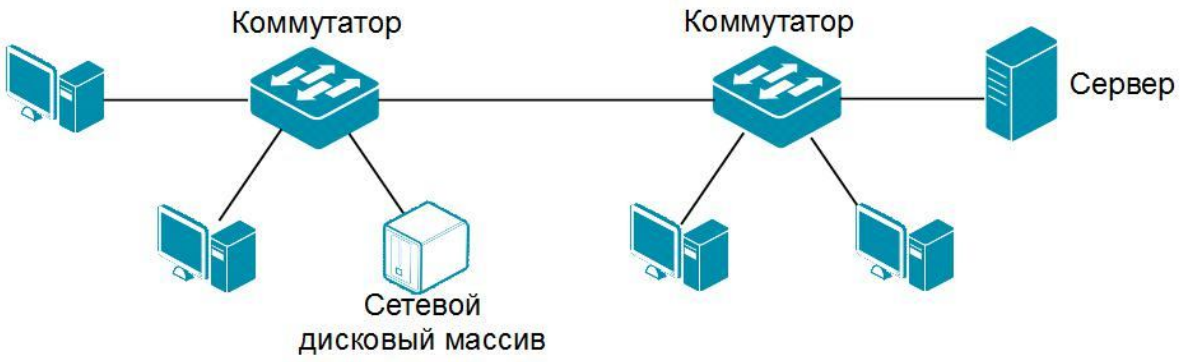


Рис. 1.8 Проводная сеть

В **беспроводных сетях** передача информации осуществляется с использованием электромагнитных волн в определенном частотном диапазоне.

Рис. 1.9 Беспроводная сеть

Одним из немаловажных вопросов при построении сети остается вопрос совместного использования ресурсов и организации взаимодействия компьютеров. В частности проектировщики решают возлагать или нет на какие-либо выделенные устройства сети функции управления ресурсами и доступом пользователей, или каждое устройство будет выполнять определенную работу в общем процессе предоставления сетевых сервисов.

По типу взаимодействия между компьютерами и с точки зрения распределения ролей между ними различают *одноранговые* и *клиент-серверные* сети.

В **одноранговой сети** *(peer-to-peer)* все компьютеры равноправны. Каждый из них может выступать как в роли сервера, предоставляя файлы и аппаратные ресурсы (принтеры, жесткие диски и т.д.) другим компьютерам, так и в роли клиента, пользующегося ресурсами других компьютеров. Число компьютеров в одноранговых сетях обычно не превышает десяти, поэтому их другое название – рабочая группа. Примерами рабочих групп являются домашние сети или сети небольших офисов.

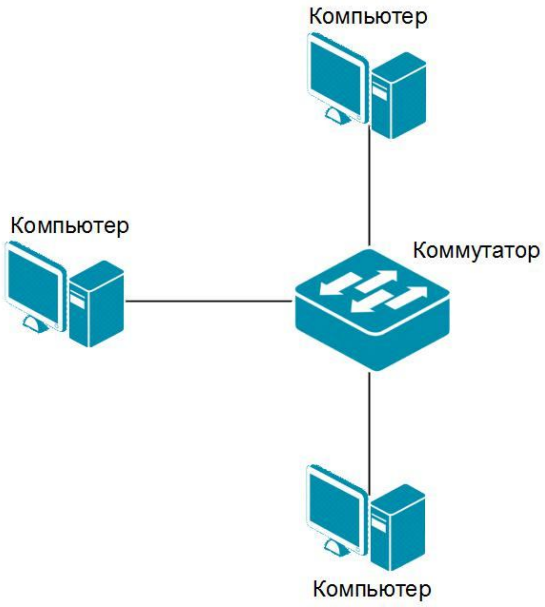


Рис. 1.10 Одноранговая сеть

Сети типа **«клиент-сервер»** *(client-server)*, как правило, создаются в учреждениях или крупных предприятиях. В таких сетях выделяется один или несколько компьютеров, называемых серверами, задача которых состоит в быстрой и эффективной обработке большого числа запросов других компьютеров – клиентов. Клиентские запросы бывают разными – начиная с простейшей проверки имени пользователя и пароля при входе в

систему, заканчивая сложными поисковыми запросами к базам данных. Обычно в роли серверов выступают мощные и надежные компьютеры, которые имеют большой объем памяти, более емкие хранилища данных, высокоскоростные сетевые адаптеры для подключения к сети. Такие компьютеры работают постоянно, круглосуточно предоставляя пользователям свои ресурсы и обеспечивая доступ к своим службам, т.е. работающим на них программам.

Службы (services) – программы, работающие на серверах и выполняющие какие-либо действия по запросу клиента.

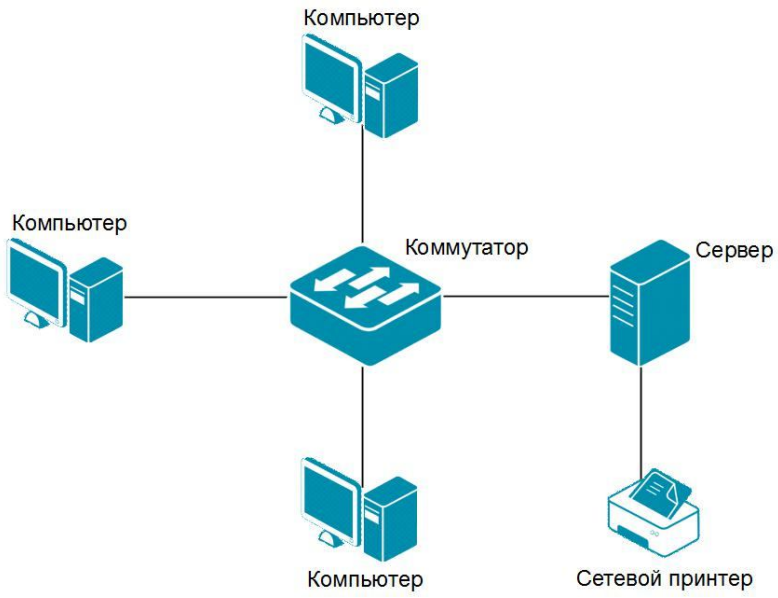


Рис. 1.11 Сеть типа «клиент-сервер»

Выбор модели взаимодействия между компьютерами зависит от конкретных потребностей определенной сети. Преимуществом одноранговых сетей является простота настройки, низкая стоимость развертывания и поддержки, независимость компьютеров и их ресурсов друг от друга, отсутствие необходимости в дополнительном программном обеспечении (кроме сетевой операционной системы) и в постоянном присутствии системного администратора. Поэтому традиционно такая модель используется в небольших сетях. Недостатками одноранговых сетей является отсутствие возможности централизованного управления сетью, доступа к данным и, как следствие, их низкая защищенность.

Клиент-серверная модель обеспечивает преимущества в части производительности, масштабируемости (т.е. расширяемости), безопасности сети и возможности централизованного управления, но обладает высокой стоимостью сопровождения, сложностью в развертывании и поддержке (требуется постоянное присутствие квалифицированного системного администратора) и наличием единой точки отказа (неисправность сервера может сделать всю сеть практически неработоспособной, а ресурсы недоступными). Тем не менее, в настоящее время сети типа «клиент-сервер» являются самыми распространенными. Клиент-серверная модель наиболее подходит для больших сетей, однако также используется в небольших сетях из-за возможности организации централизованного управления ресурсами и доступом пользователей.

Необходимо упомянуть еще одну причину доминирования клиент-серверной модели. Клиент-серверная архитектура является основой большинства сервисов и протоколов стека TCP/IP. Например, Web-браузер, который используется для просмотра страниц в Интернете,

по сути, является программным Web-клиентом, а сайт, к ресурсам которого пользователь получает доступ, является Web-сервером.

1.5 Взаимодействие компьютеров в сети

Для обеспечения взаимодействия компьютеров, объединенных в сеть, в первую очередь требуется связать между собой всех участников сети – серверы, рабочие станции пользователей, ноутбуки, планшеты, принтеры, сетевые массивы хранения данных и т.д. Решить данную задачу можно с помощью сетевых кабелей различных типов, телефонных или спутниковых каналов, и популярных в последнее время беспроводных решений – сетей Wi-Fi, 3G, 4G.

Рис. 1.12 Кабель на основе витой пары с разъемами

При использовании кабелей обычно требуются специальные *разъемы*, закрепленные на их концах. Затем кабель одним концом включается в *сетевой адаптер*, другим концом в какое-нибудь сетеобразующее устройство (концентратор, маршрутизатор, коммутатор и т.д.). В большинстве современных компьютеров сетевой адаптер является встроенным.

Сетевой адаптер – специальная печатная плата, установленная в компьютер, которая позволяет подключить его к сети.

Рис. 1.13 Сетевой адаптер DGE-560T

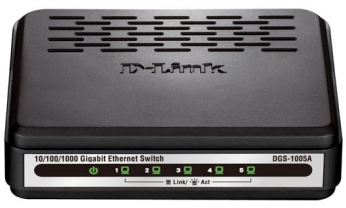


Рис. 1.14 Коммутатор DGS-1005A

При использовании беспроводного адаптера, взаимодействие с сетью осуществляется за счет передачи радиосигналов между адаптером и точкой доступа, соединенной с локальной сетью.

Рис. 1.15 Беспроводной сетевой адаптер DWA-140

Рис. 1.16 Точка доступа DAP-2310

Однако соединить компьютеры друг с другом недостаточно. Необходимо их научить «разговаривать». Для этого требуются сетевые операционные системы, поддерживающие один и тот же набор протоколов, с помощью которых компьютеры общаются по сети. И только после этого, запустив сетевое приложение (Web-браузер, ICQ, Skype и т.д.), можно обмениваться сообщениями, получать доступ к файлам, играть в сетевые игры.

Сетевая операционная система — операционная система со встроенными возможностями для работы в компьютерных сетях.

Протокол – набор правил и процедур, регулирующих порядок взаимодействия узлов в сети.

2 Модели сетевого взаимодействия

Для того чтобы передать данные с одного компьютера на другой, необходимо выполнить ряд последовательных процедур, определяемых сетевыми протоколами, различия в которых делают коммуникации между компьютерами достаточно сложной задачей. Чтобы протоколы работали надежно и согласованно, каждая процедура в них строго регламентируется. Протоколы должны соответствовать определенным промышленным стандартам, чтобы программы и оборудование разных производителей были совместимы и могли взаимодействовать друг с другом. Для облегчения разработки протоколов были созданы *сетевые* или *эталонные модели*.

Сетевая модель — это схема, определяющая общие принципы работы сетевых протоколов и способы их взаимодействия друг с другом для осуществления передачи данных по сети.

Наибольшее распространение получила *эталонная модель взаимодействия открытых систем* (Open System Interconnection Reference Model, OSI), которая будет подробно рассмотрена в этой главе.

2.1 Модель OSI

В конце 1970 года независимо друг от друга были запущены два проекта, цель которых заключалась в определении унифицированного стандарта архитектуры сетевых систем. Один проект выполнялся международной организацией по стандартизации (International Organization for Standardization, ISO), другой комитетом International Telegraph and Telephone Consultative Committee (CCITT). Обе организации разработали документы, описывающие аналогичные сетевые модели. В 1983 году эти документы были объединены в форму стандарта, получившего название «The Basic Reference Model for Open Systems Interconnection». Стандарт, который часто называют *эталонной моделью взаимодействия открытых систем* (Open Systems Interconnection Reference Model) или *моделью OSI* (OSI Model) был совместно опубликован ISO (под именем ISO 7498) и CCITT (под именем X.200) в 1984 году. В настоящее время CCITT называется ITU-T (Telecommunications Standardization Sector of the International Telecommunication Union).

Эталонная модель взаимодействия открытых систем или **модель OSI** определяет уровни взаимодействия систем, их стандартные названия и функции, которые должен выполнять каждый уровень.

Изначально модель OSI была создана как основа для разработки универсального набора протоколов, называемого OSI Protocol Suite. Однако он не получил широкого распространения, но модель стала удобным средством для обучения сетевым технологиям и разработки протоколов и устройств.

2.2 Уровни модели OSI

Модель OSI разбивает задачу перемещения информации между узлами на семь уровней, каждый из которых выполняет определенную задачу и взаимодействует с вышележащим и нижележащим уровнями. Уровни относительно независимы друг от друга, поэтому задачи, связанные с каждым из них, могут выполняться самостоятельно. Это

позволяет изменять средства их решения на одном уровне, не вызывая конфликта с другими уровнями. Такое разделение на уровни называется *иерархическим представлением*. В связи с этим модель OSI часто называют иерархической моделью.

Каждый уровень имеет имя и номер от 1 до 7, который определяет его позицию в модели OSI (Рис. 2.1).

Уровни хост-машины (host layers)	Уровень приложений	7
	Уровень представлений	6
	Сеансовый уровень	5
	Транспортный уровень	4
Уровни среды передачи данных (media layers)	Сетевой уровень	3
	Канальный уровень	2
	Физический уровень	1

Рис. 2.1 Модель OSI

Нижние уровни модели OSI (с 1 по 3) управляют физической доставкой данных по сети и реализуются в виде аппаратных средств и программного обеспечения.

Верхние уровни модели OSI (с 4 по 7) обеспечивают точную доставку данных между приложениями, работающими на сетевых узлах, и обычно реализуются только на программном уровне.

Каждый уровень, кроме уровня приложений, предоставляет сервисы вышележащему уровню. Любой уровень, кроме физического уровня, использует сервисы, предоставляемые нижележащим уровнем. Другими словами, уровень N предоставляет сервисы уровню N+1 и использует сервисы уровня N-1.

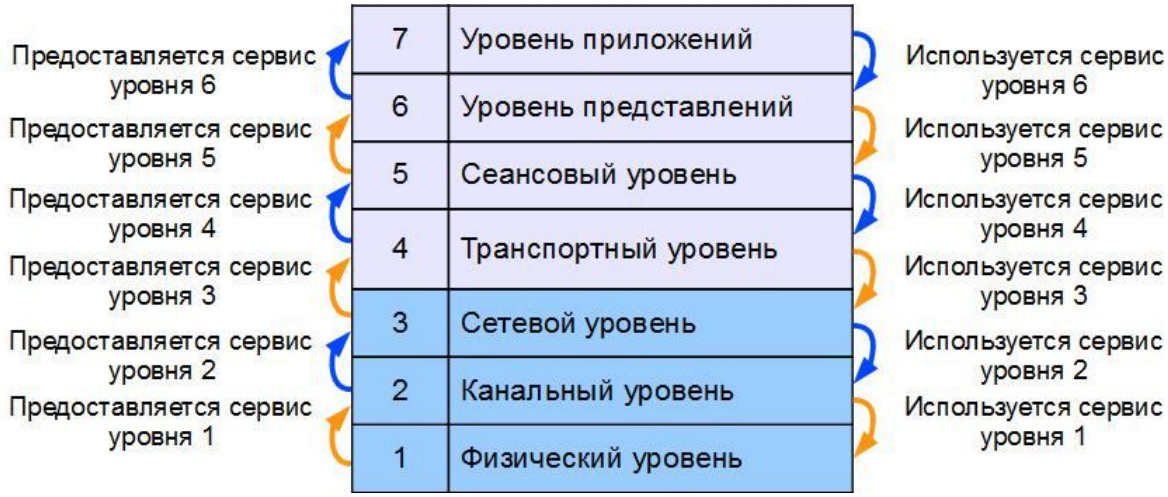


Рис. 2.2 Сервисы, предоставляемые уровнями модели OSI

Модель OSI не описывает службы и протоколы, используемые на каждом уровне, она определяет набор действий, которые должен выполнить уровень, чтобы передать информацию между узлами. Тем не менее, ISO также разработала стандарты для каждого уровня, которые не входят в саму эталонную модель, но каждый из которых опубликован как отдельный международный стандарт.

2.2.1 Взаимодействие между уровнями

Модель OSI определяет схему обмена данными между сетевыми узлами, но сама не является способом такого обмена. Обмен данными становится возможным благодаря *протоколам*.

Протокол – это формальный набор правил и соглашений, регламентирующий обмен информацией между узлами по сети. Он реализует функции одного или нескольких уровней OSI.

Существует большое количество протоколов обмена данными – протоколы локальных и глобальных сетей, протоколы маршрутизации, сетевые протоколы. *Протоколы локальных сетей* работают на физическом и канальном уровнях модели OSI и определяют правила обмена данными по различным каналам связи, используемым в локальных сетях. *Протоколы глобальных сетей* определяют правила обмена данными по различным каналам связи глобальных сетей. *Протоколы маршрутизации* – это протоколы, которые работают на сетевом уровне модели OSI и позволяют определять наилучший маршрут передачи данных между узлами. К *сетевым протоколам* относятся различные протоколы, работающие на сетевом уровне и выше.

Согласно модели OSI, каждый уровень узла, который посылает информацию, *логически* (по горизонтали) взаимодействует с аналогичным уровнем узла, который ее принимает в соответствии с правилами того или иного протокола. Каждому уровню «кажется», что он непосредственно взаимодействует с таким же уровнем другого узла. Это позволяет взаимодействовать Web-браузеру и Web-серверу, почтовому клиенту и почтовому серверу и т.д.

Однако физическое соединение устройств выполняется только на физическом уровне модели OSI, следовательно, чтобы данные были переданы по сети другому устройству, они должны «спуститься» с уровня приложений на физический уровень внутри передающего узла. Когда данные будут переданы по каналу связи, физический уровень устройства-получателя извлечет их из среды передачи и передаст вышележащему уровню. Таким образом, реальное взаимодействие одноименных уровней происходит *по вертикали* посредством взаимодействия с соседними уровнями (нижележащим и вышележащим) своего *стека протоколов*.

Стек протоколов – совокупность протоколов разных уровней. Наиболее известным является стек протоколов TCP/IP.

Правила и процедуры, которые отвечают за взаимодействие между соседними уровнями, называются *интерфейсами.*

Данные и служебная информация передается между уровнями в обоих направлениях. Существуют хорошо известные интерфейсы между уровнями, что позволяет им взаимодействовать друг с другом, не задумываясь о реализации.

Рис. 2.3 Взаимодействие между уровнями

2.2.2 Инкапсуляция данных

Взаимодействие между одноименными уровнями модели OSI осуществляется логически с использованием правил того или иного протокола. Это взаимодействие происходит в форме передачи сообщений, которые называются *блоками данных протокола (protocol data units, PDU)*. Каждый PDU имеет специальный формат, определенный в соответствии с функциями и требованиями конкретного протокола.

Для организации передачи данных, протокол уровня N должен передать PDU на нижележащий уровень N-1. Протокол уровня N-1 предоставит *сервис* вышележащему уровню N, т.е. он примет PDU протокола уровня N, который станет для него *данными,* обработает их и передает дальше на уровень N-2. На уровне N-1 PDU протокола уровня N будет называться *блоком данных сервиса (service data unit, SDU)*. Чтобы обеспечить сервис, протокол уровня N-1 помещает SDU, полученный от уровня N, в поле данных своего PDU и добавляет служебную информацию (заголовки и/или концевики), необходимую протоколу для реализации своей функции. Этот процесс называется *инкапсуляцией данных*.

Инкапсуляция – это процесс, при котором к данным добавляется служебная информация определенного протокола (уровня) перед отправкой в сеть.

Каждый уровень может использовать свое специальное название для PDU. Например, в семействе протоколов TCP/IP транспортные уровни для обмена пользуются *сегментами (segment)*. Таким образом, TCP-сегменты становятся частью *пакетов (packet)* сетевого уровня (также называемых *дейтаграммами)* и будут участвовать в обмене между соответствующими IP-уровнями. В свою очередь, на канальном уровне IP-пакеты должны стать частью *кадров (frame)*, которыми обмениваются непосредственно соединенные устройствами. При передаче данных по протоколу физического уровня с использованием аппаратных средств кадры преобразовываются в *биты*.

Рис. 2.4 PDU уровней модели OSI

Рассмотрим процесс инкапсуляции при передаче данных между узлами, показанный на Рис. 2.5. Когда приложение на компьютере А отправляет сообщение приложению на компьютер В, то оно передает его на уровень приложений компьютера А. Затем с уровня приложений, данные передаются на уровень представлений, который отправляет их ниже на сеансовый уровень. Сеансовый уровень пересылает данные транспортному уровню, который в свою очередь формирует сегмент, путем добавления служебной информации, и передает его сетевому уровню модели OSI. Сетевой уровень принимает сегмент и добавляет свой заголовок, образуя пакет, и передает его нижележащему уровню. Канальный уровень в свою очередь создает кадр, путем добавления заголовка канального уровня и концевика, затем передает его физическому уровню. На физическом уровне поток битов преобразуется в электрические, электромагнитные или оптические сигналы, которые отправляются через среду передачи компьютеру В.

Физический уровень компьютера В принимает сигналы из физической среды, извлекает из них информацию в виде потока битов. Далее из этого потока формируется кадр, который передается выше на канальный уровень. Канальный уровень принимает кадр и анализирует служебную информацию, предназначенную для него. В случае отсутствия каких-либо ошибок, канальный уровень извлекает из сообщения данные, предназначенные для вышележащего сетевого уровня, и передает их ему. Этот процесс повторяется на каждом вышележащем уровне вплоть до уровня приложений. Уровень приложений компьютера В передает информацию приложению-приемнику и процесс обмена данными завершается. Другими словами, достигнув узла-получателя, сообщение проходит через все уровни в обратном порядке (от 1-го до 7-го), последовательно преобразовываясь на каждом из них с использованием соответствующей служебной информации, пока не достигнет приложения-приемника. Этот процесс называется *декапсуляцией* данных.

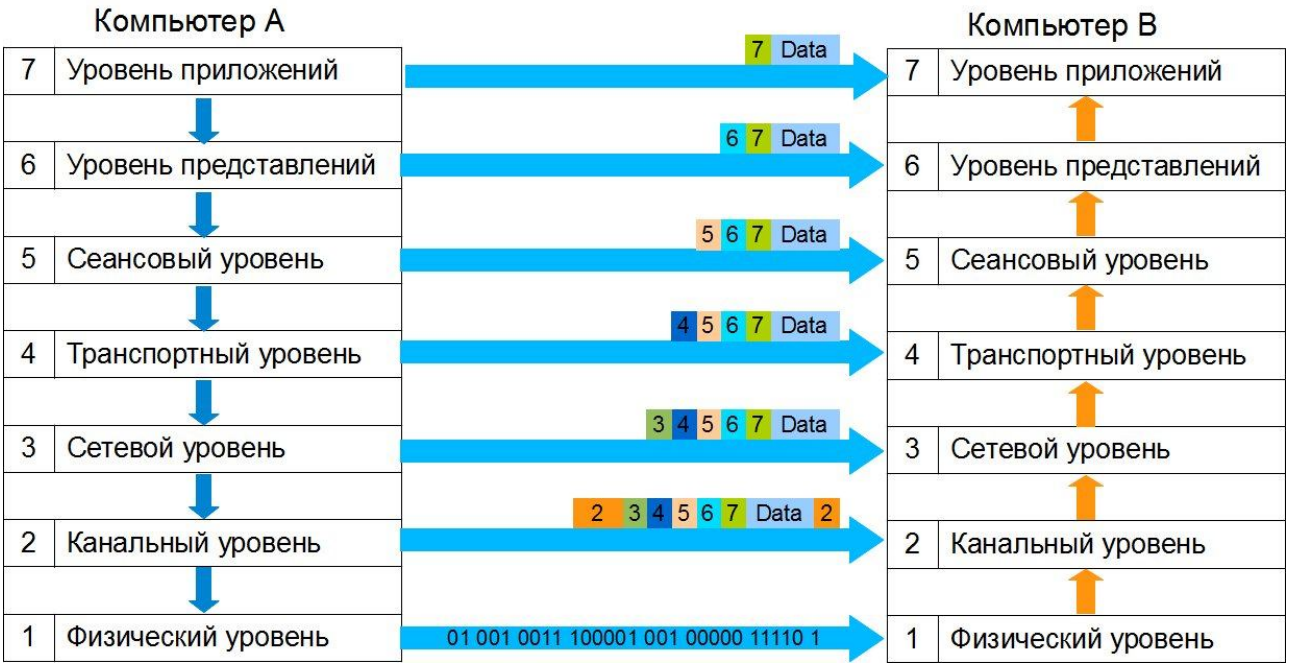


Рис. 2.5 Обмен данными между сетевыми узлами согласно модели OSI

2.2.3 Описание уровней модели OSI

Уровень приложений *(Application layer)* — это седьмой, самый близкий к пользователю уровень модели OSI. Он отличается от других уровней тем, что не предоставляет услуги ни одному другому уровню модели OSI, а только обслуживает прикладные процессы, находящиеся вне пределов модели OSI. Примерами могут служить Web-браузер, который является прикладным процессом, запущенным на компьютере и использующим сервисы, предоставляемые протоколом прикладного уровня HTTP (Hypertext Transfer Protocol); почтовый клиент, использующий сервисы протокола POP3 (Post Office Protocol Version 3).

Уровень приложений идентифицирует и устанавливает доступность предполагаемых партнеров для связи, синхронизирует совместно работающие прикладные программы, а также устанавливает договоренность о процедурах восстановления после ошибок и контроля целостности данных. Уровень приложений также определяет степень достаточности ресурсов для осуществления предполагаемой связи.

Уровень представлений *(Presentation layer)* – шестой уровень модели OSI. Он отвечает за то, чтобы информация, посылаемая уровнем приложений одной системы, могла быть прочитана уровнем приложений другой системы. При необходимости уровень представлений преобразует форматы данных, путем использования общего формата представления информации. Также он может выполнять сжатие (распаковку) данных с целью повышения пропускной способности сети. Помимо этого на уровне представлений может выполняться шифрование (дешифрование) данных, например, с использованием протокола SSL (Secure Sockets Layer). Однако шифрование данных может выполняться не только на 6 уровне модели OSI. Оно также выполняется и на более низких уровнях. Примером может служить технология IPSec. Следует отметить, что уровень представлений не всегда задействуется при организации сетевого взаимодействия, т.к. его функции могут быть реализованы в рамках уровня приложений или просто не требуются в данном конкретном случае.

Сеансовый уровень *(Session layer)* – пятый уровень модели OSI. Как следует из названия, он позволяет двум прикладным процессам устанавливать, управлять и завершать сеансы связи (сессии) друг с другом. Сеансовый уровень синхронизирует диалог между прикладными процессами и отвечает за восстановление аварийно прерванных сеансов связи.

Технологии сеансового уровня часто реализованы в виде набора программных средств, называемых *application program interfaces* (API, прикладной программный интерфейс). API предоставляют набор сервисов, позволяющих программистам разрабатывать сетевые приложения, не заботясь о транспортировке, адресации и доставке данных. Эти функции выполняют нижележащие уровни модели OSI.

Транспортный уровень *(Transport layer)* – четвертый уровень модели OSI. Современные операционные системы являются многозадачными, поэтому одновременно пользователь может работать с несколькими приложениями, которые отправляют и получают данные по сети. Транспортный уровень является связующим звеном между уровнями приложений, представлений и сеансовым уровнем, которые имеют дело только с прикладными процессами и нижележащими уровнями, которые занимаются непосредственно доставкой данных. Он изолирует верхние уровни модели OSI от проблем связанных с доставкой любой информации и отвечает за надежную передачу данных между взаимодействующими приложениями разных компьютеров за счет использования средств адресации и мультиплексирования/демультиплесирования (одновременной передачи данных от разных прикладных процессов по одному соединению и последующей доставки их соответствующим приложениям). Также транспортный уровень на стороне отправителя разбивает данные, полученные от вышележащих уровней на блоки небольшого размера, называемые *сегментами*, и доставляет их получателю в нужной последовательности. Этот процесс называется *сегментацией*. На транспортном уровне получателя эти сегменты собираются в исходный поток данных.

Протоколы транспортного уровня могут предоставлять сервисы *с установлением соединения* (*connection-oriented*) и *без установления соединения* (*connectionless*). Протоколы с установлением соединения отвечают за установку, поддержание и завершение соединения между отправителем и получателем. Они могут выполнять диагностику и исправление ошибок, возникающих при передаче информации, а также предоставлять механизмы управления потоком данных (*flow control*). Примером протоколов такого типа является протокол *TCP* (Transmission Control Protocol, протокол управления передачей). Протоколы без установления соединения не выполняют установку соединения перед передачей данных и не обеспечивают надежную доставку. Протокол *UDP* (User Datagram Protocol, протокол дейтаграмм пользователей) является примером протокола транспортного уровня без установления соединения.

Сетевой уровень *(Network layer)* – третий уровень модели OSI. Он является одним из самых важных уровней модели OSI и отвечает за соединение узлов, расположенных в географически удаленных друг от друга сетях. Сетевой уровень выполняет две основные функции – логическую адресацию и маршрутизацию. Каждому устройству, подключенному к сети, назначается логический адрес, который также называют адресом 3 уровня. Он используется для маршрутизации пакетов. *Маршрутизация* – это процесс определения наилучшего маршрута передачи информации от отправителя к получателю, когда отправитель и получатель находятся в разных сетях, соединенных произвольным образом. Также на сетевом уровне решаются задачи управления потоком данных и диагностики ошибок передачи. Сетевой уровень выполняет инкапсуляцию сегментов, полученных от транспортного уровня в *пакеты* (также называемые *дейтаграммами*). Основным протоколом сетевого уровня является протокол *IP (Internet Protocol)*.

Канальный уровень *(Data link layer)* – второй уровень модели OSI. Он обеспечивает сетевым узлам доступ к среде передачи и решает вопросы физической адресации (в противоположность сетевой или логической адресации), обнаружения и коррекции ошибок, упорядоченной доставки кадров, логической топологии. Канальный уровень завершает процесс инкапсуляции и помещает дейтаграммы (пакеты), полученные с сетевого уровня в *кадры*. Примерами протоколов канального уровня могут служить семейство протоколов Ethernet IEEE 802.3, протоколы беспроводных сетей IEEE 802.11.

Физический уровень *(Physical layer)* – самый нижний уровень модели OSI. Он выполняет передачу потока битов, полученных от канального уровня, через физическую среду в виде электрических, оптических или радиосигналов. Физический уровень отвечает за активацию, поддержание и деактивизацию физического канала между конечными системами. Спецификации физического уровня детально описывают механические, оптические, электрические, функциональные интерфейсы со средой передачи: напряжения, частоты, длины волн, разъемы, число и функциональность контактов, схемы кодирования сигналов и т.д. Также физический уровень рассматривает вопросы, связанные с физической топологией сетей.

Таблица 2.1 Сравнительная таблица уровней модели OSI

	Уровень	**Тип обрабатываемых данных**	**Функции**
7	**Уровень приложений**	Пользовательские данные	Предоставление сервисов для сетевых приложений
6	**Уровень представлений**	Закодированные пользовательские данные	Общий формат представления данных, сжатие и шифрование
5	**Сеансовый уровень**	Сессии	Установление сессий между приложениями
4	**Транспортный уровень**	Сегменты	Адресация процессов, сегментация/ повторная сборка данных, управление потоком, надежная доставка
4	**Сетевой уровень**	Дейтаграммы/ пакеты	Передача сообщений между удаленными устройствами, выбор наилучшего маршрута, логическая адресация
2	**Канальный уровень**	Кадры	Доступ к среде передачи и физическая адресация
1	**Физический уровень**	Биты	Передача электрических и оптических сигналов между устройствами

Следует отметить, что в модели OSI отдельный протокол не всегда соответствует одному из семи уровней. Иногда протокол соответствует более чем одному уровню модели OSI. Так, например, протокол ARP (Address Resolution Protocol), преобразующий сетевые адреса IPv4 (уровень 3 модели OSI) в физические MAC-адреса (уровень 2 модели OSI) можно назвать протоколом «уровня 2.5». Также несколько протоколов могут быть реализованы в рамках одного уровня, как, например, протоколы маршрутизации уровня 3 RIP (Routing Information Protocol), OSPF (Open Shortest Path First) и др.

В некоторых случаях PDU протокола уровня N может инкапсулироваться в PDU протокола уровня N+1, что характерно, в частности, для виртуальных частных сетей (VPN). Во многих реализациях VPN протоколы канального (Ethernet) или сетевого уровня (IP) инкапсулируются в протоколы транспортного уровня (чаще всего UDP). При передаче сообщений протокол маршрутизации 3 уровня RIP использует протокол транспортного уровня UDP.

2.3 Модель и стек протоколов TCP/IP

До появления модели OSI было создано множество различных сетевых моделей и стеков протоколов, поэтому построенный в полном соответствии с моделью OSI стек протоколов не получил распространения. Несмотря на это модель OSI является

концептуальной моделью и служит удобным средством для обучения сетевым технологиям и разработки протоколов и устройств.

Стек протоколов TCP/IP был создан раньше модели OSI, поэтому его разработчики не использовали модель OSI для описания архитектуры стека. Они разработали собственную модель, которая имела несколько названий, включая *модель TCP/IP* (Transmission Control Protocol/Internet Protocol), *модель DARPA* (Defense Advanced Research Projects Agency (DARPA или ARPA)) или *модель DOD* (United States Department of Defense).

Так как модель OSI имеет широкое распространение, архитектура TCP/IP часто описывается с использованием названий уровней модели TCP/IP и соответствующих уровней модели OSI.

2.3.1 Описание уровней модели TCP/IP

Модель TCP/IP, так же как и модель OSI, имеет многоуровневую структуру, но для того, чтобы данные от приложения компьютера A были переданы приложению на компьютере B, они должны последовательно пройти 4 уровня: уровень приложений, транспортный уровень, уровень Интернет и уровень доступа к среде.

Как показано на Рис. 2.6, трем верхним уровням модели OSI соответствует **уровень приложений** *(Application layer)* в модели TCP/IP, который включается в себя функции представления, кодирования и контроля над установлением соединения. Существует множество протоколов уровня приложений, из которых самыми распространенными являются FTP, TFTP, HTTP/HTTPs, DHCP, DNS, Telnet, SMTP, POP3, IMAP и др.

Транспортный уровень *(Transport layer)* модели TCP/IP выполняет те же функции, что и одноименный уровень в модели OSI. На этом уровне определены два протокола – TCP и UDP. Протокол TCP (Transmission Control Protocol) обеспечивает надежную доставку сегментов по сети за счет установления логического соединения между отправителем и получателем данных. Протокол UDP (User Datagram Protocol), в отличие от TCP, не устанавливает соединение между отправителем и получателем сообщения и не гарантирует надежную доставку данных.

Уровень Интернет *(Internet layer)* аналогичен по функциям сетевому уровню модели OSI и обеспечивает организацию связи между сетями и подсетями, образующими составную сеть. Основным протоколом уровня Интернет является IP, который выполняет две основные функции – адресацию узлов и выбор наилучшего маршрута до сети назначения (маршрутизацию). Также на этом уровня работают протоколы ICMP, IGMP, протоколы маршрутизации RIP, OSPF, BGP.

Уровень доступа к сети *(Network access layer)* объединяет функции канального и физического уровня модели OSI, обеспечивая физическую передачу данных в сети. Существует множество различных протоколов уровня доступа к сети, из которых самыми распространенными являются Ethernet, Token Ring, FDDI, PPP, IEEE 802.11 (Wi-Fi), ATM и др.

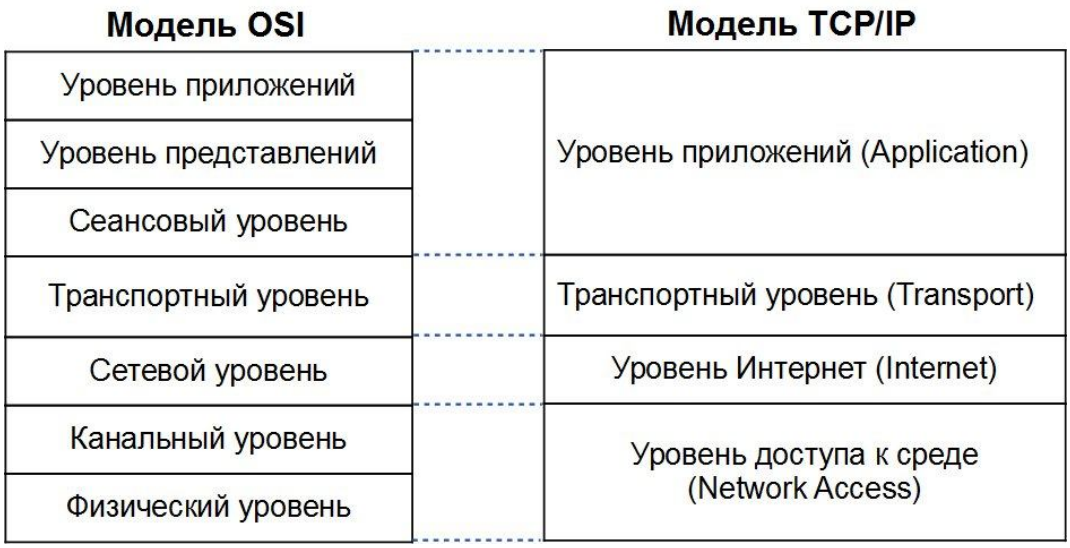


Рис. 2.6 Соответствие между уровнями модели OSI и модели TCP/IP

В настоящее время стек TCP/IP представляет собой один из самых распространенных стеков протоколов компьютерных сетей. Стек TCP/IP имеет ряд преимуществ над другими стеками протоколов (IPX/SPX, NetBIOS/SMB). Это, в частности, возможность маршрутизации пакетов, гибкая система адресации, и небольшое число широковещательных сообщений.

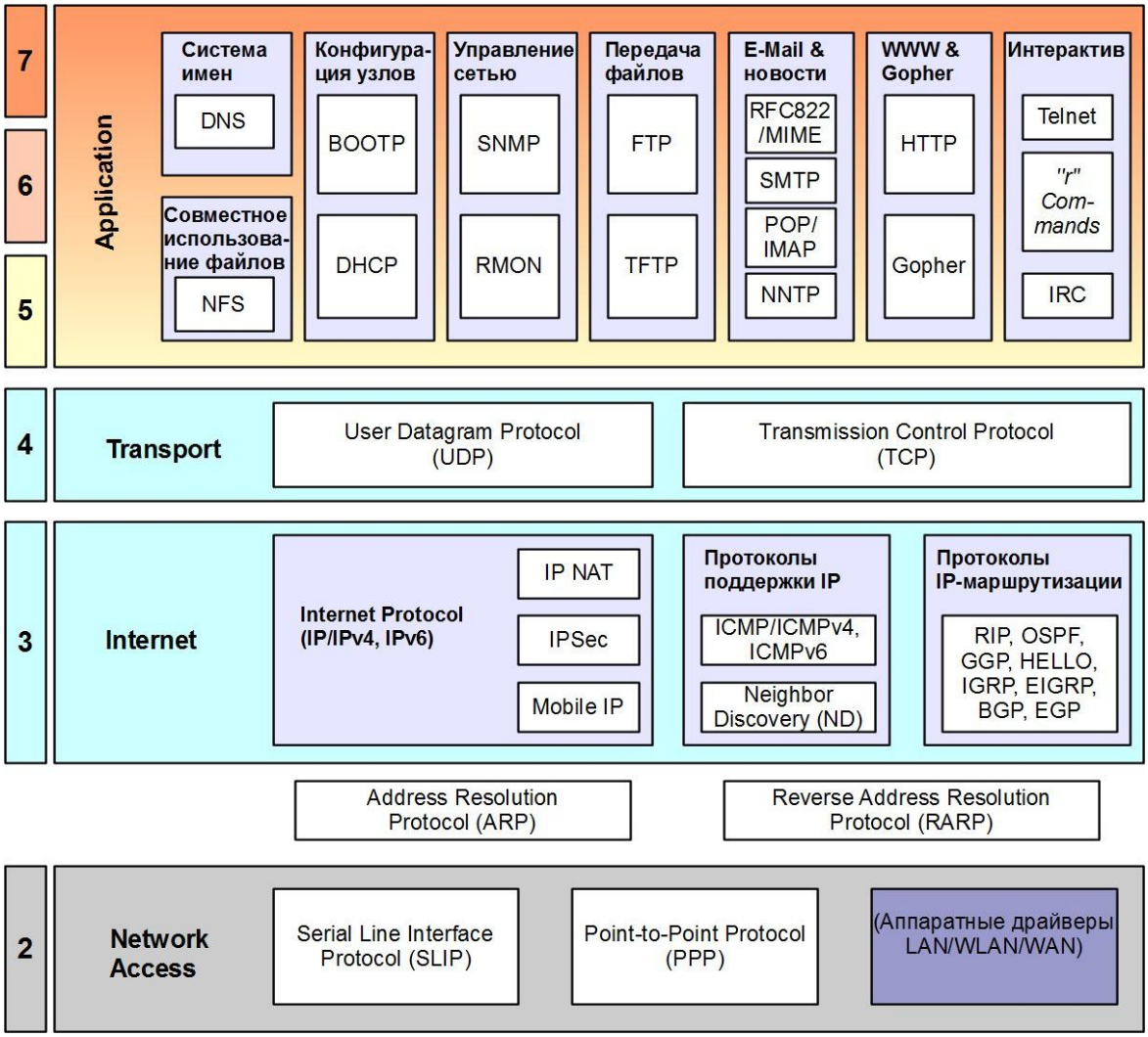


Рис. 2.7 Протоколы стека TCP/IP

3 Физический уровень модели OSI

Физический уровень – самый нижний уровень модели OSI. Он выполняет передачу потока битов, полученных от канального уровня, через физическую среду в виде электрических, оптических или радиосигналов. Физический уровень отвечает за установление, поддержание и деактивизацию канала между конечными системами, выполняет идентификацию каналов, оповещает о появлении неисправностей и отказов, а также, в требуемых случаях, прослушивает каналы с целью определения в них активности. *Международный союз электросвязи* (International Telecommunication Union, ITU) утвердил ряд стандартов физического уровня. Широко известны и применяются стандарты физического уровня, разработанные *Альянсом отраслей электронной промышленности* (Electronics Industries Alliance, EIA) и *Ассоциацией телекоммуникационной промышленности* (Telecommunications Industry Association, TIA). Спецификации физического уровня детально описывают механические, оптические, электрические, функциональные интерфейсы со средой передачи: напряжения, частоты, длины волн, разъемы, число и функциональность контактов, схемы кодирования сигналов и т.д. Также физический уровень рассматривает вопросы, связанные с физической топологией сетей.

3.1 Понятие линии и канала связи

Для передачи сигналов между взаимодействующими системами в компьютерных сетях используются линии связи.

В узком смысле под термином **линия связи** (*transmission link, link*) подразумевается физическая среда, по которой передаются сигналы между двумя конечными системами. Сигналы формируются специальными техническими средствами (передатчиками, усилителями, мультиплексорами и т.д.), относящимися к сетевому оборудованию.

Среда передачи (*transmission medium*) или **физическая среда** – материальная субстанция, через которую осуществляется распространение сигналов.

В компьютерных сетях используют два типа сред передачи: кабельную и беспроводную.

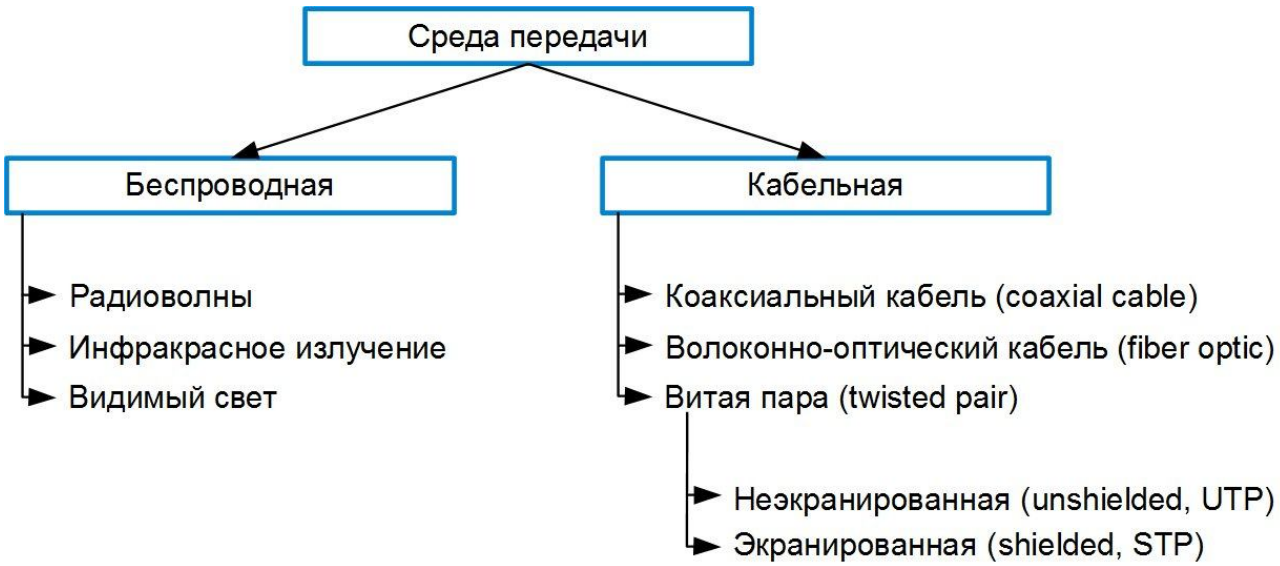


Рис. 3.1 Типы сред передачи

Основой беспроводных сред передачи является земная атмосфера или космическое пространство, через которые распространяются электромагнитные волны. В кабельных средах передачи используются кабели различных типов: коаксиальные, волоконно-оптические, витая пара. Передача сигналов в них осуществляется с помощью электрических (электрический ток) или оптических (свет) сигналов.

В широком смысле под термином «линия связи» в области компьютерных сетей подразумевают *канал связи*.

Канал связи (*channel, data link*) представляет собой совокупность одной или нескольких физических сред передачи и каналообразующего (сетевого) оборудования, которые обеспечивают передачу данных между взаимодействующими системами в виде сигналов, соответствующих типу физической среды.

В этом контексте термины «линия связи» и «канал связи» являются синонимами.

Рис. 3.2 Канал связи

Различают **физические** (*physical link*) и **логические** (*logical link*) каналы. Физический канал связи представляет собой средство передачи сигналов между взаимодействующими системами. В зависимости от типа передаваемых сигналов и физической среды, используемой для их распространения, физические каналы подразделяются на *электрические* (витая пара, коаксиальный кабель), *оптические* (волоконно-оптический кабель) и *беспроводные* (радиоканалы, инфракрасные каналы и т.д).

Логические каналы устанавливаются между протоколами любых уровней модели OSI взаимодействующих систем и определяют путь, по которому данные передаются от источника к приемнику через один или последовательность физических каналов.

При прокладке в физическом канале нескольких логических каналов, ресурсы физического канала распределяются между логическими каналами с помощью методов *мультиплексирования*.

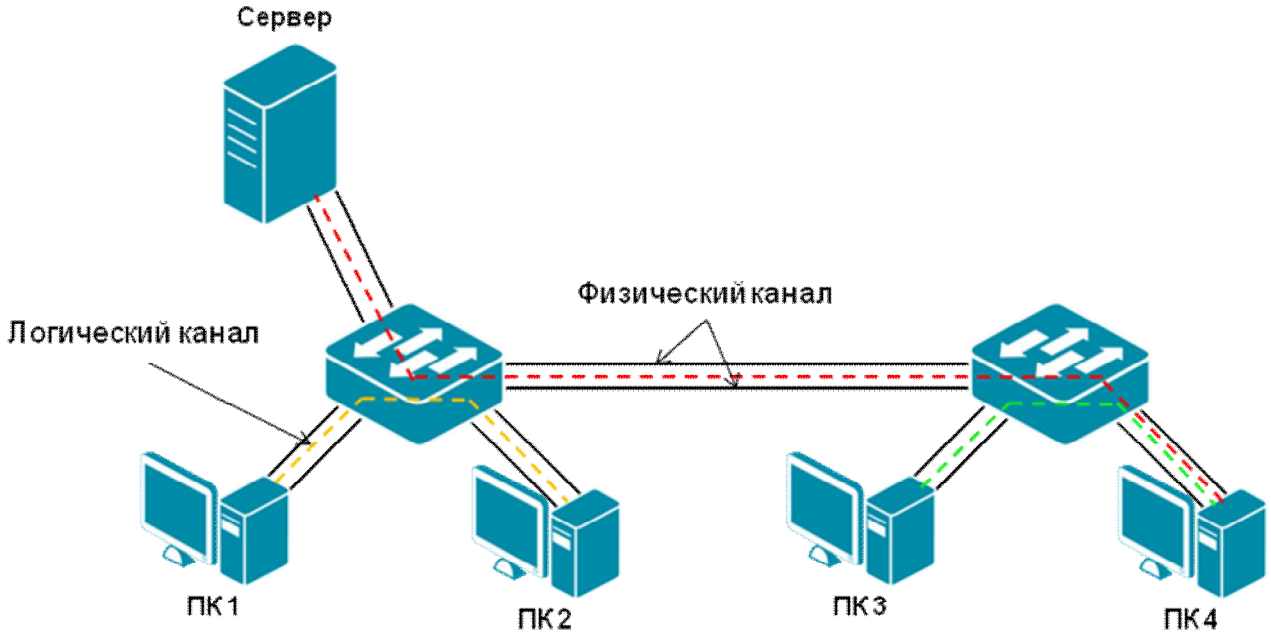


Рис. 3.3 Физический и логический каналы связи

Каналы (линии) связи можно классифицировать на основе следующих признаков:

- по типу физической среды;
- по типу представления передаваемой информации;
- по направлению передачи данных;
- по времени существования;
- по способу подключения;
- по ширине полосы пропускания.

В зависимости от типа представления передаваемой информации каналы делятся на **аналоговые**, предназначенные для передачи аналоговых сигналов и **дискретные**, служащие для передачи дискретных (цифровых) сигналов.

В зависимости от направления передачи данных различают каналы:

- **симплексные** (*simplex*), в которых передача осуществляется только *в одном* направлении;
- **полудуплексные** (*half-duplex*), в которых передача ведется *поочередно* в прямом и обратном направлении;
- **дуплексные** (*duplex*), в которых передача ведется *одновременно* в двух направлениях – прямом и обратном.

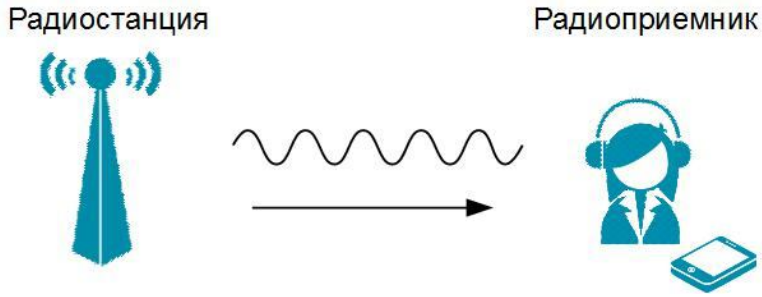


Рис. 3.4 Симплексный канал

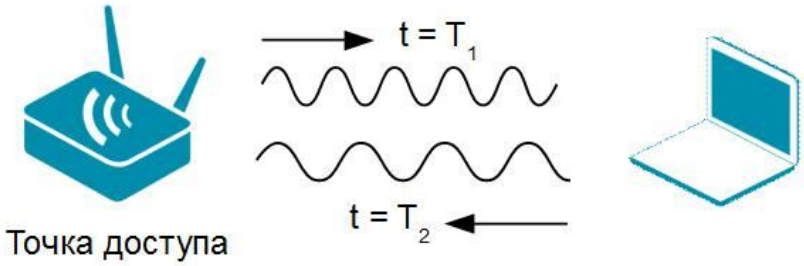


Рис. 3.5 Полудуплексный канал

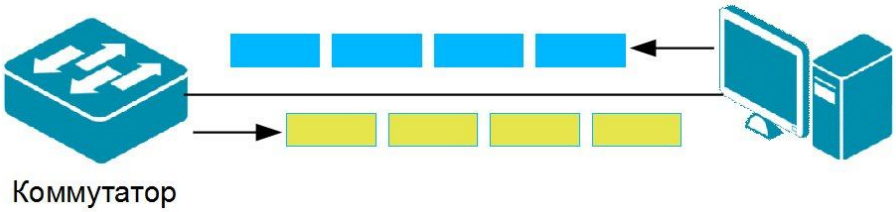


Рис. 3.6 Дуплексный канал

Также каналы можно классифицировать по времени доступности для абонента. Каналы между конечными системами, которые доступны для передачи данных на длительное время за счет постоянно существующего соединения с заданными характеристиками, называются **выделенными** или **некоммутируемыми**. Каналы связи, передача данных по которым возможна только после установления соединения между взаимодействующими системами, называются **коммутируемыми** или **временными**. При этом канал будет существовать только в течение сеанса связи, т.е. времени, требуемого для передачи данных.

По способу подключения каналы делятся на: **«точка-точка»** (*point-to-point*), **«точка-многоточка»** (*point-to-multipoint),* **«многоточка»** (*multipoint*). Канал «точка-точка» связывает только два узла или две взаимодействующих системы. Канал «точка-многоточка» обеспечивает соединение одной центральной системы (узла) с группой других систем (узлов). Канал «многоточка» обеспечивает подключение друг к другу группы узлов или систем.

Важной характеристикой канала связи является его **полоса пропускания** (*bandwidth*). В зависимости от ширины полосы пропускания (разности между граничными частотами полосы пропускания) и способа передачи сигналов каналы делятся на **основополосные** (*baseband channel*) и **широкополосные** (*broadband channel*).

Основополосный канал характеризуется простотой и дешевизной реализации, в связи с чем, широко используется в локальных сетях (слово «BASE» в названиях спецификаций физического уровня Ethernet (например, 10BASE-T, 100BASE-FX, 1000BASE-SX), указывает на основополосную передачу). Сигнал по основополосному каналу передается в основной полосе частот, т.е. без модуляции несущей, при этом вся полоса пропускания используется для передачи только одного сигнала.

В отличие от основополосного канала, вся полоса пропускания широкополосного канала разделяется между несколькими логическими каналами с помощью методов мультиплексирования, что позволяет одновременного и независимо друг от друга выполнять передачу сигналов между несколькими парами взаимодействующих систем. Технологии широкополосного доступа (например, xDSL, PowerLine (PLC), 3G (UMTS), 4G (LTE)) используется при организации подключения к набору услуг, предлагаемых операторами связи.

3.2 Сигналы

Передача данных по каналам связи осуществляется с помощью их физического представления – электрических (электрический ток), оптических (свет) или электромагнитных сигналов.

Если рассматривать сигнал как функцию времени, то он может быть:

- **аналоговым** (*непрерывным*) – его величина непрерывно изменяется во времени;
- **цифровым** (*дискретным*) – имеющим конечное, обычно небольшое число значений.

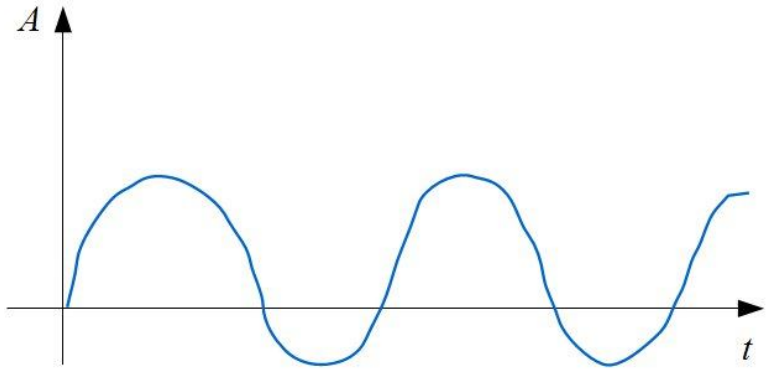


Рис. 3.7 Аналоговый сигнал

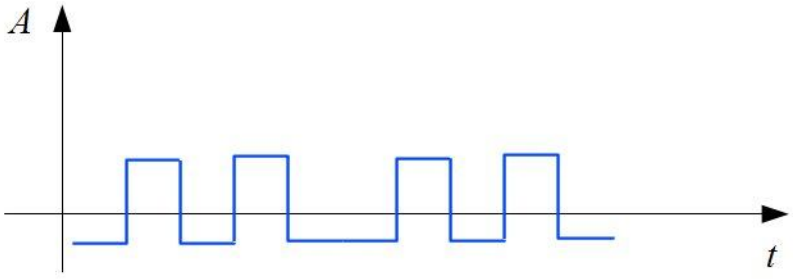


Рис. 3.8 Цифровой сигнал

Сигналы, используемые для передачи потока данных должны быть информативными, т.е. иметь некоторые изменяющиеся параметры, которые позволят приемнику идентифицировать полученные данные. В качестве такого сигнала часто используется *гармонический сигнал*.

Гармонический сигнал – это гармонические колебания, со временем распространяющиеся в пространстве, которые несут в себе информацию или какие-то данные.

Гармонические колебания – это колебания, при которых физическая (или любая другая) величина изменяется с течением времени по синусоидальному или косинусоидальному закону.

Гармонический сигнал несет в себе информацию в виде трех параметров: *амплитуды*, *фазы* и *частоты* и описывается формулой:

$$y(t) = A\cos(\omega t + \varphi_0),$$

где A – амплитуда сигнала; ω – круговая частота: $\omega = 2\pi f$ (f – линейная частота: $f=1/T$, величина обратная периоду T); φ_0 – начальная фаза гармонического сигнала; t – время.

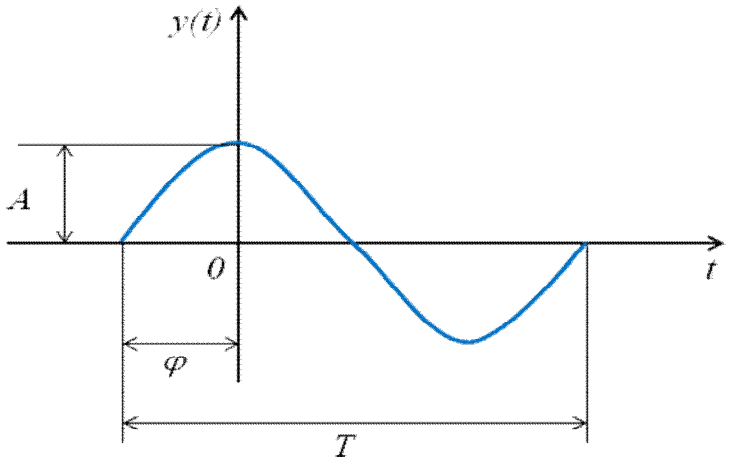


Рис. 3.9 Гармонический сигнал

Для обеспечения высокой скорости передачи данных важна частота: чем выше частота, тем больше скорость передачи.

Функция времени *y(t)* может быть произвольной и иметь различные частоты.

Вспомним теорию гармонического анализа и преобразование Фурье. Французский ученый Ж. Б. Фурье доказал, что любое изменение во времени некоторой функции можно аппроксимировать в виде конечной или бесконечной суммы ряда гармонических колебаний с разными амплитудами, частотами и начальными фазами.

Другими словами, любой периодический сигнал (аналоговый или цифровой), описываемый сложной функцией времени, может быть представлен в виде бесконечной или конечной суммы простых гармонических колебаний (гармоник) с частотами кратными основной частоте $\omega = 2\pi/T$:

$$y(t) = \sum_{i=0}^{\infty} A_i \cos(\omega_i t + \varphi_i) = \frac{A_0}{2} + \sum_{i=1}^{\infty} A_i \cos(\omega_i t + \varphi_i)$$

где i – номер гармоники; A_i – амплитуда, φ_i – начальная фаза, ω_i– круговая частота i-й гармоники; t – время.

Первая гармоника ω_1 называется первой или основной гармоникой сигнала, все остальные гармоники называются высшими. При этом частота каждой последующей гармоники больше предыдущей $\omega_1 < \omega_2 < \omega_3 \ldots\ldots < \omega_\infty$.

Периодическим сигналом называют такой вид воздействия, когда форма сигнала повторяется через некоторый интервал времени T, который называется периодом.

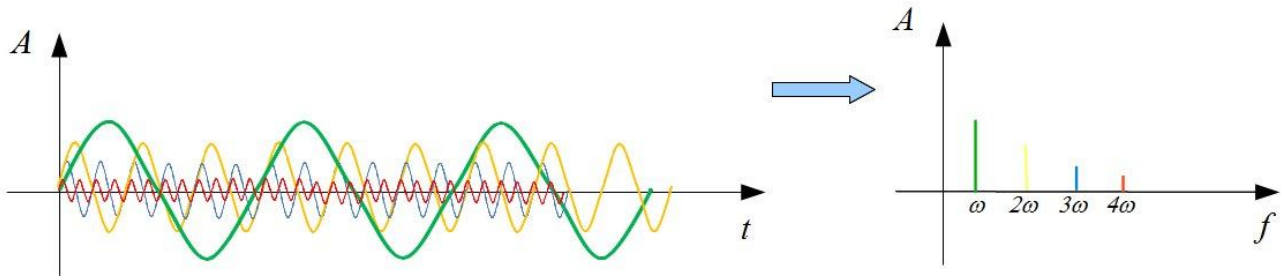


Рис. 3.10 Формирование сигнала из суммы первых 4 гармоник и спектральная амплитудная диаграмма периодического сигнала

Набор гармонических колебаний, в сумме составляющий исходный сигнал, образует *частотный спектр* этого сигнала, т.е. область частот, составляющих данный сигнал.

Сигналов, которые обладали бы бесконечным спектром, в природе практически нет. Преобладающая часть энергии реальных сигналов сосредоточена в ограниченной области (полосе) частот, а сам сигнал представляется в виде конечной суммы гармонических колебаний. В этом случае спектр сигнала *y(t)* определяется как разность между частотами верхней и нижней гармоник: f_n-f_1, где n<∞.

Из набора гармоник, составляющих сигнал, выделяют и различают *амплитудный* и *фазовый* спектр. Амплитудным спектром называют набор амплитуд всех гармоник, который обычно представляют диаграммой в виде набора вертикальных линий, длины которых пропорциональны (в выбранном масштабе) амплитудным значениям гармонических колебаний, а место на горизонтальной оси определяется частотой (номером гармоники) данной составляющей. Амплитудный и фазовый спектр однозначно определяют сигнал. Однако для многих практических задач достаточно ограничиться амплитудным спектром.

При передаче сигнала по каналу связи его форма искажается вследствие неодинаковой деформации гармоник различных частот. Это происходит из-за того, что физические параметры канала связи отличаются от идеальных. На сигнал влияют такие факторы, как затухание, шумы и помехи. Однако, основным фактором, оказывающим влияние на форму сигнала, является полоса пропускания канала связи. Для того чтобы передать сигнал без значительных искажений, канал связи должен иметь *ширину полосы пропускания не менее ширины спектра частот* передаваемого сигнала.

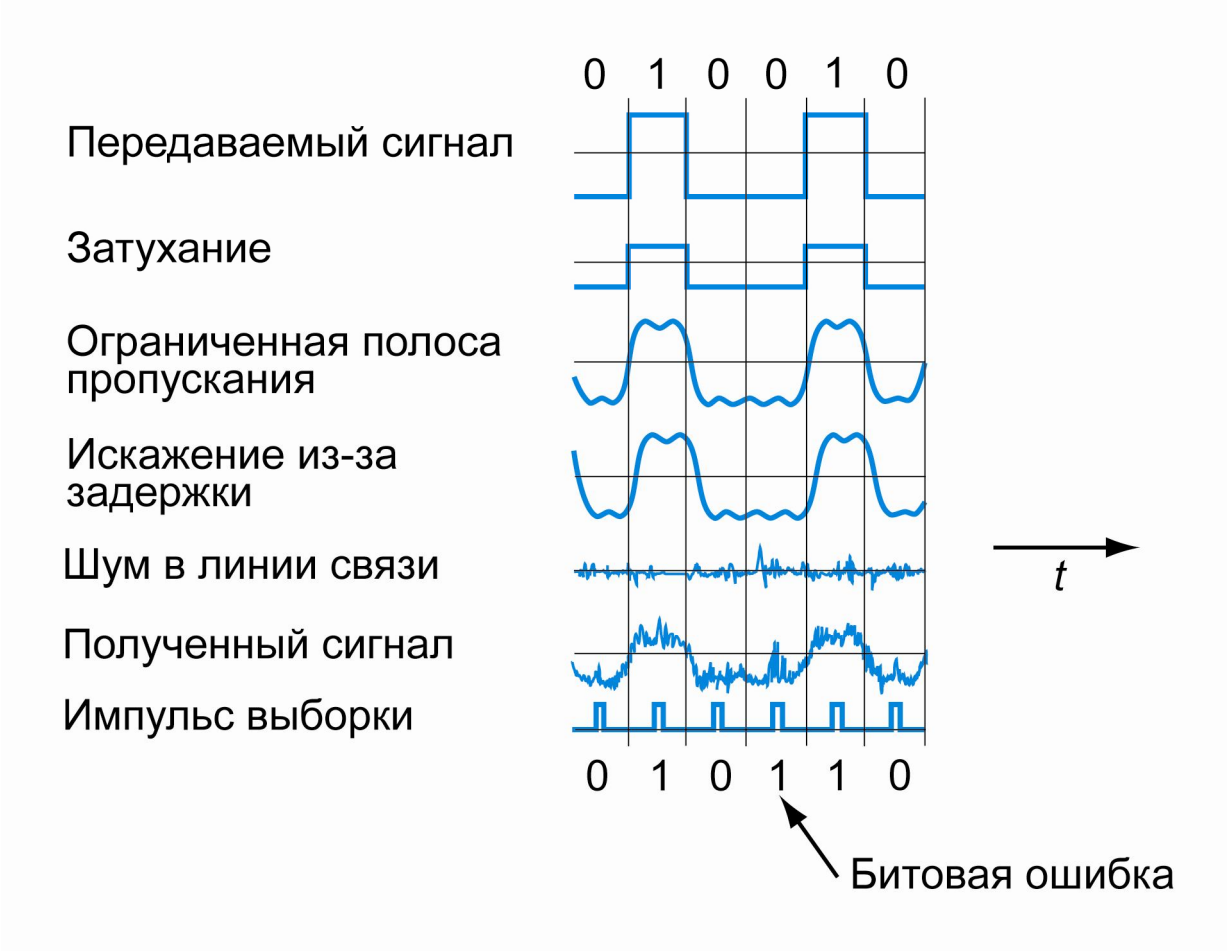


Рис. 3.11 Влияние физических параметров среды передачи на сигнал

3.3 Основные характеристики канала связи

К основным характеристикам канала (линии) связи существенно влияющим на качество передачи сигнала можно отнести:

- полосу пропускания;
- затухание;
- помехоустойчивость;
- пропускную способность;
- достоверность передачи данных.

3.3.1 Полоса пропускания

Полоса пропускания (*bandwidth*) – диапазон частот, в пределах которого амплитудно-частотная характеристика (АЧХ) канала (линии) связи достаточно равномерна для того, чтобы обеспечить передачу сигнала без существенного искажения его формы.

Ширина полосы пропускания F определяется как разность верхней $f_в$ и нижней $f_н$ граничных частот участка АЧХ, на котором мощность сигнала уменьшается не более чем в 2 раза по сравнению с максимальным значением: $F = f_в - f_н$ (что приблизительно соответствует −3 дБ).

Измеряется полоса пропускания в герцах (Гц).

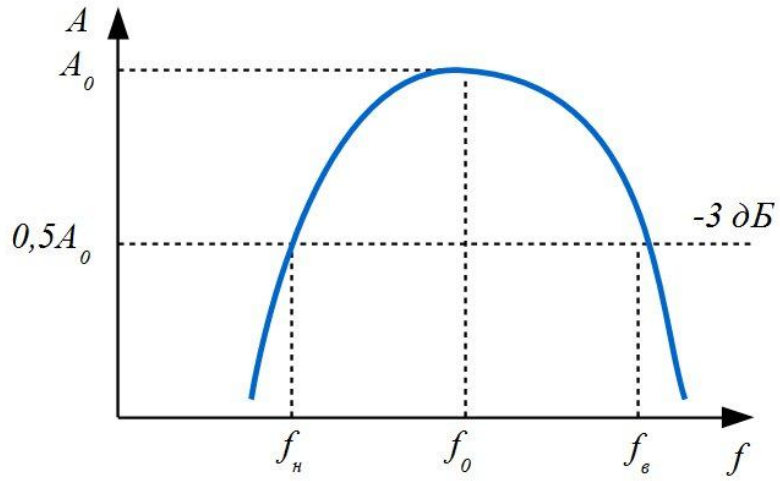


Рис. 3.12 Полоса пропускания канала связи

Ширина полосы пропускания существенным образом влияет на максимально возможную скорость передачи информации по каналу связи и зависит от типа среды передачи, наличия в каналах частотных фильтров.

Сигналы составлены из большого набора гармоник, однако приемник может получить лишь те гармоники, частоты которых находятся внутри полосы пропускания канала. Чем шире полоса пропускания канала, тем выше может быть скорость передачи данных и тем более высокочастотные гармоники сигнала могут передаваться. Если в полосу пропускания канала попадают гармоники, амплитуды которых вносят основной вклад в результирующий сигнал, форма сигнала претерпит незначительные изменения, и сигнал будет правильно распознан приемником.

В противном случае форма сигнала будет значительно искажаться, что приведет к снижению скорости передачи информации по каналу вследствие проблем с его распознаванием, которые вызовут ошибки связи и повторные передачи.

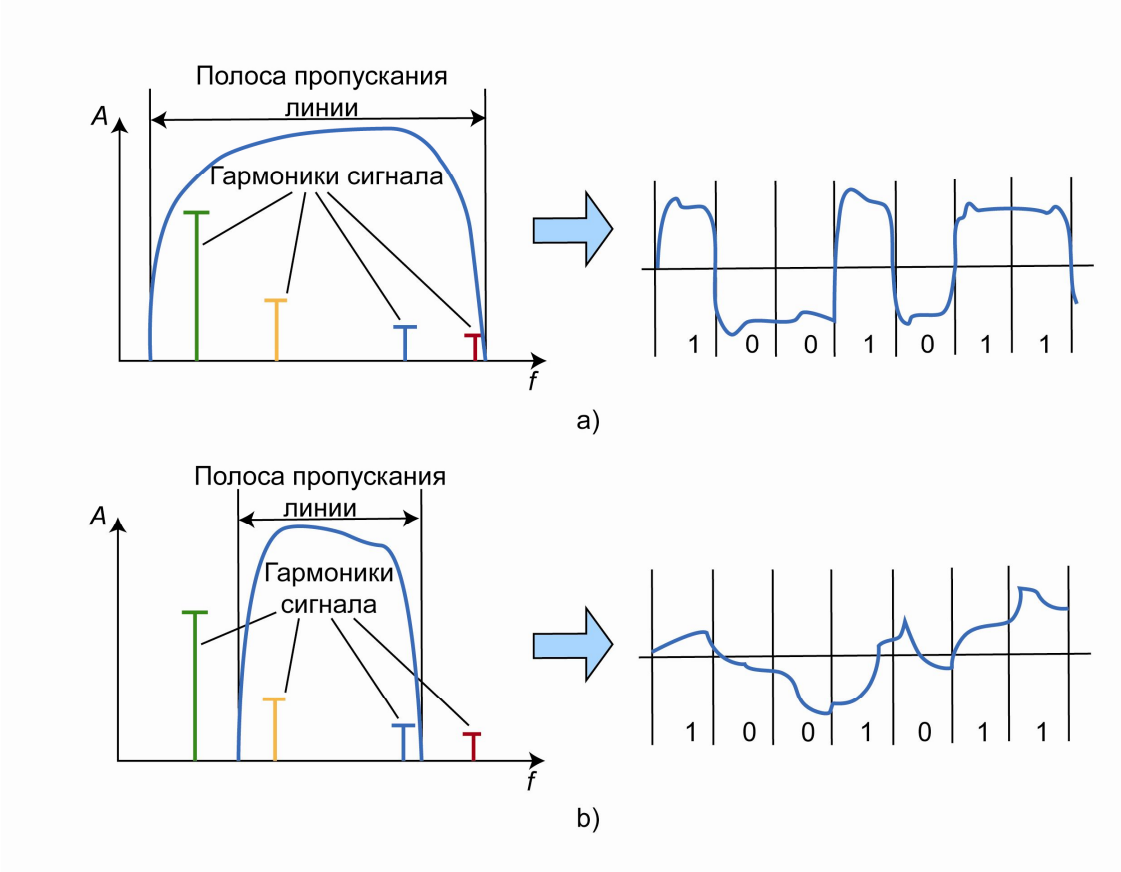


Рис. 3.13 Влияние полосы пропускания на сигнал

3.3.2 Затухание

При передаче сигнала по каналу связи, происходит его постепенное ослабление (*затухание*), что обусловлено физическими и техническими свойствами среды передачи и используемых сетевых устройств. Для корректного распознавания сигнала в точке приема это ослабление не должно превышать некоторой пороговой величины.

Затухание (*attenuation*) — это величина, показывающая, насколько уменьшается мощность (амплитуда) сигнала на выходе канала связи по отношению к мощности (амплитуде) сигнала на входе. Коэффициент затухания *d* измеряется в децибелах (дБ, dB) на единицу длины и вычисляется по следующей формуле:

$$d[\text{дБ}] = 10 \lg \frac{P_{вых}}{P_{вх}},$$

где $P_{вых}$ – мощность выходного сигнала; $P_{вх}$ – мощность входного сигнала.

Затухание характерно как для аналоговых, так и для цифровых сигналов. Оно увеличивается с ростом частоты сигнала: чем выше частота, тем сильнее сигнал подвержен затуханию. По этой причине приемникам высокоскоростного оборудования значительно сложнее распознать исходный сигнал.

Затухание сигнала влияет на расстояние, которое он может пройти между двумя точками без усиления или восстановления. Затухание является одним из важных параметров определенных для кабелей (витой пары, волоконно-оптического, коаксиального). Чем

меньше затухание, тем более качественным является кабель. Поэтому при проектировании проводных каналов связи надо учитывать характеристики кабелей и использовать кабели с наименьшим значением затухания для достижения максимальной длины канала.

3.3.3 Помехоустойчивость

В реальном канале связи существуют помехи, обусловленные характеристиками среды передачи, каналообразующей аппаратуры, влиянием электромагнитных полей различных электронных устройств. В результате действия различных помех в канале связи появляются ошибки.

Одним из важнейших показателей канала связи является его **помехоустойчивость**, под которой понимают способность канала противостоять воздействию помех. Помехоустойчивость основывается на возможности отличить сигнал от помехи с заданной достоверностью, поэтому при построении канала связи нужно учитывать возможные помехи и предельно использовать различие между ними и сигналом.

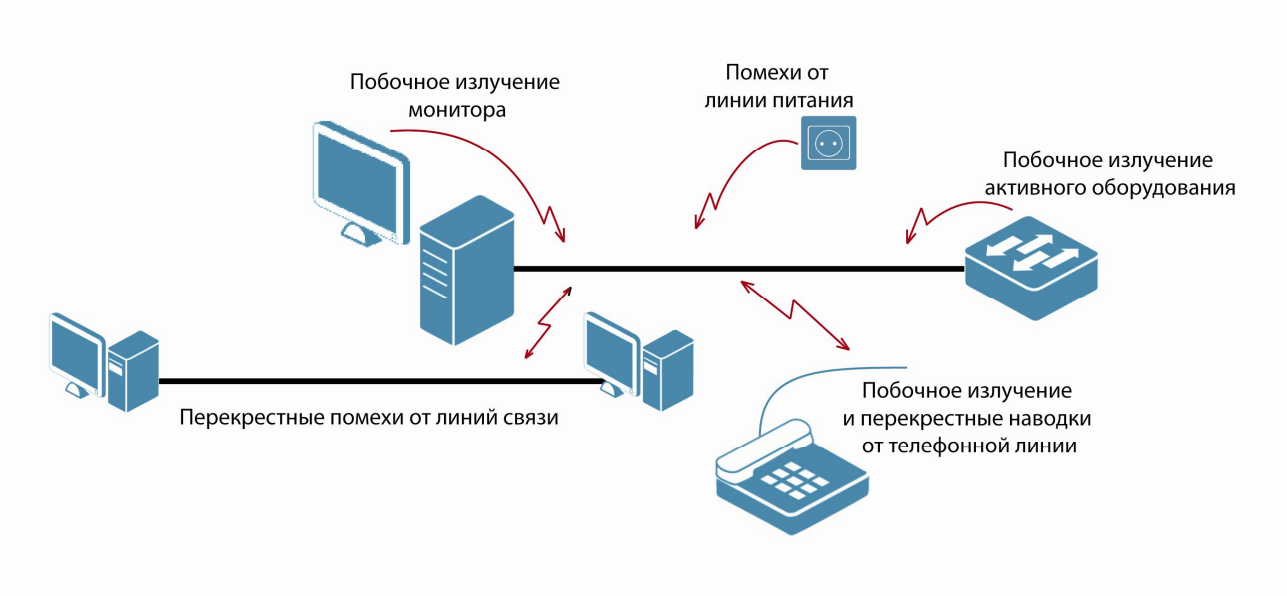


Рис. 3.14 Влияние помех на канал связи

В зависимости от источника возникновения и от характера их воздействия помехи делятся на внутренние, внешние и взаимные. *Внутренние помехи* или шумы возникают от источников находящихся в данном канале связи и появляются сразу же после включения оборудования связи. Они в основном определяются тепловыми, дробовыми, контактными и импульсными шумами и практически неустранимы.

Внешние помехи делятся на промышленные, радиопомехи, атмосферные и космические. Промышленные помехи (*электромагнитная интерференция*, Electro Magnetic Interference (EMI)) создаются в результате влияния на канал связи электромагнитных полей различных электрических устройств: ламп дневного света, бытовых приборов, компьютеров, радиосистем, линий электропередач, электрооборудования промышленных предприятий, медицинских установок, контактных сетей электрифицированного транспорта (трамвая, троллейбуса и т.п.), световой рекламы на газоразрядных лампах и т.п.

Радиопомехи (*радиочастотная интерференция*, Radio Frequency Interference (RFI)) возникают от излучения радиостанций различного назначения, спектр которых по каким-либо причинам накладывается на спектр полезных сигналов канала связи.

К атмосферным помехам относятся помехи, вызванные различными атмосферными явлениями: магнитными бурями, северными сияниями, грозовыми разрядами и т.д. К

космическим помехам относятся электромагнитные помехи, создаваемые излучениями Солнца, видимых и невидимых звезд, туманностей в соответствующих диапазонах частот.

Взаимные (перекрестные, cross talk*) помехи* или наводки возникают при передаче информации по смежным каналам – сигнал, переданный по одному каналу связи, создает нежелательный эффект в другом (возникает интерференция сигналов).

Наименее защищенными от влияния помех являются беспроводные каналы связи. На них действуют как внешние, так и перекрестные помехи. В беспроводных домашних сетях внешние помехи возникают от работающих микроволновых печей, компьютеров, сотовых телефонов и т.д. А перекрестные наводки связанны с помехами от другого беспроводного оборудования, работающего на той же частоте. Это особенно актуально в многоквартирных домах, где домашние сети в основном построены с использованием беспроводных технологий.

Среди кабельных каналов наиболее подвержены влиянию помех каналы на основе электрических кабелей. Для борьбы с помехами разработчики электрических кабелей используют: э*кранирование* (shielding) и *скручивание проводников*. Экранирование используется для защиты от электромагнитных и радиопомех. Экран представляет собой металлическую оплетку или фольгу, которая окружает каждый провод или группу проводов в кабеле. Он действует как барьер для взаимодействующих сигналов.

Электрические кабели сами являются источником электромагнитного излучения, которое может вызывать перекрестные помехи. В кабелях на основе витой пары эти помехи известны как *перекрестные наводки на ближнем конце* (Near End Cross Talk, NEXT) и *перекрестные наводки на дальнем конце* (Far End Cross Talk, FEXT) и связаны с взаимным влиянием электромагнитных полей сигналов, передаваемых по разным парам проводников. Для подавления этих электромагнитных полей используется скручивание проводников витой пары.

Наиболее защищенными от помех являются оптические каналы. На волоконно-оптические кабели не воздействуют электромагнитные помехи (EMI), радиочастотные помехи (RFI), молнии и скачки высокого напряжения. Также волоконно-оптические кабели не создают никаких электромагнитных или радиочастотных помех.

Чтобы шумы заметно не снижали качества передачи их влияние необходимо ограничивать. Методы борьбы с шумами заключаются в обеспечении такого уровня сигнала в месте приема, который бы обеспечил требуемое качество принимаемого сигнала.

Одним из важных параметров канала связи, позволяющим оценить мешающее воздействие помех на сигнал является **отношение сигнал/шум** (*SNR, Signal-to-Noise Ratio*). Оно определяется как отношение мощности сигнала P_c к мощности шума (помех) $P_ш$ и выражается в децибелах (дБ):

$$SRN\ [\text{дБ}] = 10lg\ (P_c / P_ш),$$

где P_c – мощность сигнала; $P_ш$ - мощность шума (помех).

При этом чем больше отношение сигнал/шум, тем меньше шум влияет на полезный сигнал при его передаче по каналу связи и ведет к хорошему распознаванию сигнала приемником.

Для повышения помехоустойчивости канала связи применяются следующие методы:

- увеличение отношения сигнал/шум;
- расширение спектра сигнала;
- увеличение избыточности информации;
- применение помехоустойчивых кодов;
- фильтрация полезного сигнала.

3.3.4 Пропускная способность

Пропускная способность (*throughput*) канала связи – максимально возможная *информационная* скорость передачи данных – количество данных, которое может быть передано по каналу связи за единицу времени. Измеряется пропускная способность в битах в секунду (бит/с или bps – bits per second).

Максимальная пропускная способность зависит от полосы пропускания канала связи и отношения сигнал/шум и может быть рассчитана по формуле Клода Шеннона:

$$C = F \log_2(1 + \frac{P_c}{P_ш})$$

где C – максимальная пропускная способность канала (бит/с); F – ширина полосы пропускания канала (Гц); P_c – мощность сигнала; $P_ш$ – мощность шума (помехи).

Как видно из формулы, пропускная способность канала может быть повышена за счет увеличения полосы пропускания F или увеличение отношения сигнал/шум. При этом первый способ более эффективен и менее трудоемок по сравнению со вторым, в связи с логарифмической зависимостью C от $P_c/ P_ш$.

Реальная скорость передачи данных по каналу связи обычно *меньше* его *пропускной способности* и зависит от параметров каналообразующей аппаратуры, способов организации передачи данных, количества узлов, подключенных к каналу связи. Также на снижение скорости влияют накладные расходы, связанные с передачей по сети служебных сообщений, которые требуется для работы сетевых протоколов.

Следует понимать различие между информационной скоростью и символьной скоростью. *Информационная скорость* (information rate, bitrate) – это скорость передачи битов, измеряемая в бит/с и производных единицах. *Символьная скорость* (symbol rate) или *скорость модуляции* – это скорость изменения символов, измеряемая в бодах или символах в секунду. Каждый символ представляет один или несколько битов информации в зависимости от выбранного способа их кодирования.

3.3.5 Достоверность передачи данных

Качество передаваемой по каналу связи информации принято оценивать достоверностью передачи данных, т.е. степенью соответствия принятого сообщения переданному. *Достоверность передачи данных* характеризуется вероятностью ошибочного приема каждого передаваемого бита данных, т.е. частотой появления ошибочных битов. Иногда этот же показатель называют *интенсивностью битовых ошибок* (Bit Error Rate, BER).

BER определяется как отношение количества ошибочно принятых битов к общему числу переданных.

В основном появление ошибок происходит из-за наличия помех и шумов в канале. Для каналов связи без дополнительных средств защиты величина BER составляет от 10^{-4} до 10^{-6}, в оптических каналах – 10^{-9}. Значение достоверности передачи данных, например в 10^{-4}, говорит о том, что в среднем из 10000 битов искажается значение одного бита.

Повысить достоверность передаваемых данных можно путем повышения помехоустойчивости канала связи.

3.4 Методы совместного использования среды передачи канала связи

На практике часто приходится выполнять передачу потоков данных от множества пользователей, используя общую (разделяемую) среду передачи (*shared medium*), т.к.

прокладка отдельного канала связи между всеми взаимодействующими системами слишком дорогостояща, сложна или невозможна. Чаще всего это связано с ограничениями в виде уже сформированных телефонных сетей, проложенных каналов связи, распределенного радиочастотного ресурса, невозможности прокладывания новых каналов связи из-за особенностей городской застройки и т.д.

Для того чтобы по одному кабелю или беспроводному каналу связи могло одновременно передаваться множество сигналов от разных пользователей используют методы *мультиплексирования* (*уплотнения каналов*).

Мультиплексирование (*multiplexing*) – это технология передачи данных нескольких каналов с меньшей пропускной способностью по одному каналу с большей пропускной способностью.

Задача мультиплексирования – выделить каждому каналу связи время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик общей среды передачи.

В результате мультиплексирования в одном физическом канале создается группа логических каналов. При этом *пропускная способность* физического канала *делится* между всеми *логическими каналами* и *должна быть достаточной*, чтобы обеспечивать необходимые скорости передачи данных по логическим каналам.

Мультиплексирование осуществляется с помощью программы или устройства, называемого *мультиплексором* (multiplexer, MUX). Мультиплексор соединяет группу низкоскоростных входных каналов с одним высокоскоростным физическим каналом.

Процесс обратный мультиплексированию называется *демультиплексированием*, а устройство или программа, которое выполняет этот процесс – *демультиплексором* (demultiplexer, DEMUX). Демультиплексор распределяет данные, полученные из общего физического канала по группе выходных каналов.

В компьютерных сетях используются следующие основные виды мультиплексирования:

- временно*е* мультиплексирование (TDM);
- частотное мультиплексирование (FDM);
- волновое мультиплексирование (WDM);
- мультиплексирование с кодовым разделением (CDM).

3.4.1 Мультиплексирование с разделением по времени

Мультиплексирования с разделением по времени (*Time Division Multiplexing, TDM)* или временное мультиплексирование заключается в поочередном предоставлении взаимодействующим системам всей полосы пропускания канала на небольшой промежуток времени. Другими словами: все отправители используют один и тот же диапазон частот общего канала в разные промежутки времени. Технология TDM используется в цифровых каналах связи.

Каждому входному каналу для передачи блока данных выделяется временной промежуток, называемый *тайм-слотом* или временным слотом. В качестве тайм-слота может служить интервал времени, необходимый для передачи одного бита, байта, кадра или пакета.

Существуют два типа временного мультиплексирования — *синхронный* и *асинхронный*.

В синхронном (*Synchronous Time Division Multiplexing*) режиме время работы канала делится на повторяющиеся циклы, состоящие из кадров TDM. Каждый кадр TDM начинается с синхронизирующей последовательности и включает n тайм-слотов одинаковой длительности, по одному на каждый логический канал. Тайм-слоты назначаются всем, подключенным к мультиплексору входным каналам, нумеруются и располагаются в кадре TDM в строго определенном порядке.

Входные каналы по очереди передают блоки данных одинакового размера в течение выделенных им тайм-слотов в каждом цикле. На рисунке 3.15 иллюстрируется синхронное временное мультиплексирование, обеспечивающее параллельную передачу данных между четырьмя парами устройств. Блок данных полученный портом 1 мультиплексора будет передаваться в течение тайм-слота 1 для соединения A1-A2. Блок данных полученный портом 2 будет передаваться в течение тайм-слота 2 для соединения B1-B2. Блок данных полученный портом 3 будет передаваться в течение тайм-слота 3 для соединения C1-C2. Блок данных полученный портом 4 будет передаваться в течение тайм-слота 4 для соединения D1-D2.

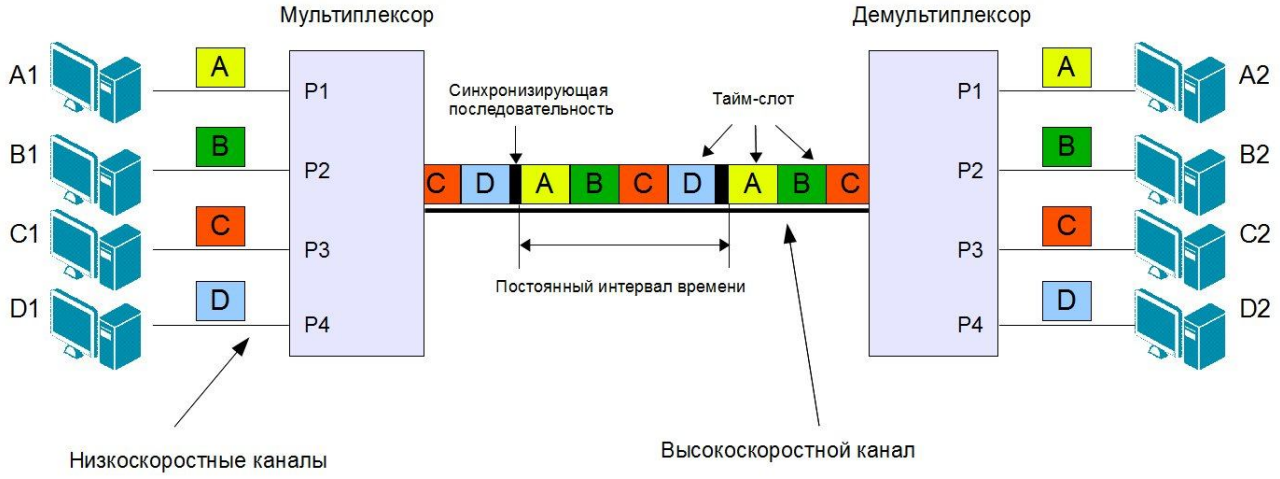


Рис. 3.15 Синхронное мультиплексирование с разделением по времени

При использовании этого метода может оказаться так, что в одном и том же цикле у одной системы не будет данных для передачи, а другой системе не будет хватать выделенного времени. При отсутствии данных для передачи у какого-либо устройства, выделенный ему тайм-слот останется пустым и не сможет быть занят другим устройством.

Для того чтобы демультиплексор на другом конце канала связи мог корректно считывать блоки данных и распределять их по соответствующим выходным каналам, порядок следования тайм-слотов в кадре TDM должен четко соблюдаться. Каждый входной канал в синхронном TDM идентифицируется своей временной позицией внутри уплотненного кадра, т.е. номером тайм-слота. Эта позиция используется как адресная информация.

Чтобы приемник мог определить начало очередного тайм-слота в кадре TDM требуется синхронизация. Синхронизация может выполняться разными способами. Например, одним из способов является передача синхронизирующей последовательности в начале кадра TDM, которая позволяет отличить один кадр из другого. Нарушение синхронности приводит к тому, что приемная сторона не может корректно распределять поступающий поток данных, так как при этом изменяется относительное положение тайм-слотов, а значит, теряется адресная информация.

Синхронный TDM используется *в сетях с коммутацией каналов*. Двумя базовыми архитектурами, основанными на синхронном TDM являются системы плезиохронной цифровой иерархии (PDH, Plesiochronous Digital Hierarchy), используемые для цифровой передачи нескольких телефонных разговоров по каналам T1 (1,544 Мбит/с), E1 (2 Мбит/с), а также цифровые системы передачи SDH/SONET, обеспечивающие передачу цифровых потоков данных как через медные, так и через оптические линии связи. Интерфейсы BRI (Basic Rate Interface) и PRI (Primary Rate Interface) сетей ISDN (Integrated Services Digital Network) также служат для транспортировки данных на основе синхронного TDM.

Пропускная способность общего канала при синхронном TDM определяется как сумма пропускной способности всех входных каналов плюс некоторые административные издержки. Одним из основных недостатков синхронного режима является привязка между

входными каналами и тайм-слотами. Если у устройства нет данных для передачи, другое устройство не может передать данные в этот тайм-слот. Это приводит к неэффективному использованию полосы пропускания и соответственно к уменьшению пропускной способности канала связи.

В качестве достоинства синхронного TDM можно назвать прозрачность для протоколов верхних уровней, т.к. он реализуется на физическом уровне модели OSI. В течение тайм-слотов можно передавать разный тип трафика: данные, голос, видео. Т.к. взаимодействующие системы получают в каждом цикле тайм-слот с одним и тем же номером, передаваемые блоки данных появляются на приемной стороне через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. В связи с этим не требуется использование буферов, т.к. поток данных передается и принимается с одной скоростью.

Буфер – это область памяти, в которой сетевое устройство временно хранит передаваемые данные.

Альтернативой синхронному временному мультиплексированию служит *асинхронное* (Asynchronous TDM, ATDM) или *статистическое* (Statistical TDM).

Статистическое мультиплексирование отличается тем, что отправитель получает тайм-слот только в том случае, если у него имеются данные для передачи. Тайм-слоты не имеют фиксированной длительности (размер передаваемого блока данных может быть переменным), не привязываются к конкретному входному каналу, а выделяются динамически, согласно статистики их запросов. Если отправитель не имеет данных для передачи, тайм-слот не остается пустым, а передается тому устройству, которое готово к передаче. Более того, отправитель, в зависимости от того сколько у него данных, может получить не один, а несколько тайм-слотов подряд.

Пропускная способность общего канала связи будет определяться средней пропускной способностью, подключенных входных каналов.

В отличие от синхронного TDM, где в качестве адресной информации использовалась позиция тайм-слота в кадре TDM, в статистическом TDM передаваемый блок данных должен содержать точную адресную информацию, чтобы данные были переданы нужному получателю.

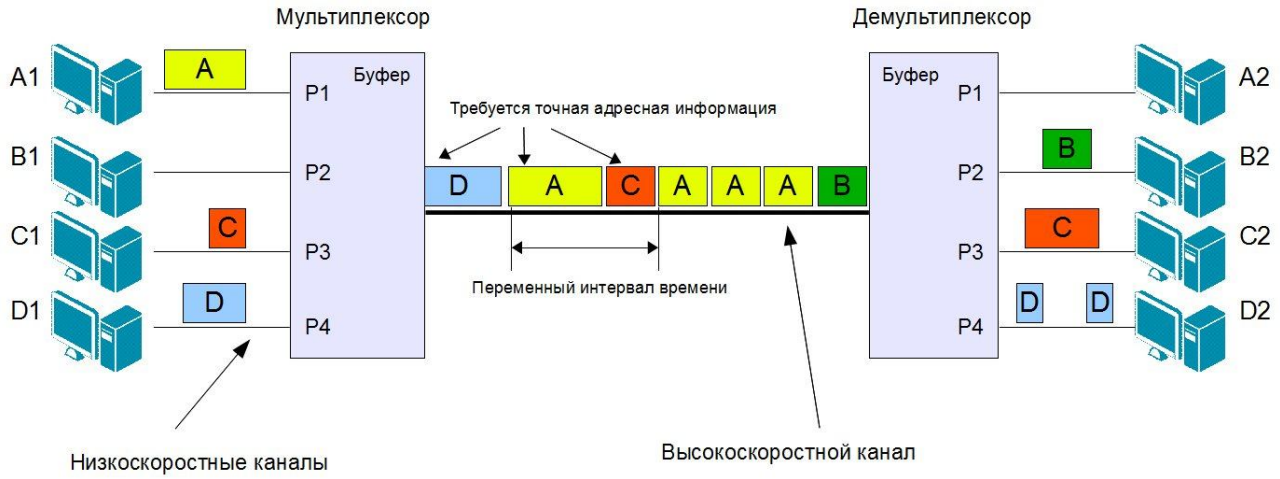


Рис. 3.16 Асинхронное мультиплексирование с разделением по времени

Обычно сетевые устройства взаимодействуют статистическим (произвольным) образом, т.к. не все из них имеют данные для передачи в одно и то же время. Если данные поступили одновременно на несколько входных портов, то использовать общий канал для передачи сможет только одна пара взаимодействующих устройств. Остальные данные,

поступившие на другие порты мультиплексора, будут помещены в буфер, и находиться там до освобождения общего канала. В противном случае они могут быть потеряны. Для решения проблемы, когда несколько отправителей хотят одновременно использовать общий канал применяются *методы множественного доступа* (*multiple access*), реализуемые на канальном уровне модели OSI.

Одна пара взаимодействующих устройств не может монопольно захватить общий канал для передачи, иначе возникло бы переполнение буфера мультиплексора (перегрузка сети). Для предотвращения переполнения буферов мультиплексоров используются специальные *методы управления потоком* (*flow control*).

Обычно буферизированные блоки данных передаются через выходной порт мультиплексора в том порядке, в котором они поступили, т.е. «первым пришел, первым ушел» (FIFO, First Input, First Output). Однако можно организовать дифференцированную или гарантированную передачу блоков данных, обеспечивая *качество обслуживания* (*Quality of Service*, QoS).

Термин «качество обслуживания» обозначает не «как быстро» пакеты передаются от отправителя к получателю, а каким образом. Пакеты от отправителя к получателю могут передаваться по разным маршрутам, могут помещаться в буфер устройства связи и долго ожидать своей очереди на передачу или наоборот передаваться раньше других, могут отбрасываться. Трафик разных приложений предъявляет разные требования к пропускной способности. Функции QoS в современных сетях заключаются в обеспечении гарантированного или дифференцированного уровня обслуживания сетевого трафика. Подробнее про функции качества обслуживания можно прочитать в книге «Технологии коммутации и маршрутизации в локальных компьютерных сетях» Е.В. Смирнова и др.

Статистический TDM используется *в сетях с коммутацией пакетов* и *в сетях с коммутацией ячеек*. В отличие от синхронного TDM, он не является прозрачным для протоколов, т.к. он реализуется на канальном и более высоких уровнях модели OSI. Конечные узлы и сетевые устройства должны поддерживать одни и те же протоколы. Примерами использования синхронного TDM могут служить протоколы семейства Ethernet, протокол IP, протоколы TCP и UDP, протокол ATM (Asynchronous Transfer Mode).

3.4.2 Мультиплексирование с разделением по частоте

При частотном мультиплексировании или **мультиплексировании с разделением по частоте** (*Frequency Division Multiplexing, FDM*) широкая полоса пропускания физического канала F делится на n узких полос частот $f<<F$, в каждой из которых создается логический канал. Размеры частотных полос f могут быть различными. Каждой взаимодействующей системе назначается отдельный поддиапазон частот (логический канал). Отправители могут посылать сигналы одновременно. Передаваемые по разным логическим каналам сигналы накладываются на разные несущие и поэтому в частотной области не должны пересекаться. Для исключения влияния друг на друга сигналов, передаваемых по разным логическим каналам, между ними формируются защитные полосы, служащие границами между каналами.

Однако, несмотря на наличие защитных полос, спектральные составляющие сигнала могут выходить за границы логического канала и вызывать помехи в соседнем логическом канале.

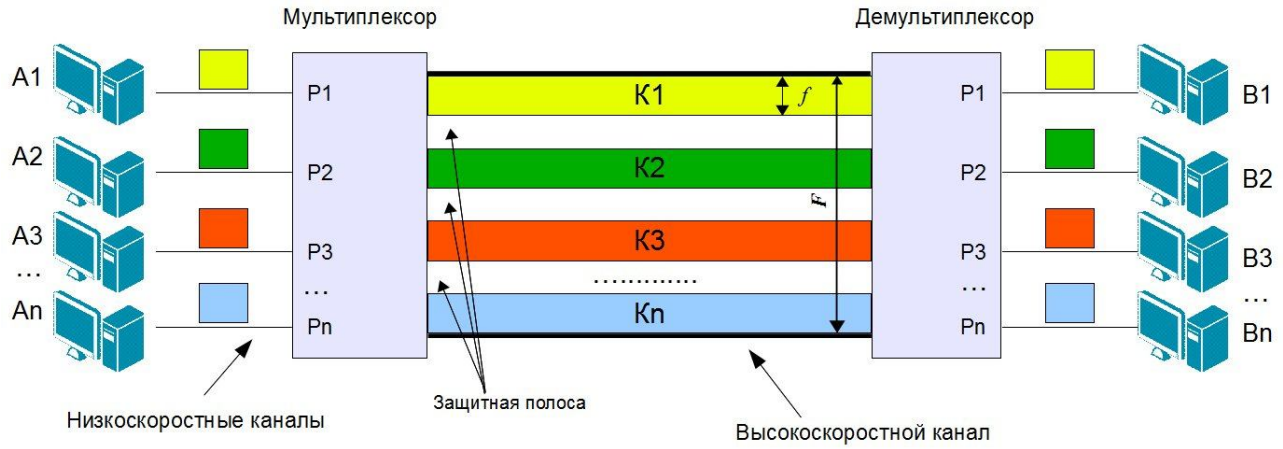


Рис. 3.17 Мультиплексирование с разделением по частоте

Преимуществом частотного мультиплексирования является возможность одновременной передачи сигналов несколькими взаимодействующими системами. Однако из-за того, что каждой системе статически назначается отдельный канал, происходит неэффективное использование полосы пропускания общего канала связи. В какой-то момент времени у одной системы данные для передачи могут отсутствовать и канал останется пустым, в то время как другим системам будет не хватать ресурсов, выделенных им логических каналов. Также наличие защитных полос между логическими каналами уменьшает доступную для передачи полосу пропускания.

Мультиплексирование с разделением по частоте является широко используемым методом мультиплексирования, используемым в теле- и радиовещании и сотовой связи. Также оно применяется в сетях на основе технологий xDSL.

Однако при частотном мультиплексировании можно делить полосу пропускания на каналы не используя защитные полосы. При **мультиплексировании с ортогональным частотным разделением** (*Orthogonal Frequency Division Multiplexing, OFDM*) вся полоса пропускания физического канала разделена на достаточно большое количество *поднесущих* (от нескольких сот до тысяч). Каждой взаимодействующей системе (передатчику и приемнику) назначают для передачи несколько таких поднесущих, выбранных из множества по определенному закону. Центры поднесущих частот размещены так, что пик каждого последующего сигнала совпадает с нулевым значением предыдущих. Такое размещение позволяет более эффективно использовать доступную полосу частот. Передача ведется одновременно всеми поднесущими, т. е. в каждом передатчике исходящий высокоскоростной поток данных разбивается на n низкоскоростных потоков (n - число поднесущих, назначенных данному передатчику), которые передаются на поднесущие параллельно. Это разделение используется для того, чтобы бороться с дефектами канала связи. На уровне поднесущих это сделать легче. Распределение поднесущих в ходе работы может динамически изменяться, что делает этот метод не менее гибким, чем статистическое временное мультиплексирование.

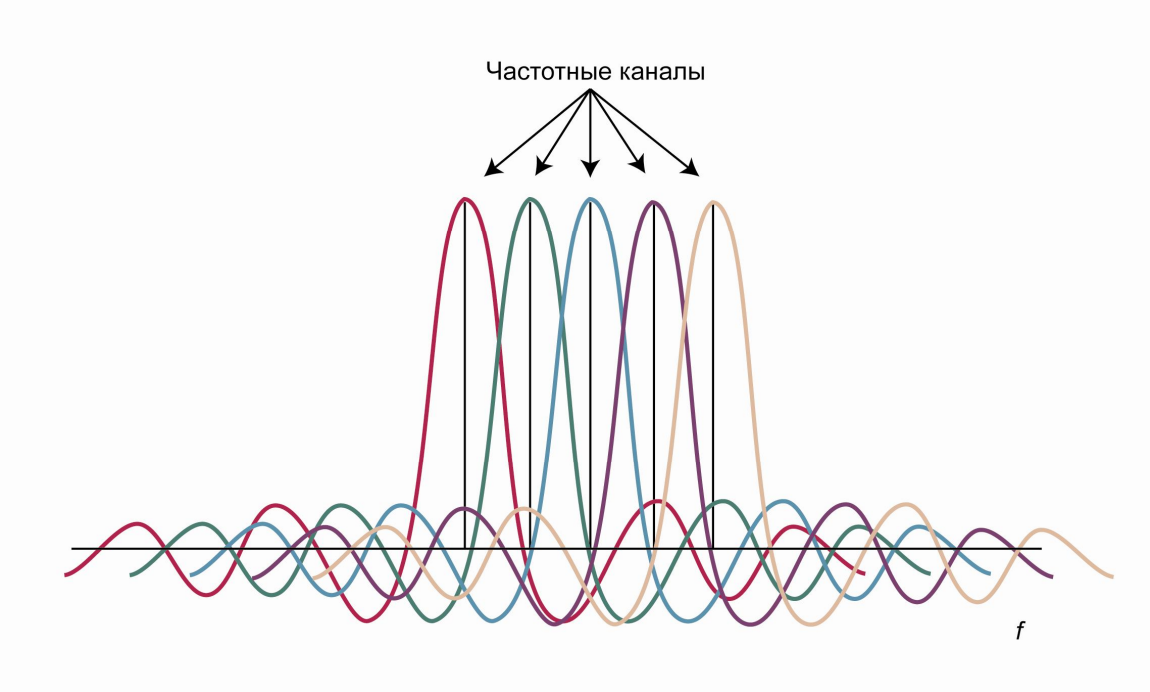


Рис. 3.18 Мультиплексирование с ортогональным частотным разделением

OFDM используется с беспроводных сетях стандарта 802.11, сетях кабельного телевидения, в сетях на основе электрической проводки, в сетях на основе технологий xDSL, в сетях мобильной передачи данных 4-го поколения LTE.

3.4.3 Мультиплексирование со спектральным разделением

Мультиплексирование со спектральным разделением (*Wavelength Division Multiplexing, WDM*) или волновое мультиплексирование используется в оптических каналах связи и является вариантом частотного мультиплексирования. Технология WDM позволяет по одному оптическому волокну одновременно и независимо передавать два и более оптических сигнала, используя разные длины волн. Эта технология также делает возможной двунаправленную передачу сигналов по одному волокну (передача на одной длине волны, прием на другой длине волны).

Сигналы каждого входного канала переносятся в собственном диапазоне частот. Далее они собираются в мультиплексоре и передаются уже по одному волокну, образуя широкополосный канал. Разделение частоты в оптическом волокне выполняется направлением в него лучей света с разными длинами волн: каждый лазерный передатчик излучает свет на заданной частоте (частоте светового диапазона) в один световод. Излучение каждого из них проходит через световод независимо друг от друга. Таким образом, в одном волокне параллельно создается несколько независимых каналов (каждый на своей длине волны), что позволяет повысить пропускную способность системы передачи в целом.

На приемной стороне демультиплексор разделяет частоты сигналов с помощью фильтров.

Рис. 3.19 Мультиплексирование со спектральным разделением

Технология WDM реализуется на физическом уровне модели OSI и поэтому прозрачна для протоколов верхних уровней. Большинство WDM-систем используют для работы одномодовые оптические кабели с диаметром волокна 9/125 мкм.

Самая простая и дешевая реализация технологии WDM использует два канала – один на длине волны 1310 нм, другой на длине волны 1550 нм. Для создания такой WDM-системы могут использоваться оптические трансиверы без жесткого контроля длин волн.

Технология CWDM (Coarse WDM, мультиплексирование с разреженным спектральным разделением) является развитием технологии WDM, которая позволяет использовать до 18 оптических каналов (как определено в ITU-T G.694.2), отстоящих друг от друга на расстоянии 20 нм для передачи оптических сигналов. Оптические каналы лежат в диапазоне от 1271 до 1611 нм. Из-за высокого затухания в диапазоне 1271-1451 нм большинство CWDM-реализаций используют 8 каналов в диапазоне 1471-1611 нм. Данные по каждому каналу могут передаваться со скоростью до 10 Гбит/с.

Для создания CWDM-систем используются оптические трансиверы, мультиплексоры и демультиплексоры с определенными длинами волн, но так как эти длины волн не требуется жестко контролировать, стоимость этого оборудования ниже, чем стоимость оборудования для DWDM-систем.

Технология Dense WDM (DWDM, мультиплексирование с плотным спектральным разделением) также является вариантом технологии WDM и позволяет разместить 40, 80 и даже 160 оптических каналов в узком диапазоне между 1525-1565 нм или 1570-1610 нм (сетка частот DWDM определена в ITU-T G.694.1-2012). Оптические каналы отстоят друг от друга на расстоянии около 0,8 нм, 0,4 нм или 0,2 нм. Данные по каждому каналу передаются со скоростью 10 Гбит/с, при этом возможен дальнейший переход на сервисы 40 Гбит/с и 100 Гбит/с.

Технология DWDM сложнее, чем технология CWDM и требует жесткого контроля длин волн и стабилизации температуры со стороны оборудования – оптических трансиверов, мультиплексоров и демультиплексоров.

Компания D-Link выпускает оптические трансиверы SFP, XFP и SFP+ для создания WDM и CWDM-систем. Обзор оптических трансиверов будет приведен в главе 5.

Технология WDM применяется в основном на линиях связи большой протяженности, где требуется большая полоса пропускания. Использование технологии WDM позволяет исключить дополнительную прокладку оптических кабелей в существующей сети и повысить пропускную способность имеющегося оптического канала за счет увеличения количества логических каналов (длин волн излучаемых лазерными передатчиками). На фоне постоянно увеличивающегося объема трафика это особенно актуально для провайдеров услуг, которые хотят предоставлять клиентам дополнительные сервисы. Новый сервис может быть добавлен поверх существующего оптического кабеля без приостановки предоставления услуг клиентам.

Помимо предоставления сервисов, использование технологии WDM позволяет операторам связи оказывать такую услугу как предоставление в аренду «виртуального волокна», т.е. предоставление в аренду отдельных длин волн.

Частотное (волновое) и временное мультиплексирование может применяться одновременно. В этом случае в физическом канале выделяются частотные полосы. В любой из этих полос каждой системе для передачи данных предоставляются определенные интервалы времени.

Примером комбинации частотного и временного мультиплексирования служит система сотовой связи GSM (Global System for Mobile Communications).

3.4.4 Мультиплексирование с кодовым разделением

Мультиплексирование с кодовым разделением (*Code Division Multiplexing, CDM*) отличается от частотного и временного мультиплексирования. В данном методе все каналы используют один и тот же спектр частот в одно и то же время, но при этом каждый канал имеет свой уникальный код.

При кодовой модуляции используется метод *расширения спектра* (*Spread Spectrum*), который служит для защиты от узкополосной интерференции. Основная его идея заключается в преобразовании информационного сигнала с узкой полосой пропускания в сигнал с широкой полосой пропускания. Достигается это кодированием информационного сигнала шумоподобным псевдослучайным кодовым сигналом, который полностью независим от информационного сигнала и имеет большую полосу пропускания. При преобразовании исходного сигнала его мощность не изменяется, а распределяется по более широкой полосе пропускания и становится сопоставима с интегральной мощностью шума.

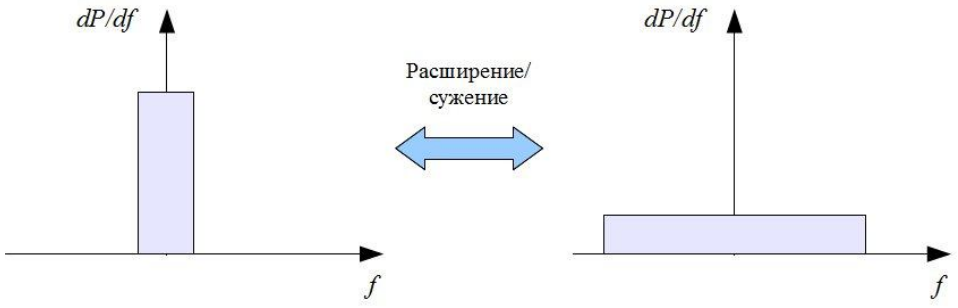


Рис. 3.20 Метод расширения спектра

Каждый передатчик заменяет каждый бит исходного потока данных на кодовую последовательность длиной в 11, 16, 32, 64 и т. п. бит (их называют чиповыми последовательностями или чипами) с помощью операции XOR. Кодовая последовательность уникальна для каждого передатчика и служит для идентификации соединения. Сходства кодовых сигналов со случайным (гауссовым) шумом добиваются, используя генератор псевдослучайных последовательностей. Далее такой шумоподобный сигнал передается передатчиком в общий канал, через который одновременно передаются сигналы от множества других передатчиков.

Приемник знает кодовую последовательность передатчика, сигналы которого должен принимать. Это позволяет выделить предназначенный ему сигнал из множества других сигналов. При этом сигналы других передатчиков с другими кодовыми последовательностями приемник воспринимает как аддитивный шум.

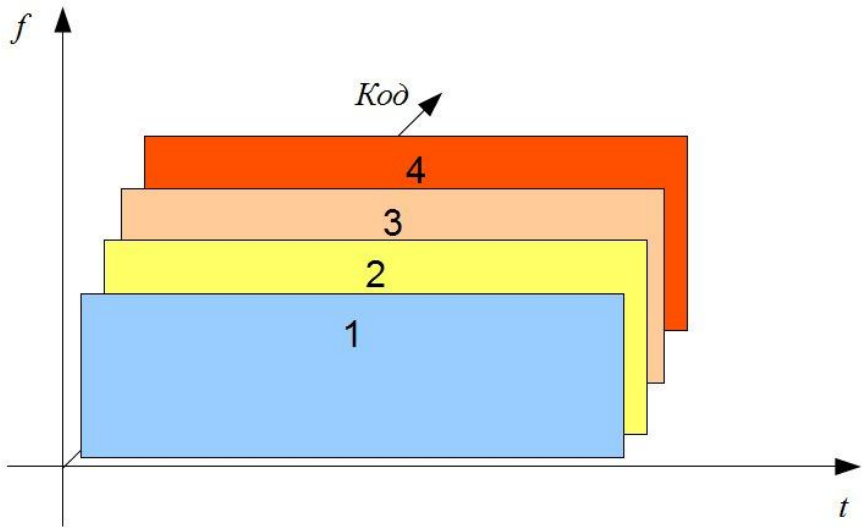


Рис. 3.21 Мультиплексирование с кодовым разделением

Основное достоинство данного способа мультиплексирования заключается в повышенной защищенности и скрытности передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев – и обнаружить его присутствие. Изначально это метод использовался в военных приложениях (первая статья по этой теме была опубликована в 1935 г. советским ученым Д. В. Агеевым), а позже стал использоваться в гражданских приложениях. Кроме того, кодовое пространство несравненно более значительно по сравнению с частотной схемой мультиплексирования, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код. Основной же проблемой кодового мультиплексирования до недавнего времени являлась сложность технической реализации приемников и необходимость обеспечения точной синхронизации передатчика и приемника для гарантированного получения блока данных.

Используется CDM в основном в сетях мобильной и беспроводной связи стандарта IEEE 802.11. На этом механизме основан метод *множественного доступа с кодовым разделением* (*Code Division Multiple Access, CDMA*), именем которого назван стандарт сотовой телефонной связи IS-95a, а также ряд стандартов третьего поколения сотовых систем связи (CDMA2000, WCDMA и др.).

3.4.5 Мультиплексирование и методы множественного доступа

Мультиплексирование и **множественный доступ** (multiple access) сходны тем, что предполагают разделение общего ресурса между пользователями. Мультиплексирование позволяет множеству пользователей одновременно использовать один общий физический канал для передачи множества сообщений. Методы множественного доступа основаны на методах временного, частотного и кодового мультиплексирования и определяют, как логические каналы распределяются между множеством пользователей, а также упорядочивают ситуацию, в которой несколько пользователей одновременно хотят использовать один канал (в том случае, если логических каналов меньше чем пользователей).

Мультиплексирование реализуется на физическом уровне модели OSI, в то время как методы множественного доступа реализуются на физическом уровне и *подуровне MAC* (*Media Access Control, управление доступом к среде*), который является частью канального уровня модели OSI.

Методами доступа, основанными на мультиплексировании TDM являются *множественный доступ с разделением времени* (TDMA, Time division multiple access),

множественный доступ с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access With Collision Detection, CSMA/CD), *множественный доступ с контролем несущей и предотвращением коллизий* (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA), *передача маркера* (Token passing).

Методами доступа, основанными на мультиплексировании FDM являются *множественный доступ с разделением частоты* (Frequency Division Multiple Access, FDMA), *множественный доступ с ортогональным частотным разделением* (Orthogonal Frequency Division Multiple Access, OFDMA), *множественный доступ с разделением длины волны* (Wavelength Division Multiple Access, WDMA).

На мультиплексировании CDM основан метод *множественного доступа с кодовым разделением* (Code Division Multiple Access, CDMA).

3.5 Модуляция и кодирование сигналов

Как правило, информационные сигналы являются низкочастотными и ограниченными по ширине спектра (*основополосными*). Передачу основополосных сигналов напрямую (в основной полосе частот) выполняют основополосные каналы связи (baseband channel). Они имеют узкую полосу пропускания, поэтому она вся используется для передачи сигнала.

Однако не во всех случаях исходный сигнал можно напрямую передать по каналу связи. Например, канал связи является высокочастотным, широкополосным и рассчитан на передачу сигналов от множества источников одновременно с частотным разделением каналов.

Для того чтобы перенести спектр сигнала из низкочастотной области в выделенную для их передачи область высоких частот используется *модуляция*.

Допустим, что низкочастотный сигнал, подлежащий передаче по каналу связи, задается функцией s(t). В канале связи для передачи данного сигнала выделяется определенный диапазон высоких частот. На входе канала связи в специальном передающем устройстве формируется вспомогательный, как правило, непрерывный во времени периодический высокочастотный сигнал u(t). Если изменить параметры сигнала u(t) в соответствии с формой сигнала s(t), то форма сигнала u(t) приобретает новое свойство. Она несет информацию, тождественную информации в сигнале s(t).

Поэтому сигнал u(t) называют *несущим сигналом*, *несущим колебанием* или просто **несущей (carrier)**, а процесс переноса информации на параметры несущего сигнала – его *модуляцией* (*modulation*).

Модуляция (modulation) – это процесс изменения одного сигнала в соответствии с формой другого сигнала.

Информационный сигнал s(t) называют *модулирующим (modulating signal)*, результат модуляции – *модулированным сигналом (modulated signal)*. Обратную операцию выделения модулирующего сигнала из модулированного колебания называют **демодуляцией (demodulation)**.

Выполняются операции модуляции и демодуляции с помощью *модема* (modem, **mo**dulator - **de**modulator), который может быть отдельным устройством или входить в состав других устройств.

Основным назначением модуляции является сдвиг спектра сигнала в другой частотный диапазон, обеспечение механизма представления информации в наименее чувствительной к помехам и интерференции форме и возможность использования методов мультиплексирования и множественного доступа.

При широкополосной передаче использование нескольких несущих с различными частотами позволяет в одном физическом канале прокладывать несколько логических каналов.

Для того чтобы различать модуляцию аналоговых и цифровых сигналов модуляцию аналогового сигнала на основе несущей называют **аналоговой модуляцией** (**analog modulation**), модуляцию цифрового сигнала на основе несущей называют **цифровой модуляцией** (**digital modulation**) или *манипуляцией*.

Несущая, как правило, требуется при передаче данных через телефонные провода, атмосферу или оптический кабель. Однако в некоторых случаях модуляция может выполняться на основе дискретных сигналов в виде импульсов. Для передачи аналоговых сигналов на основе периодических последовательностей импульсов используется **импульсная модуляция** (**pulse modulation**).

При передаче цифровых сигналов через основополосные каналы связи применяются методы **линейного или цифрового кодирования сигналов (line coding)**.

3.5.1 Методы аналоговой модуляции

Аналоговая модуляция основана на передаче аналогового низкочастотного сигнала с помощью высокочастотной несущей. Основным видом несущих сигналов являются гармонические колебания, которые имеют три свободных параметра амплитуду, фазу и частоту.

В зависимости от того, на какой из данных параметров переносится информация, различают *амплитудную* (АМ), *частотную* (ЧМ) или *фазовую* (ФМ) модуляцию несущего сигнала. Частотная и фазовая модуляция взаимосвязаны, поскольку изменяют аргумент функции косинуса, и их обычно объединяют под общим названием - *угловая модуляция* (*angle modulation*). **Амплитудная модуляция (Amplitude modulation, AM)** связанна с изменением амплитуды несущей в соответствии с текущей амплитудой модулирующего сигнала. При **частотной модуляции (Frequency modulation, FM)** частота несущего сигнала изменяется в соответствии с текущей амплитудой модулирующего сигнала. При **фазовой модуляции (Phase modulation, PM)** сдвиг фаз несущего сигнала изменяется в соответствии с текущей амплитудой модулирующего сигнала.

Аналоговая модуляция используется в радиовещании при работе нескольких радиостанций в общей среде передачи: амплитудная модуляция для работы радиостанций в AM-диапазоне, частотная модуляция для работы в FM-диапазоне.

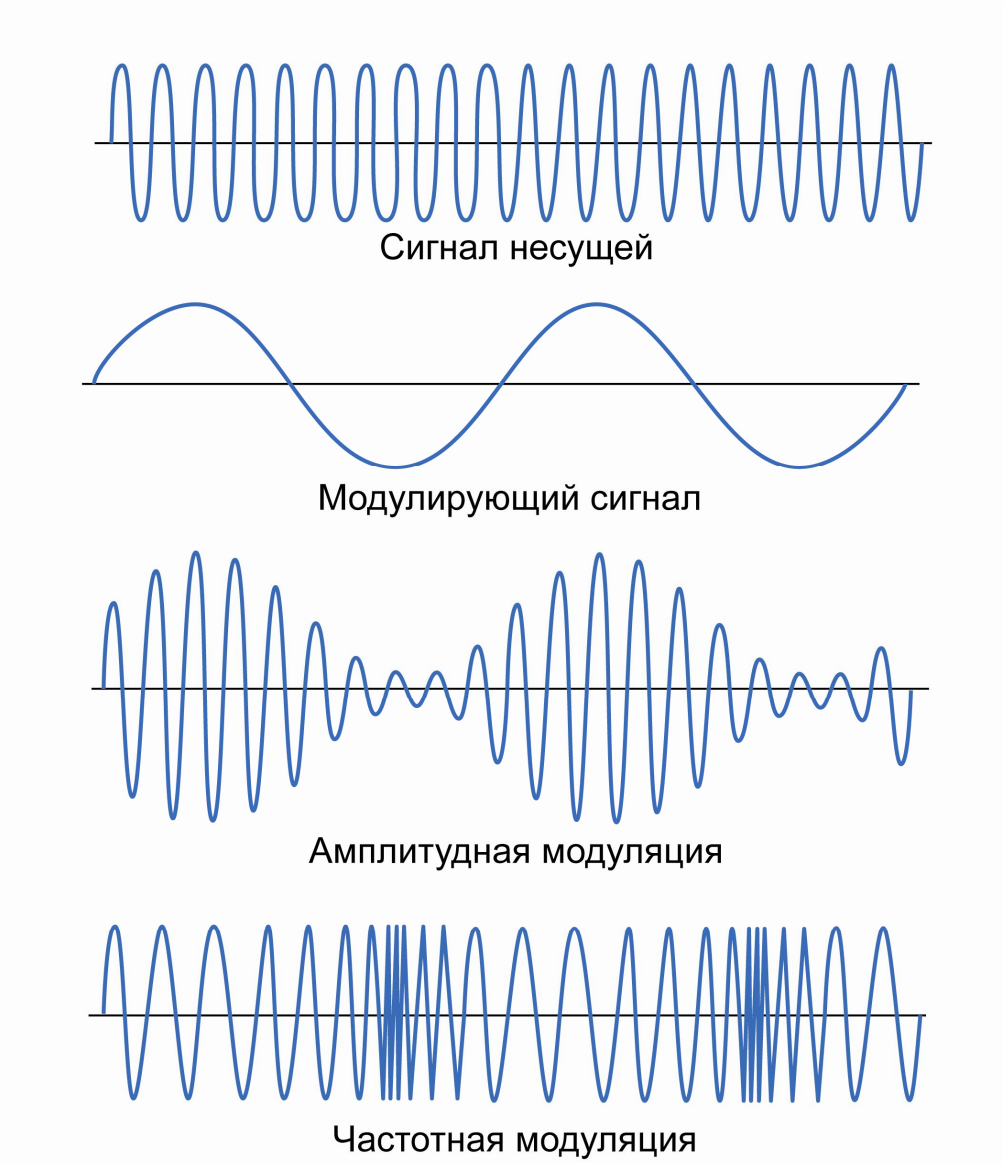


Рис. 3.22 Амплитудная и частотная модуляция аналогового сигнала

3.5.2 Методы импульсной модуляции

Импульсная модуляция позволяет передавать исходный аналоговый сигнал на основе последовательности импульсов, как правило – прямоугольных. Параметрами модуляции при этом могут быть амплитуда, длительность, частота следования импульсов и фаза (положение импульса относительно определенной точки тактового интервала). В беспроводных системах передачи данных (в радиосвязи) эти последовательности импульсов заполняются высокочастотными колебаниями, создавая тем самым двойную модуляцию.

Импульсная модуляция является распространенным методом модуляции при передаче дискретизированных данных по цифровым каналам связи, а также позволяет выполнять одновременную передачу сигналов по одному каналу связи, используя мультиплексирование с разделением по времени.

Существует несколько методов импульсной модуляции:

- амплитудно-импульсная модуляция;
- импульсно-кодовая модуляция;
- широтно-импульсная модуляция;
- позиционно-импульсная модуляция.

Амплитудно-импульсная модуляция (АИМ) (Pulse Amplitude Modulation, PAM) заключается в преобразовании модулирующего сигнала в совокупность импульсов с определенной амплитудой при постоянной длительности импульсов и периоде их следования. Для этого модулирующий сигнал подвергается дискретизации (квантованию) по времени. Период и частота следования импульсов определяются теоремой Найквиста-Котельникова $1/T = f_d \geq 2f_в$, где f_d – это частота дискретизации; $f_в$ – это наивысшая частота в спектре информационного сигнала. В полученные таким образом дискретные моменты времени амплитуды импульсов пропорциональны амплитуде модулирующего сигнала.

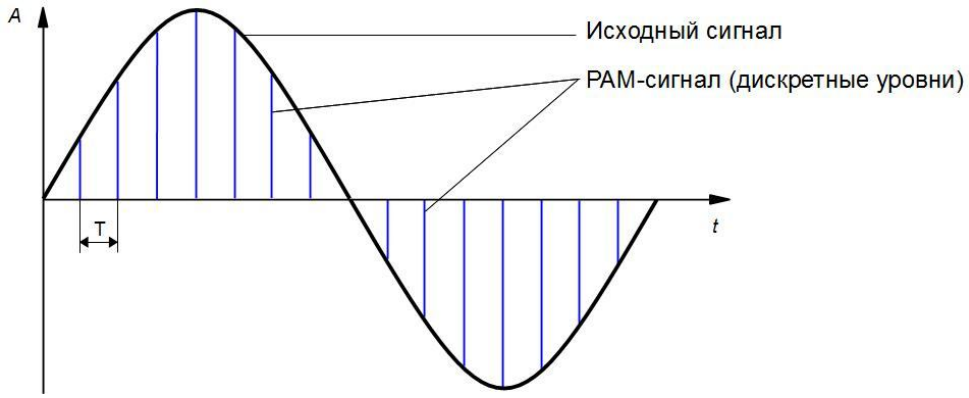


Рис. 3.23 Амплитудно-импульсная модуляция

Импульсно-кодовая модуляция (ИКМ) (Pulse Code Modulation, PCM) заключается в том, что в точках дискретизации модулирующего сигнала производится квантование его значений и кодирование квантованных значений, как правило, в двоичной системе исчисления. Кодированные значения затем передаются при помощи соответствующей кодовой последовательности стандартных символов.

Этот вид модуляции используется для передачи голоса через телефонные сети или передачи данных по оптическим каналам связи.

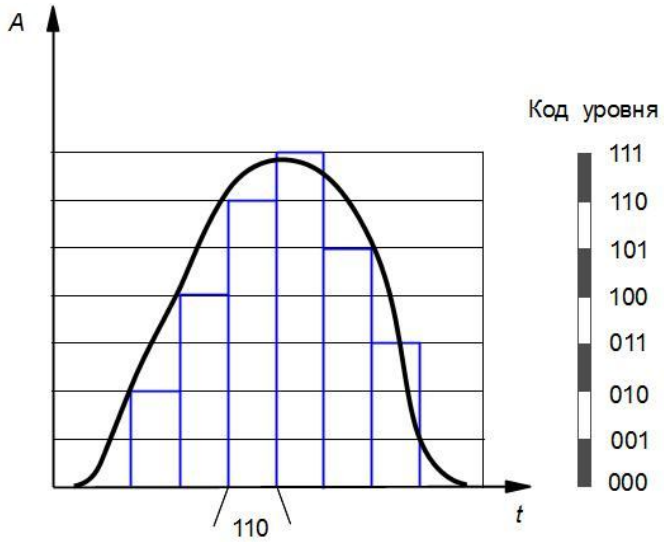


Рис. 3.24 Импульсно-кодовая модуляция

Широтно-импульсная модуляция (ШИМ) (Pulse Width Modulation, PWM), которую иногда называют модуляцией по длительности импульсов (ДИМ), заключается в управлении длительностью импульсов пропорционально функции модулирующего сигнала при постоянной амплитуде импульсов и периоде следования по фронту импульсов.

При осуществлении **позиционно-импульсной модуляции** (ПИМ) (Pulse Position Modulation, PPM) импульсы имеют одинаковую амплитуду и длительность, однако отстоят от начала периода на интервалы времени, пропорциональные информационному сигналу.

Обычно этот тип модуляции используется при передаче данных по оптическим каналам связи.

3.5.3 Методы цифровой модуляции

Процесс передачи цифровых данных с помощью несущей называется **цифровой модуляцией** или **манипуляцией**.

Для того чтобы цифровые данные могли быть переданы по аналоговому каналу они должны быть сначала преобразованы в аналоговый основополосный сигнал, а затем результирующий сигнал центрируется на несущей частоте для оптимальной передачи через среду передачи.

Существуют три основные технологии модуляции, выполняющие преобразование цифровых данных в аналоговый сигнал:

- амплитудная модуляция (Amplitude-Shift Keying, ASK);
- частотная модуляция (Frequency-Shift Keying, FSK);
- фазовая модуляция (Phase-Shift Keying, PSK).

При **амплитудной модуляции (ASK)** значения «0» и «1» представляются сигналами несущей частоты с двумя различными амплитудами. Одна из амплитуд, как правило, выбирается равной нулю; т.е. одно двоичное число представляется наличием несущей частоты при постоянной амплитуде, а другое – ее отсутствием.

При **частотной модуляции (FSK)** значения «0» и «1» передаются синусоидами с различной частотой.

При **фазовой модуляции (PSK)** значениям «0» и «1» соответствуют синусоиды с одиноковой амплитудой и частотой, но с различной фазой.

Квадратурная амплитудная модуляция (*Quadrature Amplitude Modulation, QAM*) является популярным методом аналоговой передачи сигналов, используемым в некоторых стандартах беспроводных и проводных сетей.

Данная схема модуляции совмещает в себе амплитудную и фазовую модуляции. В методе QAM использованы преимущества одновременной передачи двух различных сигналов на одной несущей частоте, но при этом задействованы две копии несущей частоты, сдвинутые относительно друг друга на 90°. При квадратурной амплитудной модуляции обе несущие являются амплитудно-модулированными. Два независимых сигнала одновременно передаются через одну среду. В приемнике эти сигналы демодулируются, а результаты объединяются с целью восстановления исходного двоичного сигнала.

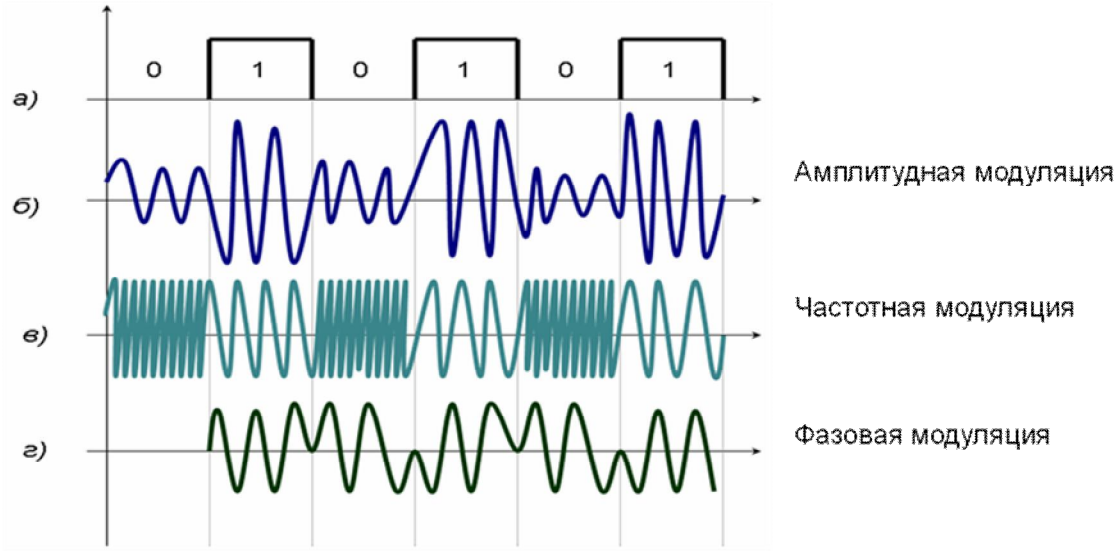


Рис. 3.25 Модуляция цифровых данных аналоговыми сигналами

3.5.4 Методы цифрового кодирования

Цифровое кодирование используется для цифровой основополосной модуляции дискретных данных и обычно отражает технические требования среды передачи, такой как оптический кабель или витая пара. Эти требования уникальны для каждой среды передачи, т.к. каждая из них имеет различную помехозащищенность, полосу пропускания и потери при затухании.

При цифровом кодировании дискретной информации применяют потенциальные и импульсные коды.

В потенциальных кодах для представления логических единиц и нулей используется только значение потенциала сигнала (уровень напряжения), а его перепады, формирующие законченные импульсы, во внимание не принимаются.

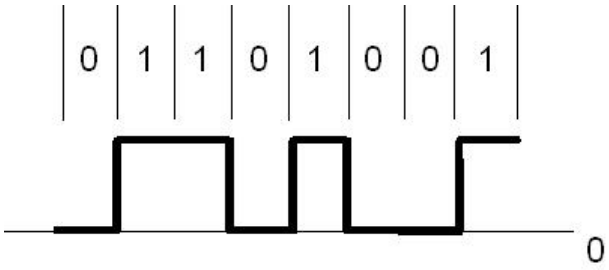


Рис. 3.26 Потенциальное кодирование

Импульсные коды позволяют представить двоичные данные изменением полярности импульса (рис. 3.27, а) или перепадом напряжения (рис. 3.27, б).

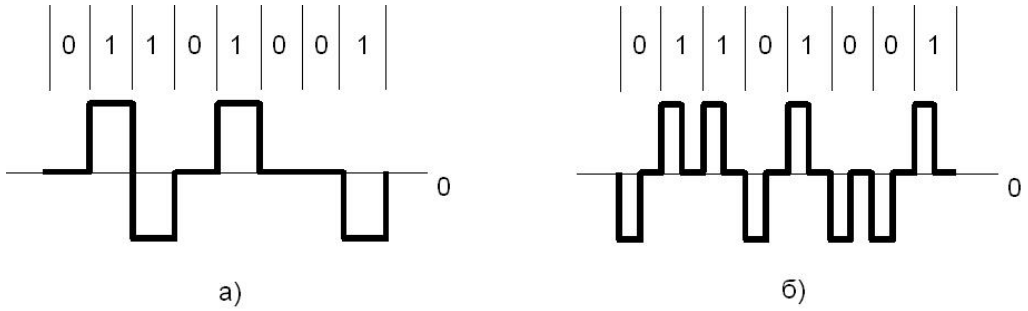


Рис. 3.27 Импульсное кодирование

Время, затрачиваемое на передачу одного бита (0 или 1) информации, называется **битовым интервалом**. Длительность битового интервала t_b связана с пропускной способностью канала следующим образом: $t_b = 1/C$.

Как известно, при передаче по каналу связи сигнал затухает, и его мощность в точке приема становится значительно ниже мощности исходного сигнала. Также в любом реальном канале связи имеются шумы, которые накладываются на информационный сигнал и могут повлиять на его нормальное распознавание. Понятно, что на приемной стороне наибольшую мощность сигнал сохраняет в центре битового интервала. Поэтому для нормального распознавания сигнала, желательно считывать его значение в центре битового интервала. Для этого передающая и приемная стороны должны иметь высокоточные таймеры, с помощью которых на передающей стороне будут определяться моменты формирования сигналов, а на приемной – моменты считывания значения сигнала. Для качественного распознавания сигнала необходимо, чтобы таймеры передатчика и приемника работали синхронно. Однако понятно, что таймеры могут иметь некоторую погрешность, которая со временем приведет к различию в их показаниях на передающей и приемной стороне. Это в свою очередь вызовет ошибки при приеме битов. Для того чтобы не возникали такие ситуации необходимо поддерживать синхронизацию таймеров передатчика и приемника. Для решения это проблемы в компьютерных сетях используются специальные методы кодирования, позволяющие автоматически выполнять синхронизацию таймеров приемника и передатчика. Такие коды называются *самосинхронизирующимися*.

При потенциальном кодировании передача длинной последовательности 0 или 1 приводит к появлению в сигнале постоянной составляющей, и частота сигнала будет равна нулю. Каналы связи с большой полосой пропускания имеют нижнюю границу частот значительно отличающуюся от нулю. Также будет трудно поддерживать синхронизацию между передатчиком и приемником. Поэтому сигнал будет передаваться с большими искажениями, что затруднит его распознавание. При передаче чередующихся 0 и 1 постоянная составляющая отсутствует.

Методы цифрового кодирования оказывают существенное влияние на качество передачи дискретных данных и определяют требуемую пропускную способность среды передачи.

Поэтому к методам цифрового кодирования предъявляют следующие требования:

- минимизация спектра результирующего сигнала при одной и той же битовой скорости;
- возможность распознавания и исправления ошибок;
- поддержка синхронизации между приемником и передатчиком;
- низкая стоимость реализации.

На принимающей стороне выполняется симметричное декодирование.

В общем случае кодирование может быть двухступенчатым:

- логическое кодирование;
- физическое кодирование.

3.5.4.1 Физическое кодирование

Физическое кодирование – способ представления дискретной информации в виде электрических или оптических сигналов, подаваемых на линию связи.

Рассмотрим наиболее часто используемые способы физического кодирования:

- Потенциальный код без возврата к нулю (NRZ, Non Return to Zero);
- Потенциальный код без возврата к нулю с инверсией при единице (NRZI, Non Return to Zero with one Inverted);
- Манчестерский код (Manchester code);
- Код трехуровневой передачи MLT-3 (Multi Level Transmission-3);
- Пятиуровневый код PAM-5 (Pulse-amplitude modulation -5).

В методе *потенциального кодирования без возврата к нулю* (NRZ) нижний потенциал соответствует 0, верхний – 1. Переходы происходят на границе такта. При передаче последовательности единиц сигнал не возвращается к нулю в течение такта.

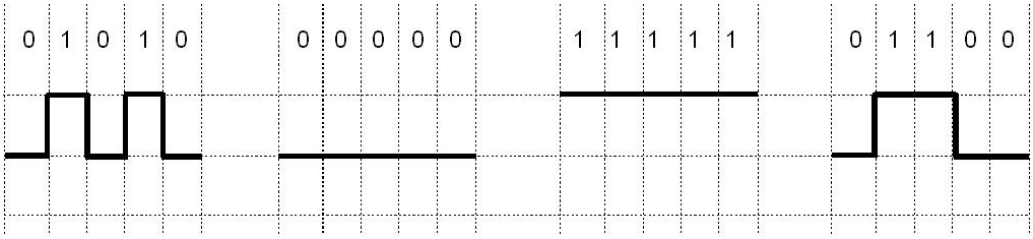


Рис. 3.28 Потенциальный код NRZ

Спектр реального сигнала постоянно меняется в зависимости от того, какова структура данных, передаваемых по каналу связи. Однако при передаче длинных последовательностей нулей или единиц спектр сигнала сдвигается в сторону низких частот, приближаясь к постоянному сигналу, и не всегда обеспечивает приемнику возможность синхронизироваться с передатчиком. С другой стороны код NRZ прост в реализации, обладает хорошей помехоустойчивостью (благодаря наличию двух резко отличающихся уровней сигнала).

Код NRZ используется на физическом уровне стандартов 1000BASE-SX, 1000BASE-LX.

Потенциальный код без возврата к нулю с инверсией при единице (NRZI) является модификацией кода NRZ.

NRZI при передаче 0 передает потенциал, который был установлен в предыдущем такте (уровень сигнала не меняется), а при передаче 1 потенциал инвертируется на противоположный.

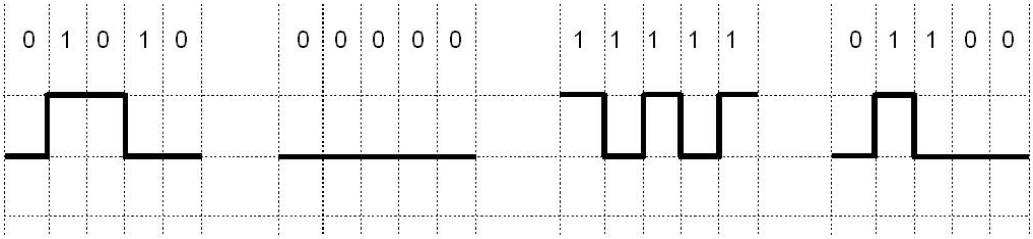


Рис. 3.29 Потенциальный код NRZI

Код NRZI обладает лучшей, по сравнению с NRZ, самосинхронизацией в том случае, если в кодируемой информации логических единиц больше, чем логических нулей. И не обеспечивает должной самосинхронизации при появлении длинных последовательностей логических нулей.

Данный метод используется на физическом уровне спецификации 100BASE-FX Fast Ethernet.

В *манчестерском коде* (Manchester code) для кодирования единиц и нулей используется перепад потенциала, то есть фронт импульса. Каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта: 1 кодируется перепадом от низкого уровня сигнала к высокому, 0 – обратным перепадом (по стандарту IEEE 802.3). Этот перепад используется для синхронизации между передатчиком и приемником.

В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей подряд.

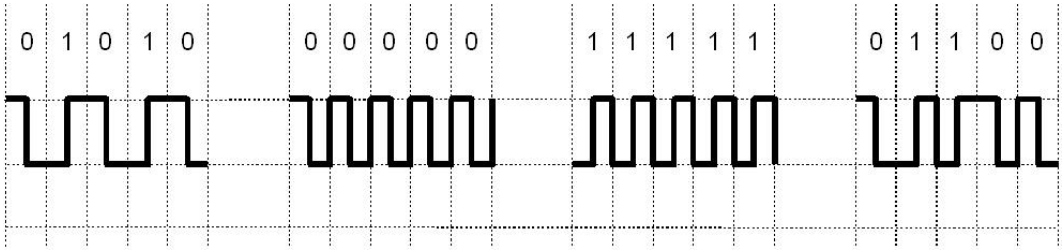


Рис. 3.30 Манчестерский код

Ширина спектра при манчестерском кодировании в два раза шире, чем при NRZ-кодировании. Данный метод используется на физическом уровне спецификаций Ethernet 10 Мбит/с (10BASE5, 10BASE2, 10BASE-T, 10BASE-F) .

Код трехуровневой передачи MLT-3 использует три уровня сигнала: +1, 0 и -1.

1 кодируется переходом с одного уровня сигнала на другой. При передаче 0 сигнал не меняется.

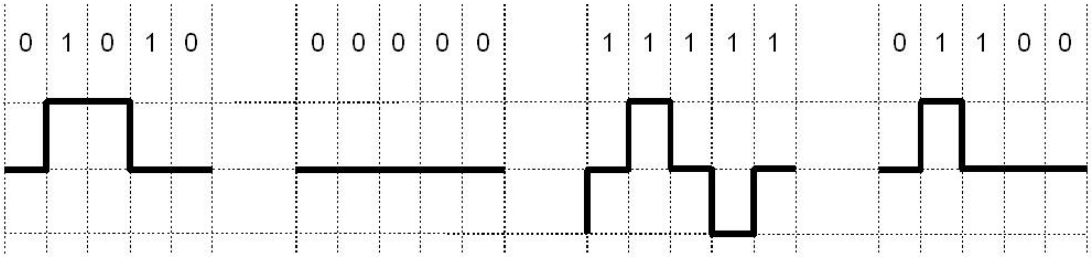


Рис. 3.31 Код MLT-3

Недостатком данного метода является отсутствие должной синхронизации при появлении длинных последовательностей логических нулей. Код MLT-3 используется на физическом уровне спецификации 100BASE-TX Fast Ethernet совместно с методом логического кодирования 4B/5B.

В *пятиуровневом коде PAM-5* используется 5 уровней амплитуды сигнала и двухбитовое кодирование. Четыре из них используются для кодирования информационных битов, а пятый предназначен для коррекции ошибок. На наборе из четырех фиксированных уровней одним дискретным состоянием сигнала можно закодировать сразу два информационных бита, поскольку комбинация из двух бит имеет четыре возможные комбинации (так называемые дибиты) — 00, 01, 10 и 11.

Переход к дибитам позволяет в два раза повысить битовую скорость по сравнению с NRZI, например. Недостатком этого метода является наличие постоянной составляющей при передаче длинной последовательности одинаковых пар и бит. Также требуется большая мощность передатчика, чтобы приемник мог четко различать уровни на фоне помех.

PAM-5 используется на физическом уровне спецификации 1000BASE-T Gigabit Ethernet. Спецификация 10GBASE-T 10 Gigabit Ethernet использует THP-версию (Tomlinson-Harashima precoded) кодирования PAM с 16 дискретными уровнями.

3.5.4.2 Логическое кодирование

Логическое кодирование, выполняемое до физического кодирования, позволяет бороться с недостатками потенциальных кодов типа NRZ, NRZI или MLT-3. Логическое кодирование подразумевает замену битов исходной информации новой последовательностью битов, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, в частности, возможностью для приемной стороны обнаруживать ошибки в принятых данных.

Также логическое кодирование позволяет исключить длинные последовательности нулей и единиц, приводящие к потере синхронизации, обеспечить распознавание границ кадра и особых состояний в непрерывном битовом потоке и улучшить спектральные характеристики сигнала.

Логическое кодирование преобразует поток битов сформированного кадра MAC-подуровня канального уровня в последовательность символов, подлежащих физическому кодированию для передачи по линии связи.

В основном для логического кодирования применяются два метода:

- избыточные коды;
- скрэмблирование.

Избыточное кодирование основано на разбиении исходной последовательности битов на участки одинаковой длины – символы. Затем каждый символ заменяется (как правило, табличным способом) на новый, имеющий большее количество битов.

Логический код 4B/5B заменяет каждые 4 бита входного потока (исходный символ) на 5-битовый выходной символ (таблица 3.1). В исходной последовательности из четырех бит существует 16 различных битовых комбинаций нулей и единиц, а в группе из пяти бит таких комбинаций уже 32. Поэтому в результирующем коде можно выбрать 16 таких комбинаций, которые не содержат большого количества нулей. При этом остальные не используемые комбинации можно считать запрещенными последовательностями. Таким образом, кроме улучшения самосинхронизирующих свойств исходного кода избыточное кодирование позволяет приемнику распознавать ошибки, так как появление запрещенной последовательности бит свидетельствует о возникновении ошибки.

Таблица 3.1

Двоичный код 4B	Результирующий код 5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010

1101	11011
1110	11100
1111	11101

Код 4B/5B используется в технологиях 100BASE-FX и 100BASE-TX.

Логический код 8B/10B заменяет каждый 8-битовый исходный символ 10-битовым выходным символом. При этом в исходной последовательности содержится 256 различных комбинаций нулей и единиц, а в результирующей 1024. Таким образом, 256 комбинаций 8-битовых символов могут быть закодированы двумя различными способами. Код 8B/10B используется в технологиях Gigabit Ethernet: 1000BASE-SX, 1000BASE-LZ.

Логический код 64B/66B применяется в технологиях 10 Gigabit Ethernet: 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-LRM, 10GBASE-KR.

Скремблирование (scramble) заключается в побитовом преобразовании исходной последовательности нулей и единиц с помощью псевдослучайного битового потока с целью улучшения спектральных характеристик и самосинхронизирующих свойств результирующей последовательности битов. Скремблирование осуществляется путем побитовой операции исключающего ИЛИ (XOR) исходной последовательности с псевдослучайной последовательностью. На стороне приемника исходный поток восстанавливается с помощью *дескремблера*.

С аппаратной точки зрения скремблер состоит из нескольких логических элементов XOR и сдвигового регистра с обратными связями в качестве генератора псевдослучайного битового потока.

Различные алгоритмы скремблирования отличаются количеством слагаемых и величиной сдвига между слагаемыми.

Достоинством скремблирования является отсутствие избыточных кодов, а недостатком – необходимость реализации на узлах связи алгоритма скремблирования/дескремблирования, что связано с дополнительными затратами.

3.6 Стандарты кабелей

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

Сегодня наиболее употребительными стандартами в мировой практике являются следующие:

- Американский стандарт EIA/TIA-568.
- Международный стандарт ISO/IEC 11801.
- Европейский стандарт EN50173.

При стандартизации кабелей принят подход, независимый от протоколов. Это означает, что стандарт не оговаривает, для какого именно протокола предназначен тот или иной кабель. Стандарт описывает электрические, оптические и механические характеристики, которым должен удовлетворять кабель или разъем. Поэтому нужно знать какие типы стандартных кабелей поддерживают протоколы, например, Ethernet или FDDI.

Кабели можно разделить на две группы: электрические кабели и волоконно-оптические кабели. К электрическим кабелям относятся витая пара, коаксиальный и твинаксиальный кабель. К волоконно-оптическим кабелям относятся одномодовые и многомодовые оптические кабели.

3.6.1 Основные характеристики электрических кабелей

Основными параметрами электрических кабелей, представляющими практический интерес и нормируемыми действующими редакциями стандартов, являются:

- затухание (коэффициент затухания);
- перекрестные наводки на ближнем конце (NEXT) и дальнем конце (FEXT);
- импеданс (волновое сопротивление);
- активное сопротивление;
- емкость;
- диаметр или площадь сечения проводника.

Напомним, **затухание** сигнала – уменьшение мощности (амплитуды) сигнала при передаче между двумя точками. Оно является одним из основных параметров, учитываемых при проектировании канала связи и расчета максимальной длины кабеля. Затухание измеряется в децибелах на метр [Дб/м] и зависит от частоты сигнала.

Перекрестные наводки на ближнем конце (NEXT) и дальнем конце (FEXT) являются результатом интерференции сигналов, передаваемых по соседним парам проводников. Значения NEXT и FEXT зависят от частоты сигнала.

Перекрестные наводки на ближнем конце (NEXT) вычисляются на том конце кабеля, где находится передатчик как отношение мощности входного сигнала к мощности наведенного сигнала. Они измеряются в децибелах [Дб] для определенной частоты сигнала.

Чем *больше* абсолютное значение NEXT (по модулю, т.к. значение этого параметра отрицательное), тем *меньше* уровень наводок от соседних пар.

Т.к. при передаче на большие расстояния сигнал ослабевает, то перекрестные наводки на дальнем конце (FEXT) создают меньше наводок, чем NEXT. Отсюда можно сделать вывод, что NEXT является более важным параметром, чем FEXT, т.е. его значение в большей мере сказывается на качестве передачи сигналов.

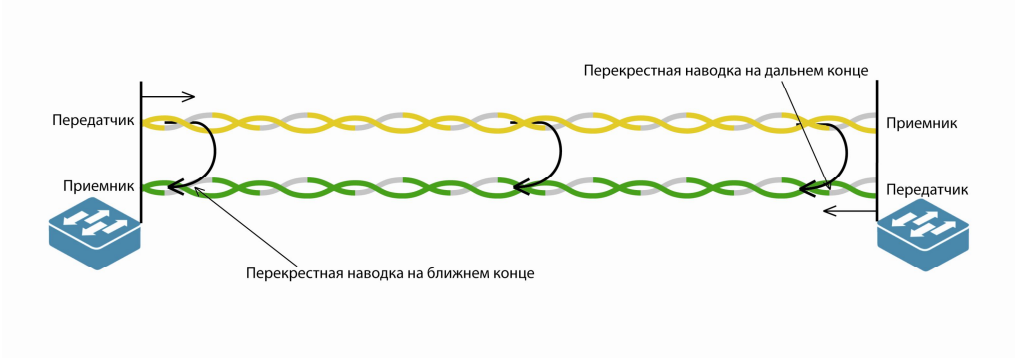


Рис. 3.32 Перекрестные наводки

Импеданс – это полное (активное и реактивное) сопротивление в электрической цепи, измеряется в Омах и является относительно постоянной величиной для кабельных систем (в области высоких частот (свыше 100 МГц) импеданс зависит от частоты). Резкие изменения импеданса по длине кабеля могут вызывать процессы внутреннего отражения, приводящие к возникновению стоячих волн. Из-за этого узлы, находящиеся вблизи источника стоячей волны не будут получать адресованные им данные.

Активное сопротивление – это сопротивление постоянному току в электрической цепи. В отличие от импеданса активное сопротивление не зависит от частоты и возрастает с увеличением длины кабеля. Измеряется в Омах.

Емкость – это свойство металлических проводников накапливать электрическую энергию. Этот параметр является нежелательным. Чем меньше значение емкости в кабеле, тем лучше, т.к. высокое значение приводит к искажению сигнала и ограничивает полосу пропускания канала связи.

Диаметр или площадь сечения проводника. В европейских и международных стандартах диаметр проводника указывается в миллиметрах. В современных компьютерных

сетях для медных проводников принято использовать американскую систему маркирования AWG (American Wire Gauge, американский калибр проводов), которая вводит некоторые условные типы проводников, например: наиболее употребительные 22AWG, 24AWG, 26AWG. Чем меньше номер AWG, тем больше диаметр проводника и ниже его сопротивление.

3.6.2 Коаксиальный кабель

Коаксиальный кабель (Coaxial cable) – электрический кабель, состоящий из соосно-расположенных центрального проводника и экрана, и служащий для передачи высокочастотных сигналов. Он характеризуется высокой помехозащищенностью и малым затуханием сигналов.

Коаксиальный кабель содержит внутренний проводник, представляющий собой монолитный медный провод или скрученный провод.

Внутренний проводник окружает изолирующая пластиковая оболочка (диэлектрик), вокруг которой находится внешний проводник. Внешний проводник представляет собой фольгу, служащую экраном от электромагнитных помех покрытую медной оплеткой. Снаружи кабель защищен жесткой пластиковой трубкой, формирующей его внешнюю оболочку (Рис. 3.33).

Рис. 3.33 Коаксиальный кабель

В локальных сетях использовались два типа коаксиального кабеля – «тонкий» и «толстый».

«Толстый» кабель RG-8 и RG-11 с волновым сопротивлением 50 Ом разработан для сетей Ethernet 10BASE5. Он имеет хорошую помехозащищенность и небольшое затухание, благодаря чему его можно использовать для передачи данных на большие расстояния. Его диаметр около 12 мм, расстояние передачи до 500 м. Однако в отличие от «тонкого» он дороже, плохо гнется и требует более сложного монтажа.

«Тонкий» кабель RG-58 был разработан для сетей Ethernet 10BASE2. Он обладает меньшей помехозащищенностью по сравнению с «толстым», но более гибкий и дешевый. Диаметр кабеля составляет около 6 мм, волновое сопротивление 50 Ом и расстояние передачи до 185 м.

В настоящее время коаксиальный кабель (RG-59) используется в основном для передачи телевизионных сигналов.

Одной из разновидностей коаксиального кабеля является *твинаксиальный кабель* (Twinaxial cable).

Твинаксиальный кабель – это высококачественный электрический кабель, похожий по конструкции на коаксиальный кабель, но содержащий два внутренних проводника. Диаметр проводников кабеля лежит в диапазоне от 30 AWG до 24 AWG. Его волновое сопротивление 100 Ом.

Рис. 3.34 Твинаксиальный кабель

Изначально твинаксиальный кабель был разработан для применения в сетях Gigabit Ethernet спецификации 1000BASE-CX для передачи данных на короткие расстояния (до 25 м). В настоящее время он широко используется для передачи данных на небольшие расстояния в высокоскоростных сетях Ethernet спецификаций 10GBASE-CX4, 40GBASE-CR4 и 100GBASE-CR10.

Для достижения наилучших характеристик производительности рекомендуется, чтобы твинаксиальные кабели для сетей спецификаций 10GBASE-CX4, 40GBASE-CR4 и 100GBASE-CR10 имели заводскую терминацию. Для этих целей производители сетевого оборудования выпускают пассивные или активные кабельные сборки, которые состоят из твинаксиального кабеля (или нескольких твинаксиальных кабелей), к концам которого напрямую подключены трансиверы SFP+ и/или QSFP+ , разъемы InfiniBand.

Рис. 3.35 Пассивный твинаксиальный кабель для прямого подключения с трансиверами QSFP+ длиной 3 метра

3.6.3 Кабель на основе витой пары

Витая пара (*twisted pair*) – изолированные проводники, попарно скрученные между собой с необходимым числом раз на единицу длины и заключенные в пластиковую оболочку.

Как уже отмечалось, попарное скручивание проводов позволяет уменьшить воздействие перекрестных помех, так как электромагнитные волны, излучаемые каждым проводом, взаимно гасятся. Шаг скрутки для разных пар различен и определен в стандартах.

Витая пара самый распространенный тип кабеля в телефонии и локальных компьютерных сетях благодаря своей дешевизне и простоте установки.

Кабель, как правило, содержит несколько витых пар: обычно в пучке 2, 4, 6, 8, 25, 50 или 100 пар. Для локальных сетей чаще всего используются кабели с четырьмя парами.

Проводники в парах изготавливаются из меди. Они могут быть цельными (из одного провода) или скрученными (из множества тесно прилегающих друг к другу тонких проводков). Толщина проводников составляет от 0,4 до 0,6 мм в метрической системе и от 26 до 22AWG в американской системе AWG соответственно. В стандартных 4-х парных кабелях в основном используются проводники диаметром 0,51 мм (24AWG).

Проводники помещены в оболочку из поливинилхлорида (PVC), полипропилена (PP) или полиэтилена (PE). Особенно качественные кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрические потери, или тефлона, обеспечивающего широкий рабочий диапазон температур.

Существуют два основных типа кабелей на основе витой пары:

- неэкранированная витая пара (UTP, Unshielded Twisted Pair);
- экранированная витая пара (STP, Shielded Twisted Pair).

Как следует из названия, неэкранированный кабель не имеет дополнительного экрана, обеспечивающего защиту от электромагнитных наводок и несанкционированного подслушивания.

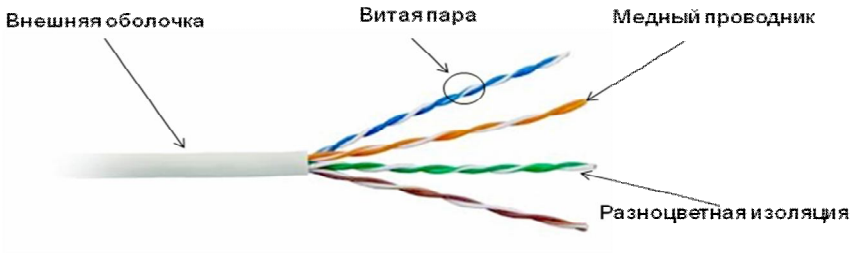


Рис. 3.36 Кабель UTP

Экранированные кабели имеют дополнительную защиту. В зависимости от используемой технологии существует несколько разновидностей кабелей на основе экранированной витой пары.

- экранированная витая пара (STP, Shielded Twisted Pair);
- защищенная витая пара (ScTP, Screened twisted pair);
- защищенная экранированная витая пара (SSTP, Screened Shielded Twisted Pair).

В экранированных кабелях STP (*U/FTP* (Unshielded/Foiled Twisted Pair) в терминологии ISO/IEC 11801) каждая пара скрученных медных проводов для уменьшения помех и взаимных наводок покрыта дополнительным защитным экраном из фольги.

Рис. 3.37 Кабель STP

В защищенной витой паре вокруг всех неэкранированных пар имеется один общий внешний экран. Существует несколько разновидностей этого кабеля. В кабеле F/UTP (Foiled/ Unshielded Twisted Pair в терминологии ISO/IEC 11801) экран сделан из фольги. В кабеле S/UTP (Shielded/Unshielded Twisted Pair в терминологии ISO/IEC 11801) экран сделан в виде проволочной оплетки. В кабеле SF/UTP (Shielded Foiled/Unshielded Twisted Pair в терминологии ISO/IEC 11801) имеется два внешних экрана из фольги и медной оплетки.

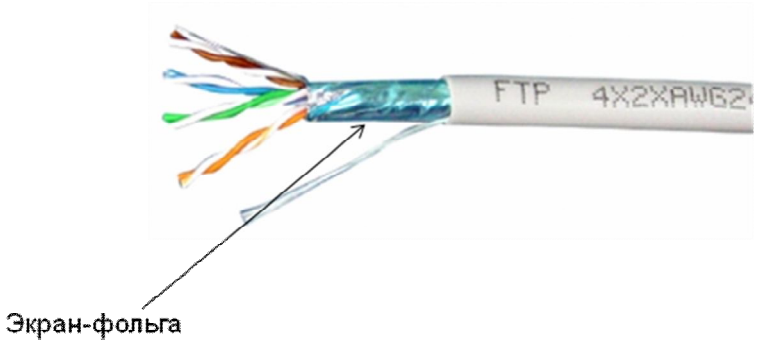


Рис. 3.38 Кабель F/UTP

Защищенная экранированная витая пара наилучшим образом защищает от электромагнитной интерференции и перекрестных наводок, т.к. является полностью экранированной. Имеется как отдельный экран вокруг каждой пары проводов, так и общий вокруг всех пар. Существует две разновидности этого кабеля: F/FTP и S/FTP в терминологии ISO/IEC 11801. В кабеле F/FTP (Foiled/ Foiled Twisted Pair) экраны вокруг пар и общий экран сделаны из фольги. В кабеле S/FTP (Shielded/Foiled Twisted Pair) экраны вокруг пар сделаны из фольги, общий экран – медная оплетка.

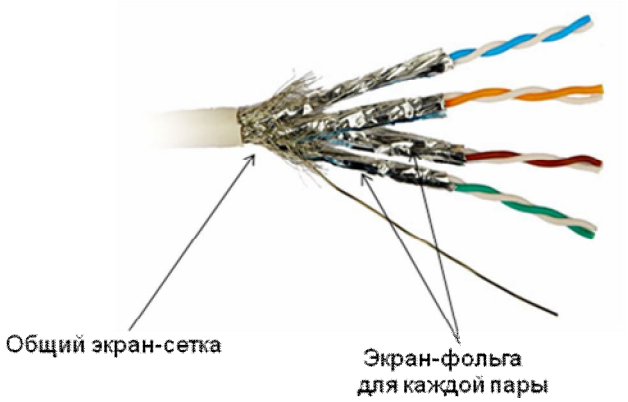


Рис. 3.39 Кабель S/FTP

Несмотря на то, что экранирование повышает помехозащищенность, оно делает экранированные кабели дороже и тяжелее по сравнению с неэкранированными. Помимо этого они требуют правильного заземления. Поэтому в локальных сетях, работающих на скоростях 100 или 1000 Мбит/с применяются в основном неэкранированные кабели. Однако стоит отметить, что для высокоскоростных сетей 10 Гбит/с, 40 Гбит/с, 100 Гбит/с стандарты определяют использование только экранированных кабелей.

Кабели на основе витой пары подразделяются на категории в зависимости от своей полосы пропускания. При этом, чем выше категория, тем большую полосу пропускания имеет кабель и тем лучше его характеристики.

Эти категории определяются в американском стандарте EIA/TIA-568 и в международном стандарте ISO/IEC 11801. В настоящее время определено 7 категорий кабеля, категория 8 находится в разработке. Описание категорий приведено в таблице 3.2.

Для неэкранированных кабелей в стандарте EIA/TIA-568 определены категории 3, 4, 5, 5e, 6, в стандарте ISO/IEC 11801 классы A, B, C, D, E. Для экранированных кабелей в стандарте EIA/TIA-568 определены категории 6a, 7, 7a, в стандарте ISO/IEC 11801 классы Ea, F, Fa .

Максимальное расстояние передачи по кабелю на основе витой пары равно 100 м, если не существует каких-либо ограничений соответствующего стандарта. Волновое

сопротивление у кабелей витой пары всех типов и категорий – 100 Ом. Остальные параметры, такие как затухание, NEXT, скорость распространения сигнала в линии и др. отличаются для различных категорий кабеля.

Таблица 3.2 Категории кабелей на основе витой пары

Название EIA/TIA-568	**Название ISO/IEC 11801**	**Полоса частот (МГц)**	**Приложения**	**Дополнения и комментарии**
-	Class A	до 100 КГц	xDSL	Телефонный кабель. Используется только для передачи голоса или данных при помощи аналогового или ADSL-модема.
-	Class B	до 1 МГц	ISDN, 1BASE5	Сейчас не используется
Category 3 (Cat. 3)	Class C	до 16 МГц	Token Ring 10BASE-T	2-х парный кабель UTP. Основное применение - передача голоса
Category 4 (Cat. 4)		до 20 МГц	Token Ring 10BASE-T 100BASE-T	4-х парный кабель UTP. В дальнейшем не рассматривается.
Category 5 (Cat. 5)	Class D	до 100 МГц	10BASE-T, 100BASE-TX (2 пары) 1000BASE-T (4 пары)	4-х парный кабель UTP. В дальнейшем не рассматривается.
Category 5e (Cat. 5e)		до 125 МГц	10BASE-T, 100BASE-TX (2 пары) 1000BASE-T (4 пары)	4-х парный кабель UTP. Наиболее распространен в современных сетях.
Category 6 (Cat. 6)	Class E	до 250 МГц	1000BASE-T 10GBASE-T	4-х парный кабель UTP. Ограничивает максимальное расстояние передачи для 10GBASE-T до 55 м.
Category 6a (Cat. 6a)	Class Ea	до 500 МГц	1000BASE-T 10GBASE-T	4-х парный кабель U/FTP, F/UTP.
Category 7 (Cat. 7)	Class F	до 600 МГц	1000BASE-T 10GBASE-T	4-х парный кабель F/FTP, S/FTP.
Category 7 (Cat. 7a)	Class Fa	До 1000 МГц	1000BASE-T 10GBASE-T	4-х парный кабель F/FTP, S/FTP.

Для подключения кабеля на основе витой пары к сетевым устройствам используется разъем 8P8C (8 Position 8 Contact). Данный разъем также называют RJ-45. Несмотря на ошибочность этого названия (настоящий RJ-45 – это разъем 8P2C), разъем 8P8C в силу внешнего сходства унаследовал от настоящего RJ-45 его название, которое и закрепилось за 8P8C. Далее мы тоже будем использовать термин RJ-45. В настоящее время этот разъем используется как для неэкранированной, так и для экранированной витой пары.

Рис. 3.40 Кабель UTP Cat. 5e с разъемами 8P8C (RJ-45)

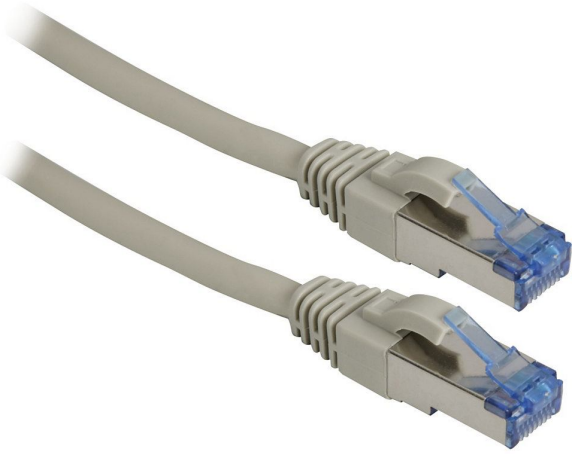


Рис. 3.41 Кабель U/FTP Cat. 6a с разъемами 8P8C (RJ-45)

Рассмотрим способы обжима разъема 8P8C на кабеле. Нумерация контактов разъема задается слева направо со стороны самих контактов (Рис. 3.42).

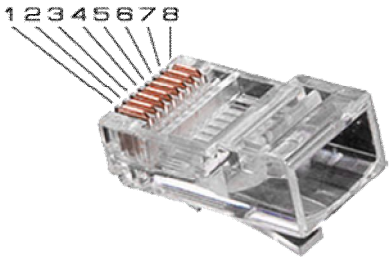


Рис. 3.42 Нумерация контактов RJ-45

Последовательность расположения пар проводников в разъеме определяется стандартами EIA/TIA-568A и EIA/TIA-568B (Рис. 3.43). Каждая пара в кабеле имеет свой цвет, при этом один проводник в паре окрашен полностью в этот цвет, а второй полосатый.

Стандарт EIA/TIA-568A определяет следующее соответствие проводников контактам разъема: 1 – бело-зеленый, 2 – зеленый, 3 – бело-оранжевый, 4 – синий, 5 – бело-синий, 6 – оранжевый, 7 – бело-коричневый, 8 – коричневый.

Стандарт EIA/TIA-568B определяет следующее соответствие проводников контактам разъема: 1 – бело-оранжевый, 2 – оранжевый, 3 – бело-зеленый, 4 – синий, 5 – бело-синий, 6 – зеленый, 7 – бело-коричневый, 8 – коричневый.

Отличаются две схемы друг от друга расположением оранжевой и зеленой пары, которые меняются местами.

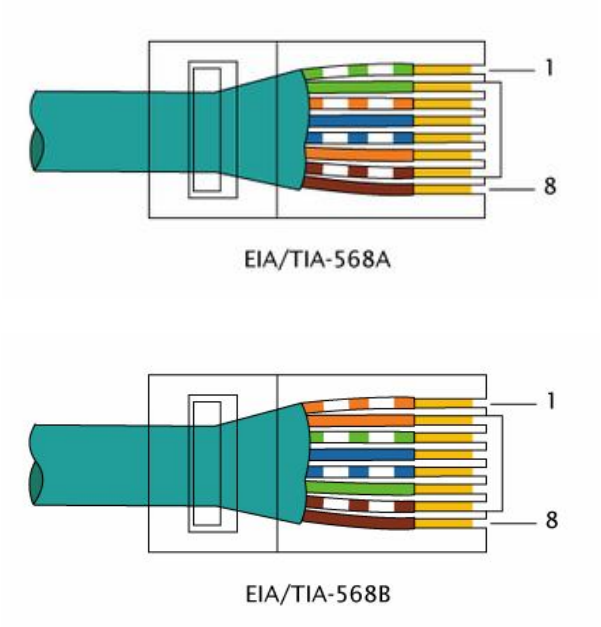


Рис. 3.43 Последовательность расположения проводников в разъеме

В зависимости от схемы расположения проводников в разъемах с двух сторон кабеля, кабели на основе витой пары делятся на:

- **Прямые** (straight through cable) – витая пара с обеих сторон обжата одинаково, без перекрещивания пар внутри кабеля.

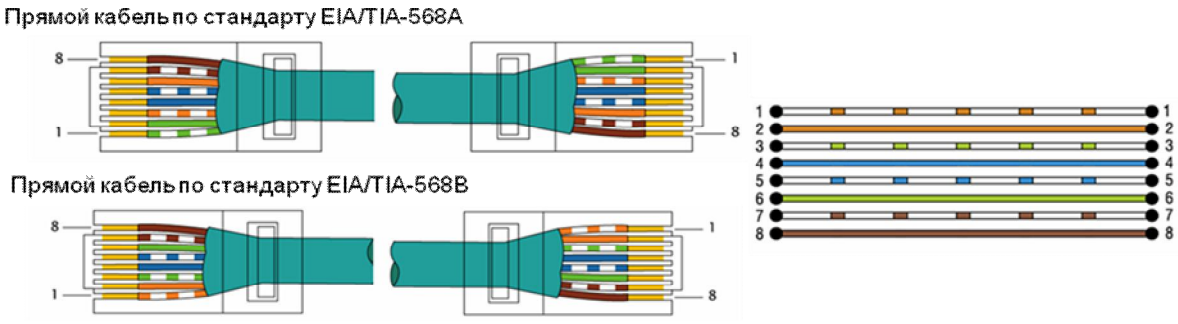


Рис. 3.44 Прямой кабель витая пара

- **Перекрестные** (crossover cable) – инвертированная разводка контактов с перекрещиванием пар внутри кабеля.

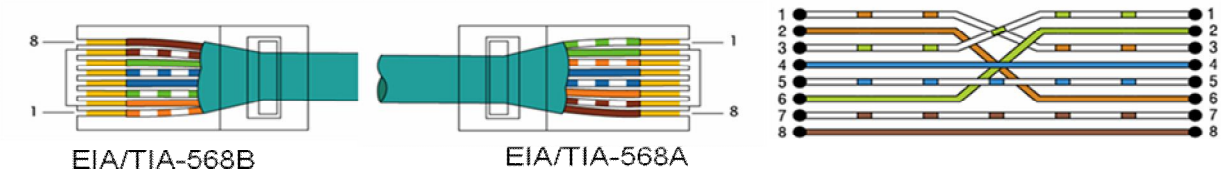


Рис. 3.45 Перекрестный кабель витая пара

Существует три типа интерфейсов (портов) Ethernet с разъемом 8P8C (RJ-45):

- **MDI** (Medium Dependent Interface) – зависимый от физической среды интерфейс.
- **MDI-X** (Medium Dependent Interface crossover) – зависимый от физической среды интерфейс, с перекрещиванием.
- **Auto MDI/MDI-X** – интерфейс с автоматическим определением конфигурации MDI или MDI-X.

Отличаются эти типы интерфейсов тем, что используют разные контакты для приема и передачи сигнала.

Как правило, MDI – это порт абонентского устройства (например, сетевой карты компьютера), в котором контакты 1 и 2 используются для передачи (Tx) данных, 3 и 6 – для приема (Rx).

Порт MDI-X используется в концентраторах, коммутаторах, маршрутизаторах. У него контакты 1 и 2 используются для приема (Rx) данных, 3 и 6 – для передачи (Tx).

Для соединения портов MDI–MDI-X (компьютер-коммутатор) применяют прямой кабель, а для соединений портов MDI–MDI (компьютер-компьютер) и MDIX–MDI-X — перекрестный.

Сегодня практически все производители сетевого оборудования оснащают Ethernet-порты поддержкой функции автоматического определения полярности Auto MDI/MDI-X, благодаря которой можно использовать любой кабель (как прямой, так и перекрестный) для соединения оборудования. Функция Auto MDI/MDI-X является частью стандарта IEEE 802.3 -2012.

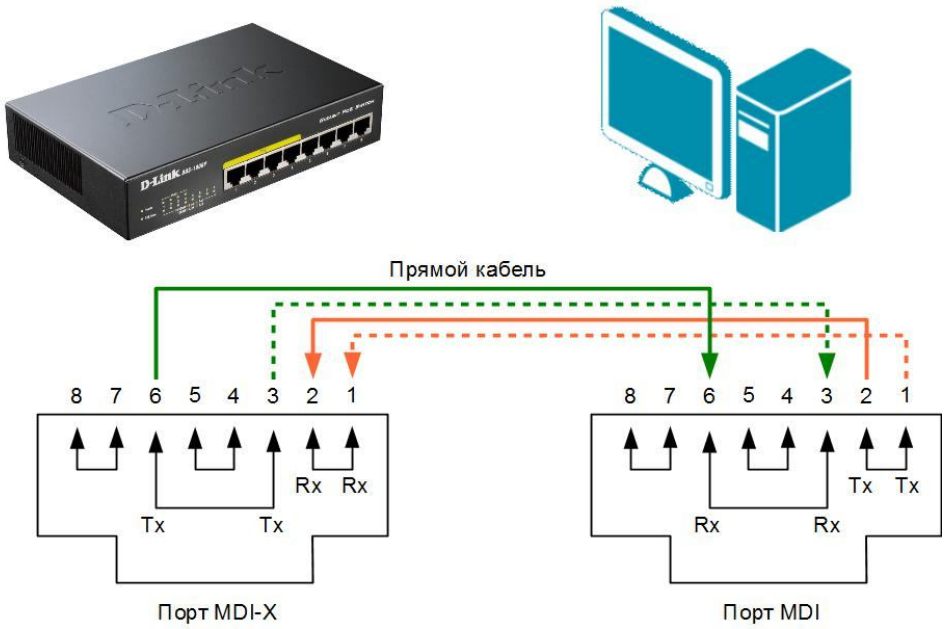


Рис. 3.46 Ethernet-порты MDI и MDI-X

Стоит отметить, что витая пара применяется не только для приема и передачи данных. В сети Ethernet она может использоваться для передачи электрической энергии удаленному устройству одновременно с данными. Эта технология называется Power over Ethernet (PoE) и описывается стандартами IEEE 802.3af-2003 и IEEE 802.3at-2009, которые в настоящее время являются частью стандарта IEEE 802.3 -2012. Технология PoE будет рассмотрена в главе 6.

3.6.4 Волоконно-оптический (оптоволоконный) кабель

Волоконно-оптический кабель, в отличие от коаксиального или кабеля на основе витой пары, передает не электрические, а световые сигналы. Особенности оптоволокна делают его идеальной средой для передачи значительного объема информации при больших скоростях на длинные расстояния. Преимущества оптического кабеля заключаются в высокой пропускной способности, высокой помехозащищенности, хорошей защите от несанкционированного доступа, малом диаметре, небольшом весе, отсутствии необходимости в заземлении и большой дальности передачи. К недостаткам оптических кабелей можно отнести сложность монтажа и высокую стоимость оптических сетевых устройств.

Волоконно-оптический кабель – это среда передачи, состоящая из оптических волокон, заключенных в защитную внешнюю оболочку.

Для обеспечения необходимой механической прочности и предотвращения больших механических напряжений в волоконно-оптическом кабеле вводятся специальные силовые элементы. Это могут быть стальная, медная, алюминиевая проволоки, арамидные нити и стеклопластиковые стержни. Силовые элементы размещаются в центре (для большей гибкости) и на периферии (для большей стойкости к ударам и растягивающим нагрузкам).

Оптическое волокно состоит из светопроводящего **сердечника (световодной жилы)** и окружающей его **оболочки** с разными коэффициентами преломления. Действие оптического волокна основано на эффекте полного внутреннего отражения света при переходе из среды с большим коэффициентом преломления в среду с меньшим коэффициентом преломления. Сердечник, по которому происходит распространение светового сигнала, изготавливается из оптически более плотного материала. Волокна различаются диаметром сердечника и оболочки, а также профилем показателя преломления сердечника. В обозначении волокна через дробь указываются значения диаметров сердечника и оболочки волокна. Важнейшими параметрами оптического волокна являются *затухание* и *дисперсия*.

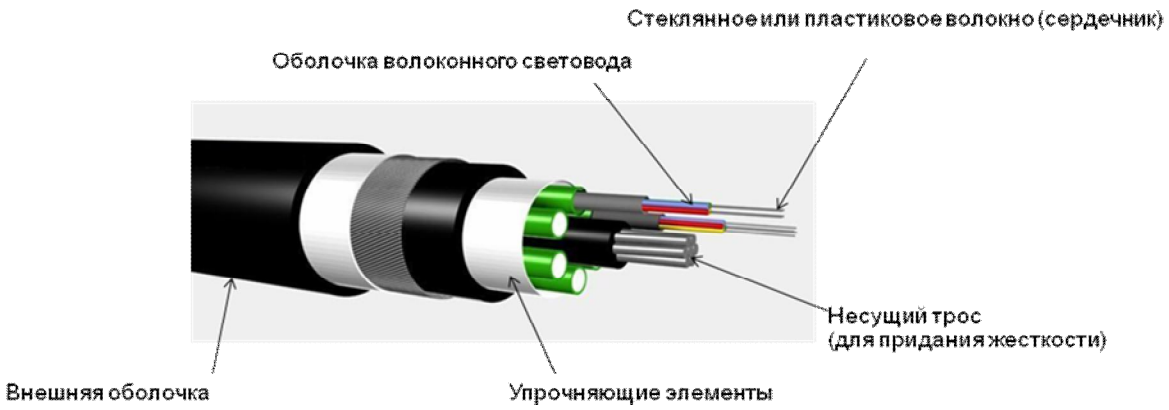


Рис. 3.47 Волоконно-оптический кабель

Оптические волокна делятся на две основные группы: *многомодовые* (Multi-Mode optical Fiber, MMF) и *одномодовые* (Single-Mode optical Fiber, SMF).

В стандартах определены два наиболее употребительных многомодовых волокна: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм – это диаметр сердечника, а 125 мкм – диаметр оболочки. Так как диаметры световодной жилы (50 и 62,5 мкм) на порядок выше длины световой волны, то по сердечнику одновременно распространяется множество электромагнитных волн различной модификации, которые называются *модами*. Входящие в световод под разными углами моды, многократно отражаясь от внутренней поверхности оболочки, проходят по сердечнику неодинаковый путь, вследствие чего достигают приемного конца линии в разное время. Происходит рассеяние мод во времени — *дисперсия*, в результате которой передаваемые световые импульсы постепенно расширяются. Это нежелательное явление ограничивает полосу пропускания света, которая обратно пропорциональна межмодовой дисперсии. В оптических волокнах полоса пропускания измеряется в мегагерцах на километр (МГц*км).

Многомодовые волокна изготавливают двух видов:

- со ступенчатым изменением показателя преломления;
- с плавным изменением показателя преломления.

Волокно со ступенчатым профилем состоит из сердечника с постоянным показателем преломления на всем сечении, окруженного оболочкой с другим постоянным на всем сечении показателем преломления. Из-за скачкообразного изменения показателя преломления свет отражается от поверхности сердечник/оболочка и проходит внутри сердечника. У волокон со ступенчатым профилем значительная дисперсия, что сильно ограничивает полосу пропускания.

У многомодового волокна с *плавным профилем* показатель преломления сердечника постепенно меняется на протяжении его сечения. В центре сердечника показатель преломления максимальный; он постепенно снижается к краям сердечника. Из-за плавного изменения показателя преломления световые лучи по мере продвижения по сердечнику искривляются (а не отражаются, как в волокнах со ступенчатым профилем) и образуют в волокне набор синусоидальных световых волн. Дисперсия волокон с плавным профилем по сравнению со ступенчатым профилем ниже, но она все еще значительна и имеет ограничивающий эффект на полосу пропускания.

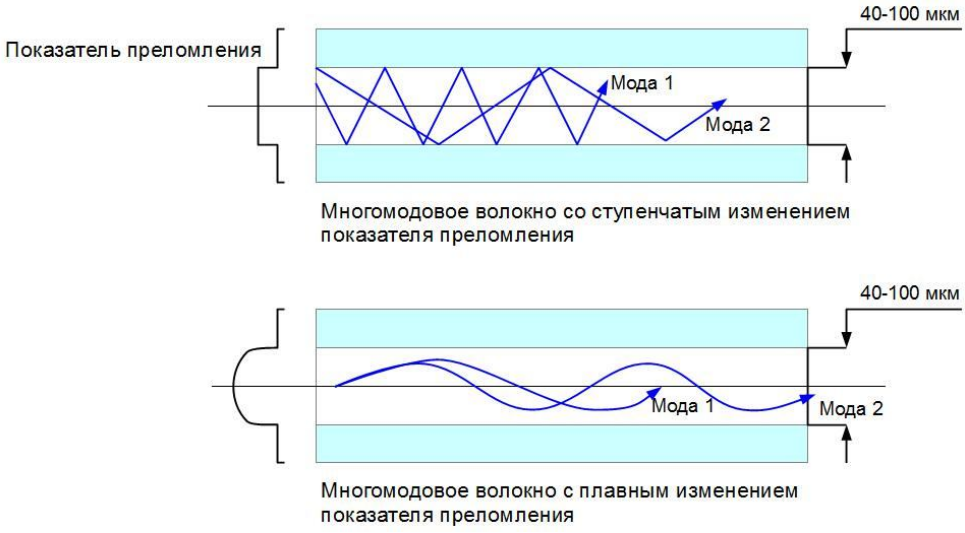


Рис. 3.48 Многомодовое оптоволокно

В качестве источников излучения света в MMF применяются светодиоды с длиной волны 850 нм и 1310 нм. Появление недорогих лазеров VCSEL (Vertical-Cavity Surface-Emitting Laser) позволило использоваться их в качестве источников света в многомодовых волокнах для создания высокоскоростных каналов связи до 10 Гбит/с. Максимальная длина многомодового волокна 2 км, поэтому применяется оно, как правило, в локальных сетях небольшой протяженности.

Одномодовое волокно представляет собой волокно со ступенчатым профилем показателя преломления. По сравнению с многомодовым одномодовое волокно имеет очень маленький диаметр сердечника (5-10 мкм, диаметр оболочки одномодового волокна 125 мкм), который сравним с длиной световой волны. В таком волокне распространяется только одна мода. Это устраняет межмодовую дисперсию и увеличивает пропускную способность одномодового волокна. Пропускная способность одномодового волокна превышает 10 Гбит/с.

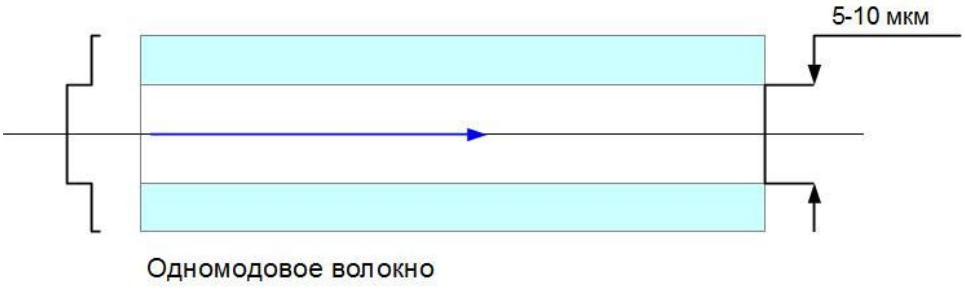


Рис. 3.49 Одномодовое оптоволокно

Максимальное расстояние передачи по одномодовому волокну может достигать 100 км и больше, благодаря чему оно используется, как правило, на протяженных линиях связи, в городских и региональных сетях.

В качестве источников излучения света в SMF применяются лазеры с длиной волны 1310 нм и 1550 нм. С точки зрения дисперсии наилучший режим распространения достигается на длине волны 1310 нм, но при этом наименьшее затухание сигнала получается на длине волны 1550 нм.

Для повышения эффективности оптического канала осуществляется его временное и волновое мультиплексирование (WDM). Большинство WDM-систем используют для работы одномодовые оптические кабели с диаметром волокна 9/125 мкм. Одномодовое волокно с ненулевой смещенной дисперсией NZDSF оптимизировано для передачи нескольких длин волн, что позволяет выполнять мультиплексирование WDM.

Классификацию оптических кабелей можно выполнять по:

- назначению;
- условиям применения;
- способу прокладки;
- конструктивным и технологическим особенностям;
- числу оптических волокон и электрических жил.

Волоконно-оптические кабели подразделяются по назначению на:

- магистральные (международные, междугородные);
- внутризоновые (соединительные, междугородные);
- местные (соединительные, распределительные, абонентские);
- внутриобъектовые (станционные, абонентские).

Согласно классификации Международного союза электросвязи (ITU-T), оптические кабели можно разделить на кабели для внешней и внутренней прокладки следующим образом:

- внешние кабели междугородные, межстанционные соединительные и распределительные (воздушный, проложенный в грунте, проложенный в канализации, проложенный в туннеле, подводный);
- внутренние кабели у абонента и на станции (внутри здания).

Защищенность от электромагнитных полей позволяет прокладывать оптические кабели вдоль линий электропередач и вдоль электрифицированных железных дорог (в полосе отчуждения).

Выбор кабеля для внешней прокладки в наибольшей степени зависит от условий, в которых планируется осуществляться его эксплуатация, от характера и силы внешних воздействий. Для внешних кабелей необходимо учитывать воздействие следующих факторов: температуры (усадка оболочки с вытягиванием сердечника, увеличение затухания под воздействием перепадов температуры, хрупкость, ломкость оболочки под воздействием низкой температуры); соленой воды (коррозия несущего троса или брони); дождя или горячего источника (коррозия несущего кабеля и внешней оболочки); постоянного тока (электролитическая коррозия); огня (пожароопасность); ветра, снега и льда (повреждение под давлением и раскачиванием ветра, под тяжестью снега и льда); водорода (увеличение потерь); а также возможность повреждения внешней оболочки кабеля грызунами, птицами и насекомыми.

Для кабелей внутренней прокладки наиболее важным фактором при выборе является его гибкость при прокладке по различным конструкциям здания и пожаробезопасность.

Международный стандарт ISO/IEC 11801 классифицирует различные виды многомодовых и одномодовых волокон для использования в помещениях пользователей. Он определяет четыре класса многомодовых волокон (от OM1 до OM4) и два класса одномодовых волокон (OS1 и OS2). Эти классы дифференцируются по затуханию и коэффициенту широкополосности (полосе пропускания).

Таблица 3.3 Классы многомодовых волокон ISO/IEC 11801

Категория	**Диаметр сердечника, нм**	**Минимальная модальная полоса пропускания, МГц*км**		
		Насыщенное возбуждение		**Лазерное возбуждение**
		850 нм	1310 нм	850 нм
OM1	50 или 62,5	200	500	н/о
OM2	50 или 62,5	200	500	н/о
OM3	50	1500	500	2000
OM4	50	3500	500	4700

Таблица 3.4 Классы одномодовых волокон ISO/IEC 11801

Длина волны, нм	**Максимальное затухание, дБ/км**	
	OS1	**OS2**
1310	1,0	0,4
1550	1,0	0,4

В стандарте оптические каналы различаются по классам (аналогично категориям кабелей на основе витой пары). OF-300, OF-500 и OF-2000 поддерживают приложения оптического класса на расстояниях до 300, 500 и 2000 м соответственно.

Таблица 3.5 Классы каналов ISO/IEC 11801

Затухание канала, дБ				
Класс канала	**MMF**		**SMF**	
	850 нм	**1310 нм**	**1310 нм**	**1550 нм**
OF-300	2,55	1,95	1,80	1,80
OF-500	3,25	2,25	2,00	2,00
OF-2000	8,50	4,50	3,50	3,50

Разъемов для волоконной оптики существует несколько десятков, но широкое применение нашли только некоторые из них. Это разъемы SC, LC, ST, FC и MT-RJ.

Разъемы типа SC (subscriber connector) широко используются как для одномодового, так и для многомодового волокна. Относятся к классу разъемов общего пользования. В разъеме используется механизм сочленения «push-pull», при котором соединитель

защелкивается. Могут 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). Позволяют достичь большой плотности монтажа на телекоммуникационной панели.

Рис. 3.50 Разъем SC

Разъем типа LC миниатюрный вариант SC. Он обеспечивает еще большую плотность монтажа. Помещен в прочный термостойкий пластмассовый корпус типа с механизмом «push-pull». Может использоваться для дуплексного соединения.

Рис. 3.51 Разъем LC

Разъем типа ST (straight tip connector) использует быстро выполняемое байонетное соединение, которое требует поворота разъема на четверть оборота для осуществления соединения/разъединения. Применяется как для одномодового, так и для многомодового кабеля. Самый дешевый разъем.

Рис. 3.52 Разъем ST

Разъемы типа FC аналогичны ST, но с резьбовой фиксацией. Ориентированы на применение с одномодовым кабелем, но могут быть использованы и для многомодового кабеля.

Рис. 3.53 Разъем FC

Разъем типа MT-RJ представляет собой миниатюрный дуплексный разъем.

Рис. 3.54 Разъем MT-RJ

3.6.5 Кабельные системы

Кабельная система представляет собой совокупность кабелей различных типов (оптических, на основе витой пары), кроссовых кабелей (патч-кордов), разъемов для кабелей, соединительных розеток, коммутационных или кроссовых панелей (патч-панелей), монтажных шкафов и телекоммуникационных стоек, предназначенных для подключения к компьютерной сети различных сетевых устройств.

Рис. 3.55 Патч-панель

Рис. 3.56 Телекоммуникационная стойка

Оборудование, используемое для организации компьютерной сети, можно разделить на два вида: *пассивное* и *активное*.

Компоненты кабельной системы представляют собой *пассивное сетевое оборудование*, сетевые устройства, которые они соединяют, являются *активным сетевым оборудование*.

Пассивное оборудование представляет собой сетевые устройства, не потребляющие электричества и не вносящие изменений в сигнал на информационном уровне. *Активным сетевым оборудованием* являются электронные и электронно-оптические устройства, обрабатывающие, формирующие, преобразующие и коммутирующие электрические, радио- и/или оптические сигналы. Для передачи и получения сигналов активное сетевое оборудование использует дополнительные источники энергии, т.е. для работы ему требуется электроэнергия.

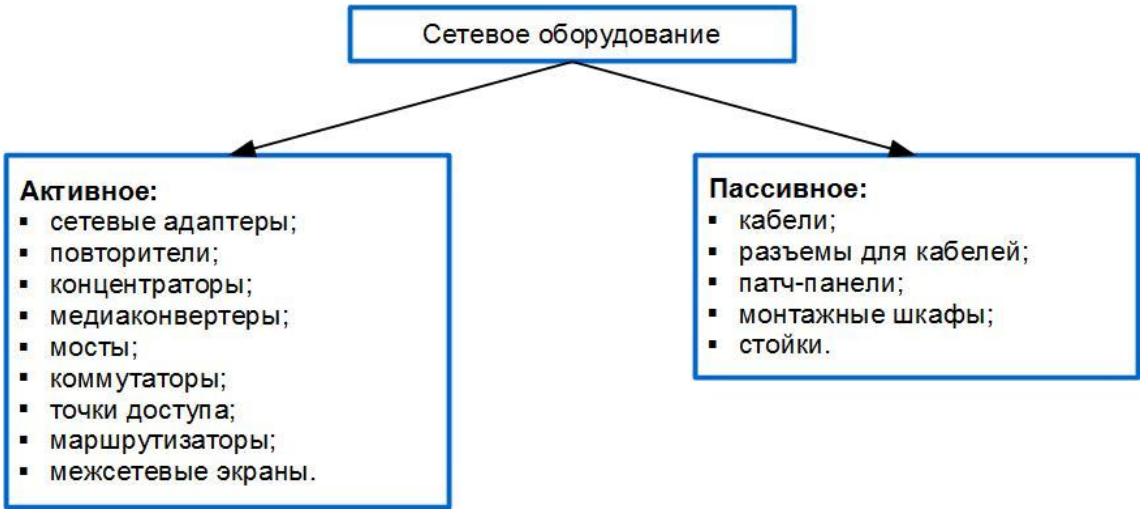


Рис. 3.57 Виды сетевого оборудования

3.6.6 Структурированные кабельные системы

Структурированной кабельной системой (СКС) называется кабельная система здания или группы зданий отвечающая требованиям стандартов. СКС определяют международные, европейские и национальные стандарты.

В настоящее время действуют три основных стандарта:

- TIA/EIA-568C Commercial Building Telecommunications Wiring Standard (американский стандарт);
- ISO/IEC 11801-2002 Information Technology. Generic cabling for customer premises (международный стандарт);
- CENELEC EN50173 Information Technology. Generic cabling systems (европейский стандарт).

В Российской Федерации введены в действие стандарты ГОСТ Р 53246-2008 и ГОСТ Р 53245-2008, которые основаны на международном стандарте ISO/IEC 11801.

Все стандарты определяют структуру СКС, рабочие параметры функциональных компонентов, принципы проектирования, правила монтажа, методику измерения, правила администрирования, требования телекоммуникационного заземления. Стоит отметить, что стандарты отличаются терминологией, перечнем функциональных компонентов СКС и количеством подсистем СКС.

Структурированные кабельные системы представляют собой универсальную кабельную инфраструктуру, обеспечивающую передачу сигналов всех типов: данные, речь и видео. Также к их достоинствам можно отнести возможность подключения любого сетевого оборудования и использования сетевых протоколов различных типов. Помимо этого они используют стандартные компоненты и материалы, позволяют комбинировать в одной сети кабели разных видов, обладают модульностью, возможностью внесения изменений и расширяемостью кабельной системы, а также обеспечивают длительный срок службы.

Простота администрирования достигается благодаря тому, что все компоненты СКС (порты, кабели, панели, шкафы и др.) промаркированы и документированы.

Рис. 3.58 Вариант установки и маркировки розеток

Недостатком СКС является то, что стандарты рекомендуют установку избыточного оборудования, что влечет существенные единовременные затраты, которые потом быстро окупаются.

Одной из важных процедур, позволяющих избежать проблем с работой приложений компьютерной сети, является тестирование и сертификация СКС. СКС может соответствовать стандартам, но не обеспечивать работу ряда приложений локальной сети по параметру интенсивности битовых ошибок (BER, Bit Error Rate). Тестирование позволяет обнаружить скрытые дефекты, которые приводят к сбоям и отказам.

Для диагностики СКС используется специальное оборудование:

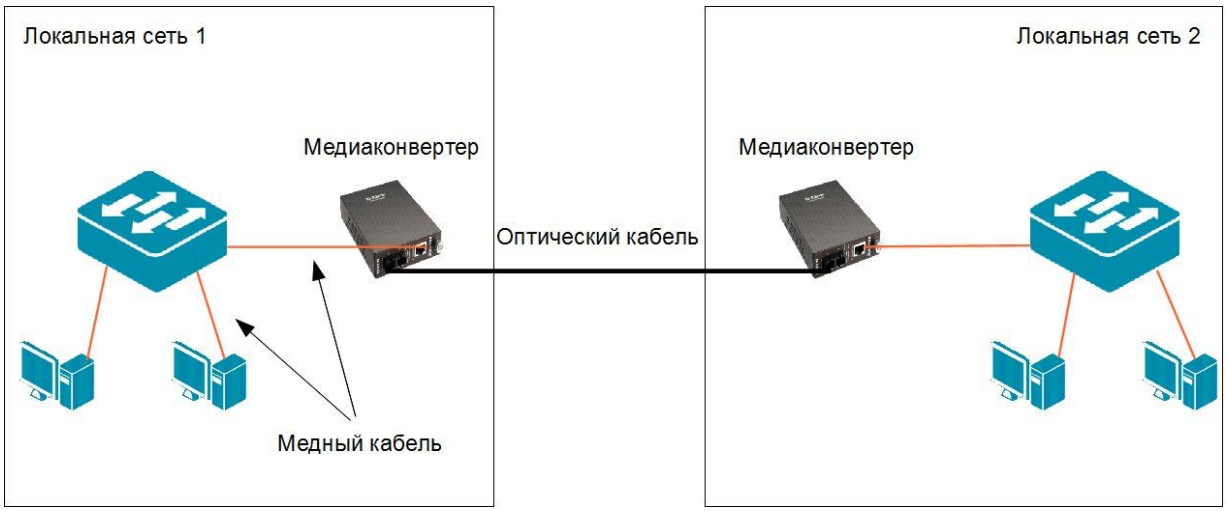
- **сетевые анализаторы** (не следует путать с анализаторами протоколов) – это эталонные измерительные устройства для диагностики и сертификации кабелей и кабельных систем в лабораторных условиях специально обученным персоналом;
- **кабельные сканеры** – это портативные устройства для сертификации кабельных систем, позволяющие определять длину кабеля, электромагнитные характеристики (NEXT, затухание, импеданс), схемы разводки кабеля, уровень электромагнитных полей, отношение сигнал/шум;
- **кабельные тестеры** – это портативные устройства, которые позволяют проводить диагностику кабельных систем на правильность их монтажа и обнаруживать неисправности в кабеле.

3.6.7 Медиаконвертеры

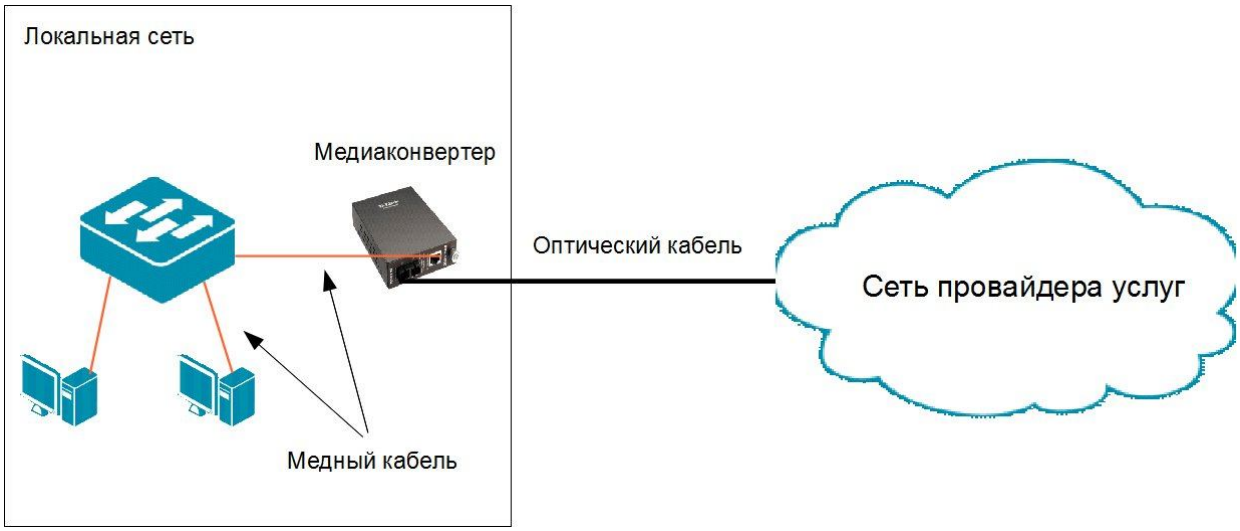
При расширении или модернизации существующей сети, а также при организации абонентского доступа в Интернет могут возникнуть проблемы связанные с несовпадением типов сред передачи и сигналов. Например, при подключении оборудования с «медным» интерфейсом к волоконно-оптическим каналам связи или наоборот. Чтобы избежать значительных финансовых затрат на проведение новых коммуникаций или покупку дорогостоящего оборудования, эти проблемы в сетях могут решаться с помощью *медиаконвертеров*.

Медиаконвертер *(Mediaconverter)* или **преобразователь среды передачи** — это устройство, преобразующее среду распространения сигнала из одного типа в другой.

Под средой распространения сигнала, которую преобразует медиаконвертер, в компьютерных сетях понимают медные и оптические кабели. Другими словами он является связующим звеном между двумя физическими средами – медным и оптическим кабелем.



а) Объединение двух локальных сетей.



б) Подключение к сети провайдера услуг.

Рис. 3.59 Использование медиаконвертера в сети

Для подключения к медному кабелю медиаконвертеры оборудованы интерфейсом RJ-45. Для подключения к оптическому кабелю используется, как правило, интерфейс SC.

Рис. 3.60 Медиаконвертер DMC-F02SC с оптическим интерфейсом SC

Для большей гибкости в выборе типа оптического подключения вместо оптического интерфейса медиаконвертер может быть оборудования слотом для установки сменных интерфейсным модулей, как правило, SFP.

Рис. 3.61 Медиаконвертер DMC-G01L со слотом SFP

Медиаконвертеры, производимые D-Link, могут работать как автономные устройства (помещены в собственный корпус и оснащены блоком питания), так и в составе шасси. Шасси с медиаконвертерами удобно использовать в сетях операторов связи, когда требуется организовать абонентский доступ в Интернет. В шасси можно установить до 16 медиаконвертеров, организовать резервирование их питания, а также осуществлять их мониторинг в режиме реального времени. Само шасси можно поместить в телекоммуникационную стойку.

Рис. 3.62 Шасси для медиаконвертеров DMC-1000

Традиционно медиаконвертеры рассматриваются как устройства, работающие на физическом уровне модели OSI. Однако развитие технологий привело к появлению медиаконвертеров с интеллектуальными функциями, работающих на канальном уровне.

Современные медиаконвертеры могут преобразовывать не только среду передачи, но и согласовывать скорость и режим передачи данных. Согласование скорости и режима работы (дуплексный/полудуплексный) выполняется портом для витой пары, который как правило является интерфейсом Ethernet. Помимо этого у медиаконвертеров появились другие сервисные функции. Например, они могут управлять потоком данных (flow control), выполнять мониторинг оптического и медного портов с целью обнаружения отсутствия сигнала (функция Link Pass Through), выполнять функции коммутации кадров в режиме Store-and-forward.

3.7 Электрическая проводка

Локальную сеть можно построить, используя обычные электрические провода 220 В, т.е. домашнюю электропроводку и передавать по ней голос или данные. Для этого аналоговый сигнал накладывается поверх стандартного переменного тока частотой 50 Гц. Причиной использования электропроводки в качестве среды передачи стало распространение домашних сетей.

Компьютер, а то и два есть практически в каждом доме. Бурно развивается технология *Smart TV* (умное телевидение) – технология интеграции Интернета и цифровых интерактивных сервисов в современные телевизоры, ресиверы цифрового телевидения, Blu-ray-проигрыватели, игровые консоли и аналогичные им устройства. По дому можно протянуть десятки метров кабелей, соединив между собой все компьютеры, принтеры, телевизоры и прочие сетевые устройства. Но тогда каждое устройство будет стационарно расположено в помещении. Перенести компьютер или телевизор, – значит переложить сетевой кабель. Можно установить дома беспроводную сеть Wi-Fi, но могут возникнуть проблемы с проникновением сигнала через стены и перекрытия.

Существует и другой способ – использовать уже существующие электрические провода и розетки, установленные в стенах. Электрические розетки есть в каждой комнате каждой квартиры каждого дома. Единственное, что для этого потребуется – соответствующие *адаптеры PowerLine*, которые подключаются непосредственно к розетке.

Адаптеры PowerLine бывают проводные и беспроводные, с поддержкой интерфейса Wi-Fi.

Помимо перечисленного, электропроводку можно использовать для реализации идеи «умного дома», где вся бытовая электроника связана в единую сеть с возможностью централизованного управления.

Применение технологии PowerLine не ограничивается только домом, она может применяться и в небольших офисах (до 15 компьютеров), где основными требованиями к сети являются простота реализации и расширяемости, мобильность устройств. При этом как вся офисная сеть, так и отдельные ее сегменты могут быть построены с помощью PowerLine-адаптеров. Часто встречается ситуация, когда необходимо включить в уже существующую сеть удаленный компьютер или сетевой принтер, расположенный в другой комнате или в другом конце здания. Такая проблема также легко решается с помощью PowerLine-адаптеров.

Технология PowerLine может быть использована в автоматизации технологических процессов, связывая блоки автоматизации по электропроводам или другим видам проводов.

Рис. 3.63 Адаптеры PowerLine AV DHP-309AV

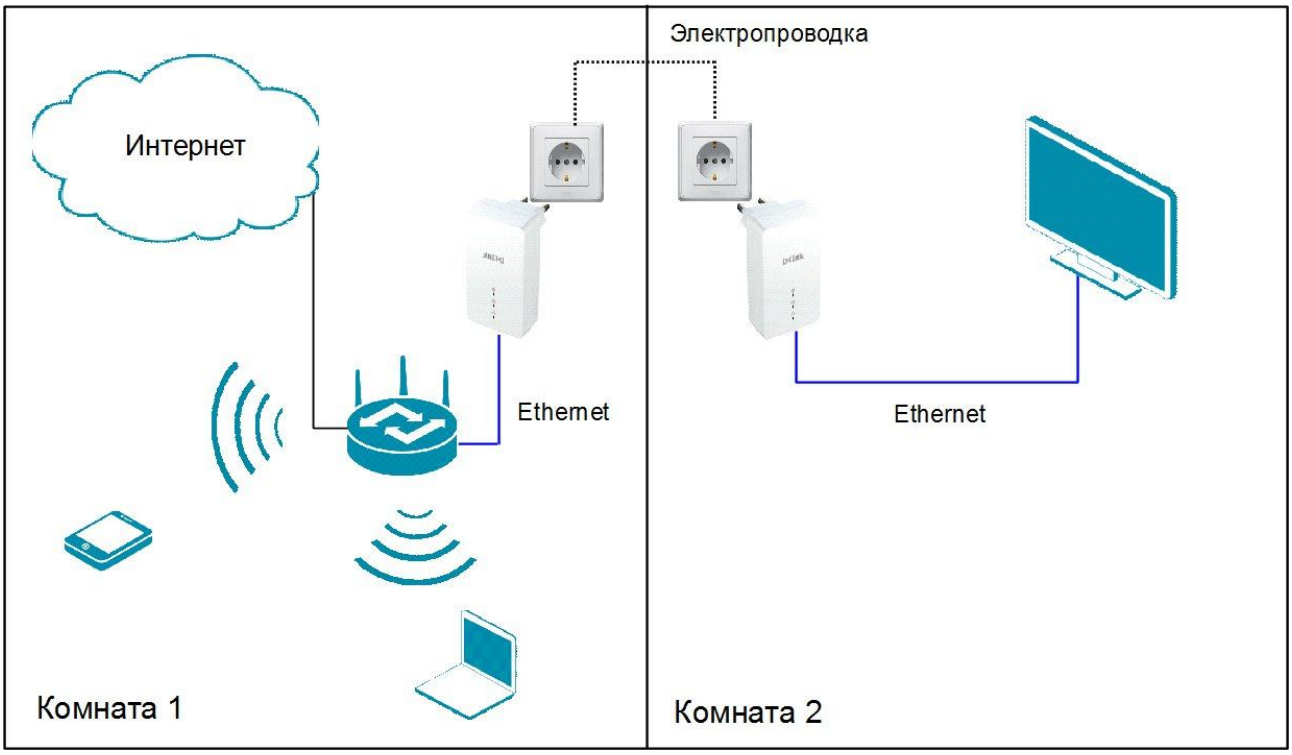


Рис. 3.64 Расширение домашней сети с помощью технологии PowerLine

В настоящее время большинство конечных подключений осуществляется посредством прокладки кабеля от высокоскоростной линии до квартиры или офиса пользователя. Это наиболее дешевое и надежное решение, но если прокладка кабеля невозможна, то можно воспользоваться имеющейся в каждом здании системой силовых электрических коммуникаций. При этом любая электрическая розетка в здании может стать точкой выхода в Интернет. От пользователя требуется только наличие PowerLine-модема или маршрутизатора для связи с аналогичным устройством, установленным, как правило, в электрощитовой здания и подключенным к высокоскоростному каналу.

Передача данных по электрическим сетям (PowerLine Communication, PLC) также является идеальным решением последней мили в коттеджных поселках и в малоэтажной застройке, в связи с тем, что организация альтернативных каналов связи стоит дороже, чем готовая электропроводка.

Для создания единого стандарта передачи данных по электрическим сетям был создан альянс HomePlug PowerLine Alliance. Стандарт IEEE 1901-2010, в основе которого лежит спецификация HomePlug AV определяет высокоскоростную широкополосную передачу данных (до 500 Мбит/с) через электропроводку. Для передачи данных в стандарте определена полоса пропускания 1,8 – 30 МГц.

Любая технология передачи данных нуждается в адаптации к физической среде, поэтому ей нужны средства обнаружения и устранения ошибок и конфликтов при совместном использовании. При передаче сигнала по электрическим сетям приходится сталкиваться со многими проблемами, основными из которых являются искажение сигнала вследствие многолучевого распространения, затухание сигнала, импульсные помехи и межсимвольная интерференция.

Структура электросетей и, в частности, домашней электропроводки изначально не предназначалась для высокоскоростной передачи данных. В ней содержится множество электрических розеток, переключателей, разделительных трансформаторов и устройств защиты от перегрузки по току (предохранителей). Путь прохождения высокочастотного сигнала от передающего устройства к приемному зависит от многих факторов. В первую очередь, от топологии электросети (т.е. пути прокладки проводов в конкретной квартире или офисе). Во-первых, из-за разветвленности сети всегда существует несколько путей

распространения сигнала от источника к приемнику. Во-вторых, из-за наличия многочисленных неоднородностей в электрической сети в точку приема поступает не только прямой сигнал, но и многочисленные задержанные во времени отраженные сигналы (явление многолучевого отражения). При распространении сигнала по линии электросети вследствие затухания происходит снижение его уровня. Еще одной причиной, вызывающей существенное уменьшение сигнала, является наличие в структуре реальной электросети коммутационных элементов. Как правило, электрическая цепь содержит разного рода рубильники, выключатели и низкочастотные (50 Гц) трансформаторы, которые являются основным препятствием для прохождения высокочастотного сигнала. Источниками помех в обычных квартирах и помещениях офисов могут быть стандартные устройства для зарядки аккумуляторов мобильных телефонов, регуляторы яркости свечения галогенных ламп, а также другие бытовые приборы.

Основной технологией PowerLine на физическом уровне является мультиплексирование с ортогональным частотным разделением (OFDM) – частотное разделение сигнала, при котором высокоскоростной поток данных разбивается на несколько относительно низкоскоростных потоков, каждый из которых передается на отдельной поднесущей частоте с последующим их объединением в один сигнал.

Использование OFDM позволяет повысить помехоустойчивость передачи за счет адаптации к параметрам физической среды передачи. Однако из-за пропадания и искажения сигнала в линии вследствие многолучевых отражений, большого уровня помех, а также коротких по длительности, но мощных импульсных помех в электросети, являющихся причиной ошибок в пакетах данных, одной только OFDM-модуляции недостаточно для надежной передачи информации. Чтобы обеспечить приемлемую достоверность данных, необходимо принять и другие меры.

Одним из методов решения данной проблемы является использование помехоустойчивого кодирование битовых потоков перед их модуляцией и последующей передачей в сеть. Суть помехоустойчивого кодирования состоит в добавлении в исходный информационный поток избыточных битов, которые используются декодером на приемном конце для обнаружения и исправления ошибок.

Сеть, построенная на электропроводке – это сеть с разделяемой средой передачи. Для решения проблем, связанных с множественным доступом к среде передачи используются методы CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) и TDMA (Time Division Multiple Access). Метод CSMA/CA похож на метод, используемый на подуровне MAC стандарта IEEE 802.11. Метод TDMA используется для обеспечения качества обслуживания (QoS).

Для обеспечения защиты от несанкционированного доступа используется 128-битное шифрование AES.

Скорость передачи данных по сети PowerLine теоретически может достигать 500 Мбит/с. Однако на пропускную способность сети сильно влияют качество проводки (материал, сечение, наличие скруток), работа других электрических приборов, количество самих PowerLine-адаптеров в сети (пропускная способность сети делится между всеми ее участниками, поэтому рекомендуется объединять в сеть не более 15 устройств), характер и объем трафика. Максимальное расстояние, на котором должны располагаться друг от друга устройства PowerLine – не более 100 м при использовании в локальной сети и не более 1500 м – при доступе в Интернет.

В 2012 г. появилась спецификация HomePlug AV2. Оборудование этой спецификации обратно совместимо с оборудованием спецификации HomePlug AV и стандарта IEEE 1901-2010. По сравнению с HomePlug AV в спецификации HomePlug AV2 расширена полоса пропускания доступная для передачи данных с 30 до 86 МГц и добавлена поддержка технологии MIMO (Multiple Input Multiple Output), что позволяет значительно увеличить пропускную способность. Также поддерживается режим сохранения энергии.

3.8 Беспроводная среда передачи

В отличие от проводных сетей, где сигналы передаются по твердым проводникам, например, медным витым парам или оптическим волокнам, в беспроводных сетях физической средой передачи является атмосфера и открытый космос. В кабельных средах передача всегда направленная, а беспроводные физические среды не могут направлять сигналы в определенном направлении. Для построения беспроводной линии связи каждый узел оснащается антенной. Антенну можно определить как проводник (или систему проводников), используемый для излучения и улавливания электромагнитных волн из пространства. Для передачи сигнала радиочастотные электрические импульсы передатчика с помощью антенны преобразуются в электромагнитную энергию, которая излучается в окружающее пространство (атмосферу, космос, воду). При получении сигнала энергия электромагнитных волн, поступающих на антенну, преобразуется в радиочастотные электрические импульсы, после чего попадает на приемник. Как правило, при двухсторонней связи одна и таже антенна может быть использована как для приема, так и для передачи сигнала. Это связано с тем, что характеристики антенны одинаковы для процесса получения и передачи электромагнитной энергии.

Электромагнитные волны – это распространяющееся в пространстве возмущение (изменение) электромагнитного поля.

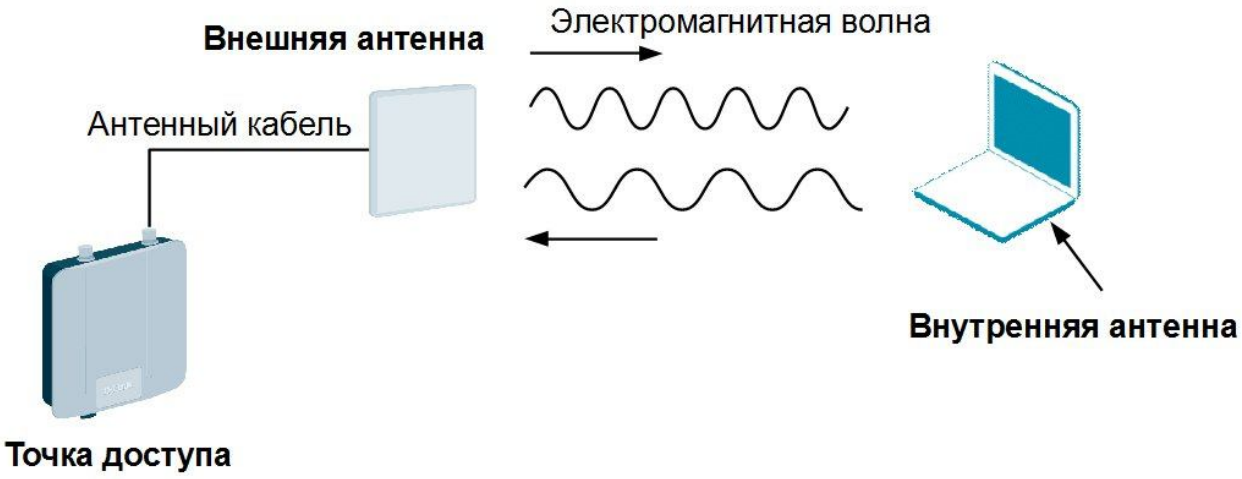


Рис. 3.65 Беспроводная линия связи

Направление распространения волн зависит от типа используемой антенны. Антенны в общем случае можно классифицировать как всенаправленные и направленные. При направленной передаче передающая антенна излучает сфокусированный электромагнитный луч, поэтому передающая и приемная антенны должны быть тщательно нацелены. При ненаправленной передаче (с использованием всенаправленной антенны) передаваемый сигнал распространяется во всех направлениях и может быть принят множеством антенн.

Наиболее распространенным способом определения направленности антенны является *диаграмма направленности*, которая представляет собой зависимость излучающих свойств антенны от пространственных координат. Один из наиболее простых типов диаграммы направленности соответствует идеальному случаю так называемой изотропной антенны. *Изотропный излучатель* – воображаемая антенна, излучающая во все направления электромагнитную энергию одинаковой интенсивности.

Диаграмма направленности для изотропной антенны представляет собой сферу, центр которой совпадает с положением антенны (Рис. 3.66а). Расстояние от антенны до любой точки диаграммы направленности прямо пропорционально энергии, которая была излучена антенной в данном направлении. На Рис. 3.66б представлен еще один идеализированный случай — направленная антенна с одним выделенным направлением излучения (вдоль горизонтальной оси).

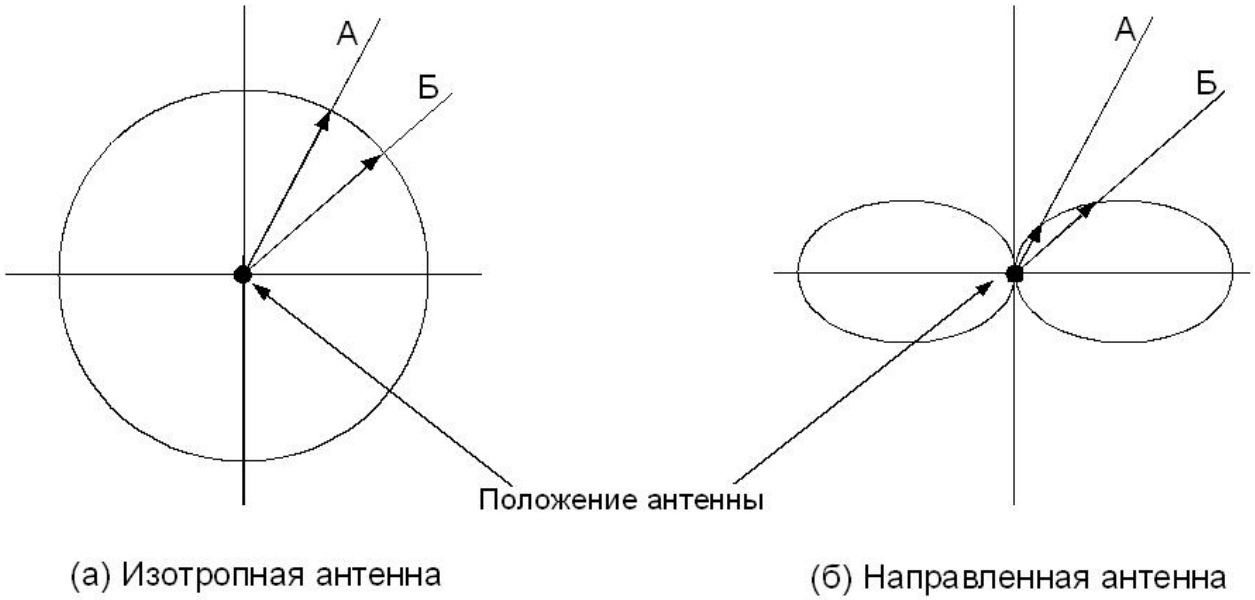


Рис. 3.66 Диаграммы направленности идеализированных антенн

Размер диаграммы направленности может быть произвольным. Важно лишь, чтобы в каждом направлении были соблюдены пропорции. Чтобы на основе относительного расстояния определить приведенную мощность в заданном направлении, от точки размещения антенны до пересечения с диаграммой направленности проводят прямую линию под соответствующим углом наклона. На Рис. 3.66 для двух идеализированных антенн сравниваются два угла передачи сигнала (А и Б). Изотропной антенне соответствует всенаправленная круговая диаграмма; векторы А и Б равны по величине. Вибратору Герца соответствует направленная диаграмма, на которой вектор Б длиннее вектора А, т.е. в направлении Б излучаемая мощность больше, чем в направлении А. Относительная длина векторов прямо пропорциональны мощности сигнала, излученной в соответствующем направлении.

Как правило, диаграммы направленности антенн представляются как два двухмерных поперечных сечения трехмерной диаграммы: горизонтальное и вертикальное сечения. В этом случае диаграмма направленности представляет собой замкнутую линию в полярной системе координат, построенную таким образом, чтобы расстояние от антенны (центр диаграммы) до любой точки диаграммы направленности было бы прямо пропорционально энергии, излучаемой антенной в данном направлении.

Направление максимального излучения называется главным лепестком антенны. Остальные лепестки диаграммы направленности антенны являются побочными, а лепесток излучения в сторону, обратную главному направлению, называется задним лепестком диаграммы направленности антенны.

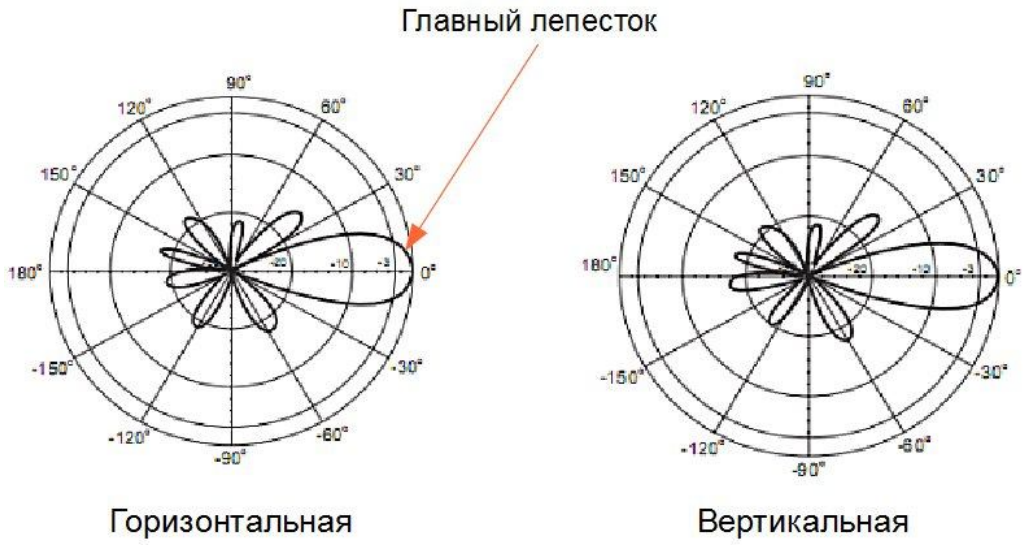


Рис. 3.67 Диаграммы направленности направленной антенны в горизонтальной и вертикальной плоскости

Диаграмма направленности является удобным средством определения такой меры направленности антенны, как **ширина луча**. Ширина луча – это угол, в пределах которого излучаемая мощность составляет не менее половины мощности, которая излучается в преимущественном направлении. Другими словами, ширина луча представляет собой угловое расстояние между точками половинной мощности на диаграмме направленности антенны любой плоскости, горизонтальной или вертикальной (точки на уровне 3 дБ). Измеряется ширина луча в градусах.

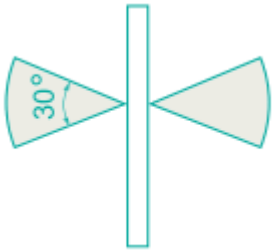


Рис. 3.68 Ширина луча антенны

В характеристиках антенн производители обычно указывают ширину луча в горизонтальной и вертикальной плоскости. Например, диаграмма направленности антенны в горизонтальной/вертикальной плоскости 80°/68° говорит о том, что антенна является направленной. Сигнал, передаваемой этой антенной, распространяется в горизонтальном направлении в зоне, определенной углом 80°, в вертикальном направлении – в зоне, определенной углом 68°. Диаграмма направленности антенны в горизонтальной/вертикальной плоскости 360°/32° говорит о том, что антенна является всенаправленной. В горизонтальной плоскости зона излучения охватывает угол в 360°, в вертикальной – 32°.

Диаграмма направленности является графическим представление зависимости *коэффициента усиления антенны* от направления антенны в заданной плоскости.

Коэффициент усиления *G* является мерой *направленности* антенны. Он определяется как отношение мощности сигнала *P1*, излученного в определенном направлении, к мощности сигнала *P2*, излучаемого идеальной всенаправленной (изотропной) антенной в любом направлении.

$$G = P1 / P2$$

Из этой формулы следует, что коэффициент усиления антенны – безразмерная величина. На практике его выражают несколько иначе – через логарифмическое отношение мощностей, напряжений или токов в децибелах (dB):

$$G = 10lg\ P1 / P2$$

В технических описаниях антенн, в частности антенн производства D-Link, единицы измерения коэффициента усиления антенн выражаются в изотропных децибелах – dBi, т.е в тех же децибелах, но с третьей буквой «i», обозначающей слово «isotropic» (изотропный).

Когда говорят, что коэффициент усиления антенны составляет 10 dBi, то имеется в виду направление, в котором достигается максимальная мощность излучения (главный лепесток диаграммы направленности в любой плоскости).

Часто название этого параметра «коэффициент усиления» приводит к ошибочному предположению, что антенны способны усиливать сигнал. На самом деле это не так – если мощность передатчика, к примеру, составляет 50 мВт, то какую бы антенну мы ни поставили, мощность передаваемого сигнала будет такой же. Дело в том, что все антенны подобного рода представляют собой пассивные устройства и брать энергию для усиления передаваемого сигнала им попросту неоткуда. Увеличение мощности сигнала в одном направлении происходит за счет остальных направлений распространения. Другими словами, увеличение мощности в одном направлении влечет за собой уменьшение мощности в других направлениях.

Еще одной важной характеристикой антенны является ее *поляризация*. Поляризация – это физическая ориентация элемента антенны, который непосредственно излучает энергию в радиочастотном диапазоне. Существуют антенны с вертикальной, горизонтальной и круговой (с правым и левым вращением) поляризациями (Рис. 3.69).

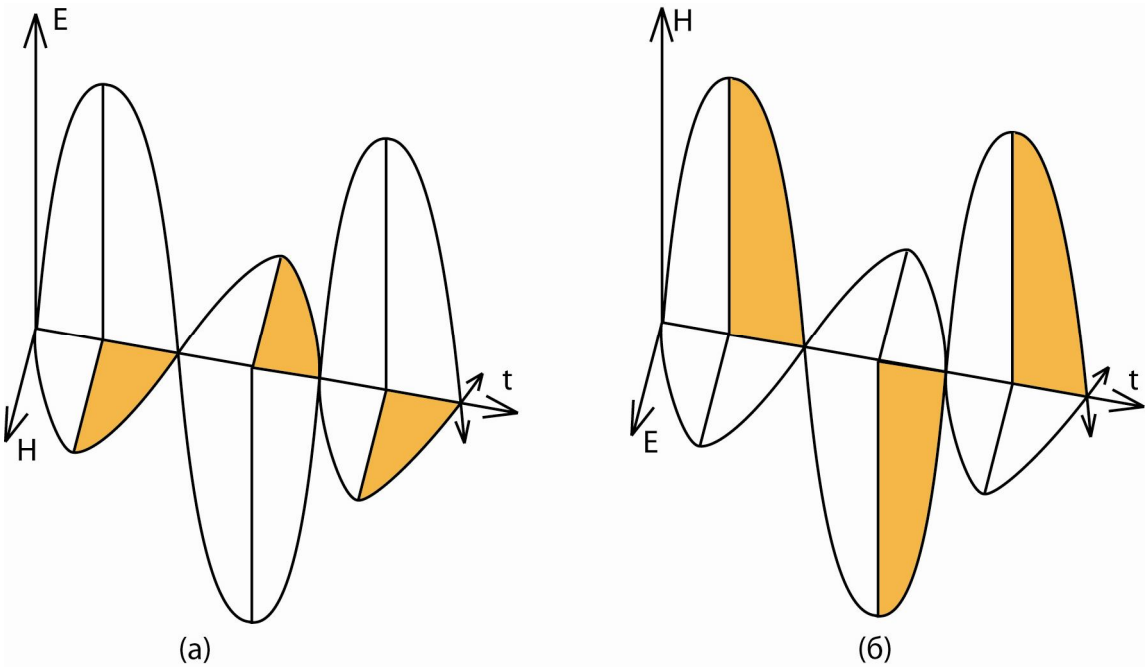


Рис. 3.69 Вертикальная (а) и горизонтальная (б) поляризации

В плоской электромагнитной волне векторы вертикального электрического E и магнитного H полей в каждый момент времени ориентированы в пространстве определенным образом. Поляризация электромагнитной волны является ее пространственно-временной характеристикой и определяется видом траектории, описываемой концом вектора электрического поля в фиксированной точке пространства. На антеннах с поляризацией имеется указатель, который и определяет необходимую поляризацию.

При круговой или циклической поляризации электромагнитное поле вращается вокруг оси t с определенным циклом, или шагом, так, что в разных точках пространства принимает или вертикальную или горизонтальную поляризацию. Такой вид поляризации сравнительно редко применяется.

Учет поляризации позволяет получить дополнительные энергетические преимущества при решении задач электромагнитной совместимости, планировании зон обслуживания и т. д. При заполнении определенного пространства точками доступа до предельного уровня, после которого взаимные радиопомехи начинают мешать нормальной работе сетей, достаточно изменить поляризацию антенн, после чего можно продолжать расширять беспроводную сеть.

3.8.1 Распространение сигналов в беспроводных средах передачи

При распространении сигнал, излученный антенной, может огибать поверхность Земли, отражаться от верхних слоев атмосферы, либо распространяться вдоль линии прямой видимости. Способ распространения сигнала, расстояние его передачи и т.п. во многом зависят от диапазона частот используемого электромагнитного спектра.

Весь спектр электромагнитного излучения разделен на частотные диапазоны в зависимости от типа электромагнитных волн:

- радиоволны;
- инфракрасное излучение;
- видимый свет.
- ультрафиолетовое излучение,
- рентгеновское излучение;
- гамма-излучение.

Для нас представляет интерес микроволновый диапазон радиочастот, в котором можно вести беспроводную передачу (Рис. 3.70).

В диапазоне частот от 30 МГц до 300 ГГц находятся ультракороткие волны, длина волны которых от 10 м до 0,1 м (чем выше частота, тем короче волна). Ультракороткие волны широко применяются для организации радиорелейных линий связи, спутниковых каналов, беспроводных локальных сетей Wi-Fi и системы фиксированного беспроводного доступа. Основное ограничение связи с помощью ультракоротких волн: приемник и передатчик должны быть *в зоне прямой видимости* друг друга. Это связано с тем, что ультракороткие волны распространяются преимущественно прямолинейно и почти не огибают природных и искусственных преград, встречающихся на их пути. На их распространение существенное влияние оказывают рельеф местности, различные препятствия и метеорологические условия. В частности, волны сантиметрового диапазона SHF (Super High Frequency (сверхвысокие частоты, СВЧ); диапазон от 3 до 30 ГГц), которые широко используется в сетях Wi-Fi, сильно поглощаются атмосферными осадками и явлениями (дождь, снег, туман и пр.), а также газами атмосферы, что в свою очередь приводит к быстрому ослаблению напряженности электромагнитного поля.

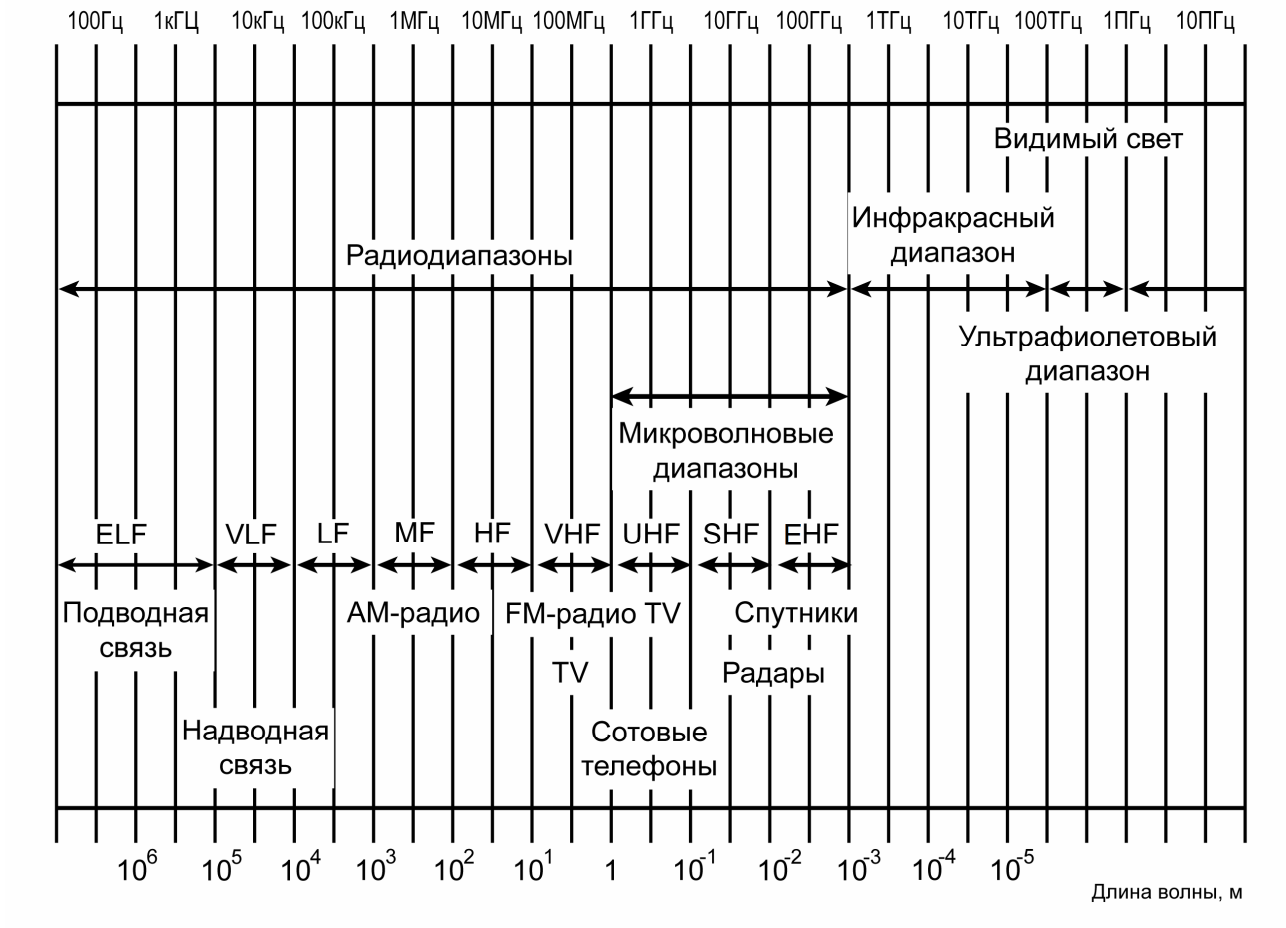


Рис. 3.70 Спектр электромагнитных волн

Если расположение антенн в системе связи является относительно произвольным, может случиться так, что беспроводной канал связи совпадет с линией прямой видимости между передатчиком и приемником (при отсутствии препятствий, приводящих к интерференции). Как правило, такое раположение выбирается для двухточечных высокочастотных каналов связи. Однако в большинстве случае, между передатчиком и приемником препятствия встречаются довольно часто. В помещениях такими препятствиями служат стены, потолки, мебель. На открытом пространстве – дома, деревья, транспорт. При встрече на пути своего распространения препятствий, электромагнитные волны могут отражаться от них, преломляться, рассеиваться или огибать препятствия.

Отражение имеет место, когда электромагнитная волна встречается с препятствием, размеры которого намного превышают длину волны. В этом случае часть энергии электромагнитной волны отражается от такого препятствия.

Рис. 3.71 Отражение электромагнитной волны

Попадая на границу раздела двух прозрачных для электромагнитной волны сред с разной плотностью, часть волны отражается, а часть проходит в другую среду, преломляясь.

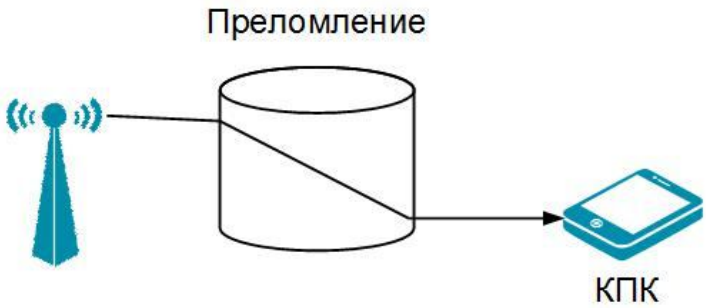


Рис. 3.72 Преломление электромагнитной волны

Если электромагнитная волна встречает непроницаемое для нее препятствие, размер которого сравним с ее длиной (дома, горы), происходит дифракция – сигнал как бы огибает препятствие. Так что такой сигнал можно получить, даже не находясь в зоне прямой видимости.

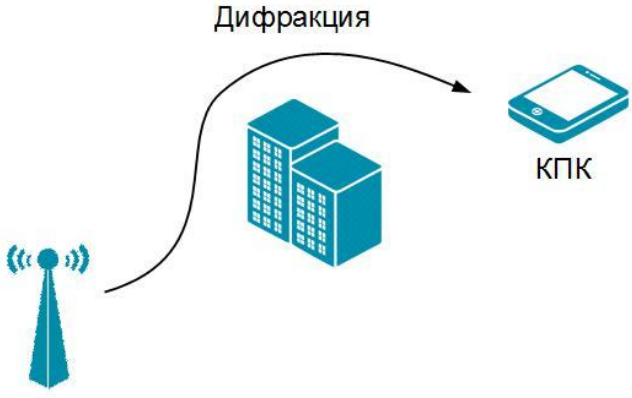


Рис. 3.73 Дифракция электромагнитной волны

При встрече с препятствием, размеры которого много меньше длины волны (туман, листья деревьев, грязь), происходит рассеяние волн – отражение под разными углами.

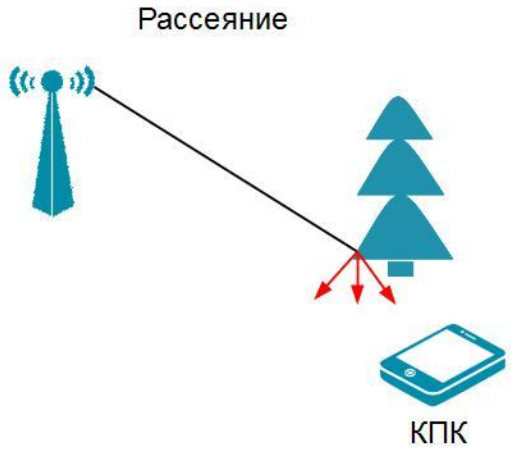


Рис. 3.74 Рассеяние электромагнитной волны

В результате отражения, дифракции и рассеяния приемник может получить исходный сигнал и его несколько отраженных копий, которые достигли его антенны разными путями и в разные промежутки времени. В точке приема исходный и отраженные сигналы накладываются друг на друга, т.е. возникает интерференция. В итоге исходный сигнал искажается, его мощность изменяется (увеличивается или уменьшается амплитуда) в зависимости от фаз складываемых сигналов. Такой эффект называется *многолучевым распространением сигнала*.

Многолучевое распространение по-разному влияет на производительность системы в зависимости от особенностей местности и перемещения мобильного устройства. В средах с прямой видимостью между источником и приемником, влияние многолучевого распространения обычно выражено слабо и легко преодолимо. Амплитуды отраженных сигналов намного слабее исходного сигнала. В условиях отсутствия прямой видимости отраженные сигналы могут иметь более высокие уровни мощности, потому что путь исходного сигнала может быть частично или полностью прегражден препятствиями. В рельтате сложения с отраженными сигналами уровень мощности исходного сигнала по отношению к шуму может снизиться, что усложнит распознавание сигнала приемником. В общем случае эффект от многолучевого распространения здесь более заметен. Однако следует отметить, что при отсутствии линии прямой видимости между передатчиком и приемником (например, в парках, транспорте с сервисом Wi-Fi) сигнал принимается в обновном благодаря дифракции и рассеянию.

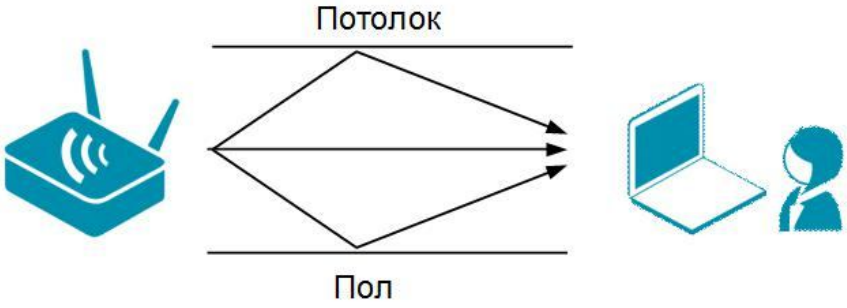


Рис. 3.75 Многолучевое распространение сигнала

Если максимальная задержка распространения между всеми сигналами (исходным и отраженными) меньше длительности одного символа (цифрового импульса), то возникает только *многолучевая интерференция*. Если она сравнима или больше длительности одного символа, то в результате интерференции складываются сигналы, представляющие разные символы, и возникает так называемая *межсимвольная интерференция*.

Для борьбы с этим эффектом используют разные технологии, такие как разнесение антенн, механизм мультиплексирования с добавлением защитного интервала и технология *MIMO*.

MIMO (*Multiple Input Multiple Output*) – это технология использования нескольких передающих и принимающих антенн с применением пространственного мультиплексирования (несколько путей распространения сигнала по одному радиоканалу).

Помимо многолучевого распространения к искажению передаваемого по беспроводному каналу связи сигнала приводит затухание, потери в свободном пространстве, шум, атмосферное поглощение.

При передаче сигнала в любой среде его интенсивность уменьшается с расстоянием, т.е. происходит затухание сигнала. Если расстояние между приемником и передатчиком превышает некоторое расчетное значение, свыше которого затухание становится неприемлемо высоким, для усиления сигнала в заданных точках пространства располагают ретрансляторы или усилители. Задача усиления сигнала значительно усложняется, если существует множество приемников, особенно если расстояние между ними и передающей станцией непостоянно.

Передаваемый сигнал рассеивается по мере его распространения в пространстве (в качестве аналогии можно представить падение с расстоянием интенсивности луча фары автомобиля). Данный тип затухания называют *потерями в свободном пространстве*. Они приводят к ослаблению сигнала при его прохождении от передатчика до приемника даже если все остальные причины затухания отсутствуют.

Причиной дополнительных потерь мощности сигнала между передающей и принимающей антеннами является атмосферное поглощение, при этом основной вклад в ослабление сигнала вносят водные пары и кислород. Дождь и туман (капли воды, находящиеся во взвешенном состоянии в воздухе) приводят к рассеиванию радиоволн и, в конечном счете, к ослаблению сигнала. Указанные факторы могут быть основной причиной потерь мощности сигнала. Следовательно, в областях, для которых характерно значительное выпадение осадков, необходимо либо сокращать расстояние между приемником и передатчиком.

Источниками шумов в беспроводных линиях связи могут служить микроволновые печи, беспроводные телефоны, радиопередатчики, датчики движения, соседние беспроводные сети, беспроводные камеры системы видеонаблюдения, молнии и др. Интенсивность битовых ошибок в беспроводных сетях BER составляет 10^{-3}.

Проблема высокого уровня помех беспроводных каналов решается различными способами. В городских условиях передатчики сигнала (и приемники, если это возможно) стараются разместить на высоких зданиях или вышках, чтобы избежать многократных отражений. В домашних беспроводных сетях одним из решений проблемы является смена рабочего частотного канала работы точки доступа, в том случае, если какой-то посторонний передатчик излучает электромагнитные волны в этом же канале, а также отключение всех приборов, например микроволновых печей, перед подключением к беспроводной сети.

Важную роль играют специальные методы модуляции и кодирования, распределяющие энергию сигнала в широком диапазоне частот. Также для быстрой коррекции ошибок, возникающих при передаче, используют протоколы канального уровня с установлением соединений и повторными передачами кадров.

4 Топологии компьютерных сетей

4.1 Понятие топологии сети

При организации компьютерной сети одним из важных вопросов является выбор ее *топологии,* т.к. правильная сетевая конфигурация необходима для обеспечения надежной и эффективной работы всей сети, а также возможности дальнейшего ее расширения с наименьшими затратами.

Топология сети – это способ описания конфигурации сети, схемы расположения и соединения сетевых устройств с помощью кабельной инфраструктуры.

Следует различать понятия *физической топологии*, которая описывает реальное расположение и соединение узлов сети, и *логической топологии* – способов взаимодействия узлов и характер распространения сигналов по сети в рамках физической топологии.

Другими словами физическая топология определяет, как расположены и соединены устройства, а логическая топология – как данные передаются между устройствами, несмотря на их физическое размещение.

Логическая и физическая топология сети не обязательно должны совпадать. Например, локальная сеть Ethernet, построенная с использованием концентраторов и кабеля на основе витой пары в качестве среды передачи, имеет физическую топологию «звезда», а логическую топологию «шина». Логическая топология обычно определяется сетевыми протоколами и ассоциируется с методами управления доступом к среде передачи. Ее можно динамически изменить, благодаря применению сетевого оборудования, такого как маршрутизаторы, коммутаторы или точки доступа.

Физическая топология определяется местом расположения и возможностями сетевых устройств, среды передачи и стоимостью развертывания сетевой и кабельной инфраструктуры.

Существуют следующие базовые топологии, на основе которых строятся компьютерные сети:

- «шина» (bus);
- «кольцо» (ring);
- «звезда» (star).
- «дерево» (tree);
- ячеистая полносвязная топология (fully connected mesh);
- ячеистая топология частичной (неполной) связности (partially connected mesh).

Прежде чем перейти к рассмотрению сетевых топологий, давайте познакомимся с сетевым оборудованием, которое обеспечивает формирование структуры сети.

4.2 Сетевое оборудование в топологии

Для построения компьютерной сети требуется *сетевое* или *телекоммуникационное оборудование*, основной задачей которого является объединение компьютеров и других устройств в сеть и передача данных между ними, подключение компьютерных сетей разных топологий и технологий друг к другу, увеличение расстояния передачи сигнала. Кроме того, сетевое оборудование позволяет решать такие задачи, как обеспечение безопасности сетей, управление потоками данных, предоставление качества обслуживания и др.

Далее в данном разделе будет дано краткое описание сетевых устройств, которые используются в локальных сетях Ethernet, т.к. на данный момент эта технология является самой распространенной технологией локальных сетей. Описание устройств будет

выполняться исходя из соответствия их функций уровням модели OSI, начиная с физического уровня.

4.2.1 Повторители и концентраторы

На физическом уровне работают такие устройства как *повторители* и *концентраторы*. Повторители и концентраторы являются устаревшими устройствами, но рассмотрение их принципа работы важно для понимания принципа работы коммутаторов локальных сетей.

Повторитель *(repeater)* являлся самым простым из сетевых устройств. Он представлял собой устройство физического уровня модели OSI, используемое для соединения сегментов среды передачи данных с целью увеличения общей длины сети.

В сетях Ethernet (10BASE2 и 10BASE5) на основе коаксиального кабеля применялись двухпортовые повторители, связывающие два физических сегмента. Работал повторитель следующим образом: он принимал сигналы из одного сегмента сети, усиливал их, восстанавливал синхронизацию и передавал в другой. Повторители не выполняли сложную фильтрацию и другую обработку трафика, т.к. не являлись интеллектуальными устройствами. Также общее количество повторителей и соединяемых ими сегментов было ограничено из-за временных задержек и других причин.

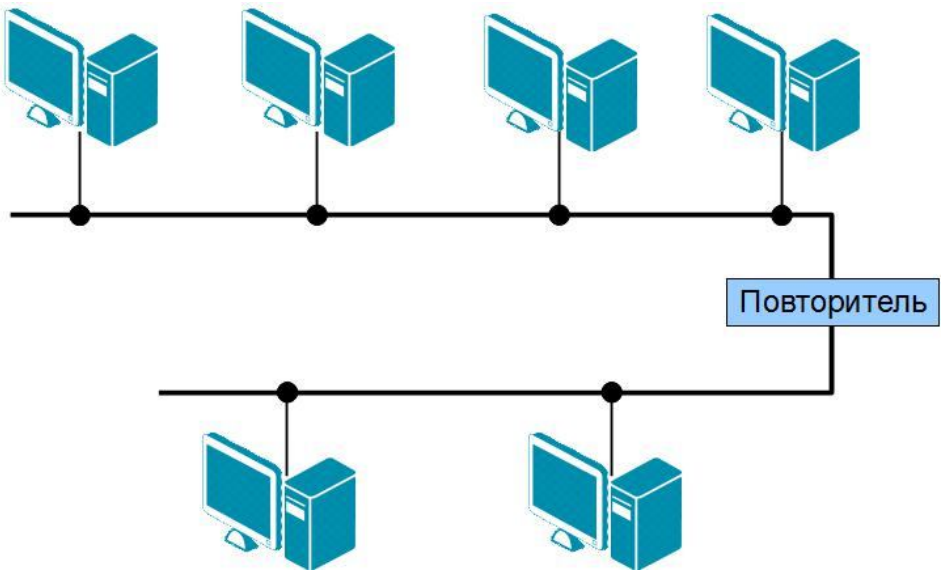


Рис. 4.1 Применение повторителя в сети

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов сети, называется **концентратором** *(concentrator,* также известен как *хаб (hub))*. Концентратор представляет собой устройство физического уровня модели OSI, основной задачей которого является повторение сигнала, поступившего с одного из своих портов на все остальные активные порты, предварительно восстанавливая их. Он не выполняет никакой фильтрации трафика и другой обработки данных, поэтому сети, построенные с использованием концентраторов, могут иметь различную физическую топологию, но логическая топология всегда останется шинной.

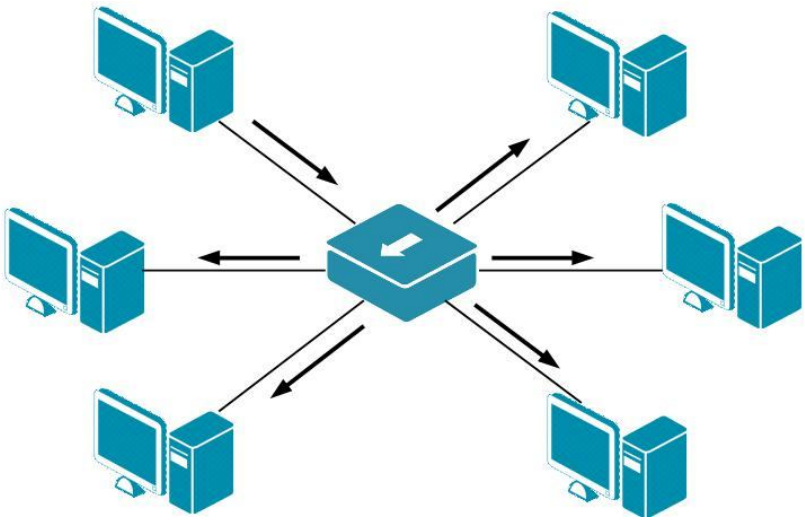


Рис. 4.2 Обмен данными в сети через концентратор

Устройства, которым требовалось подключение к локальной сети, соединялись с концентратором отдельным кабелем. Концентратор создавал общую среду распространения сигнала для всех узлов локальной сети. В один момент времени в такой сети мог передавать данные только один компьютер. В случае одновременного поступления сигналов на два или более порта концентратора возникала *коллизия*, которая приводила к повреждению передаваемых кадров. Таким образом, все подключенные к концентратору устройства находились в одном *домене коллизий*.

Коллизия (*collision*) – наложение или столкновение сигналов, которое возникает во время одновременной передачи данных двумя или более узлами и приводит к повреждению данных.

Домен коллизий *(collision domain)* – часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети она возникла.

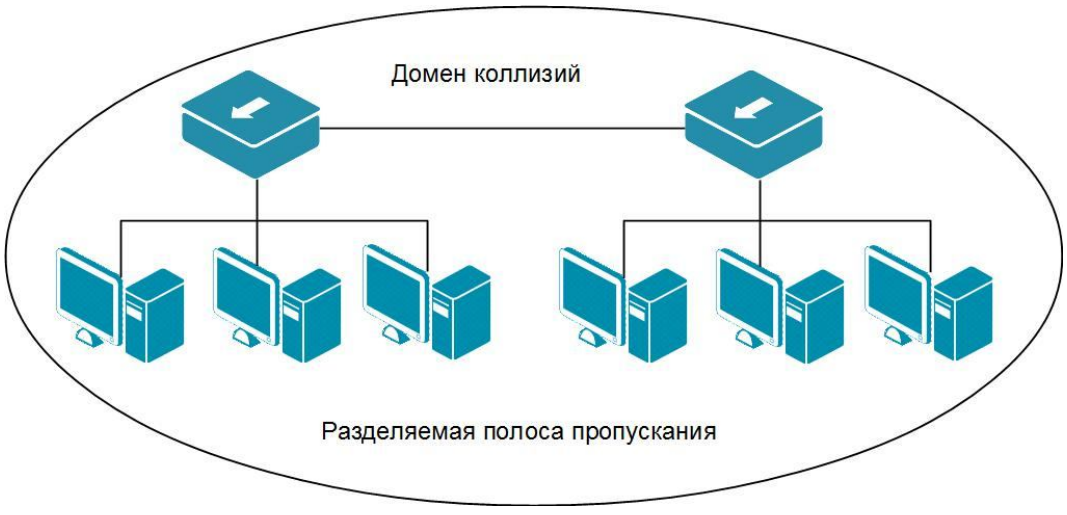


Рис. 4.3 Домен коллизий

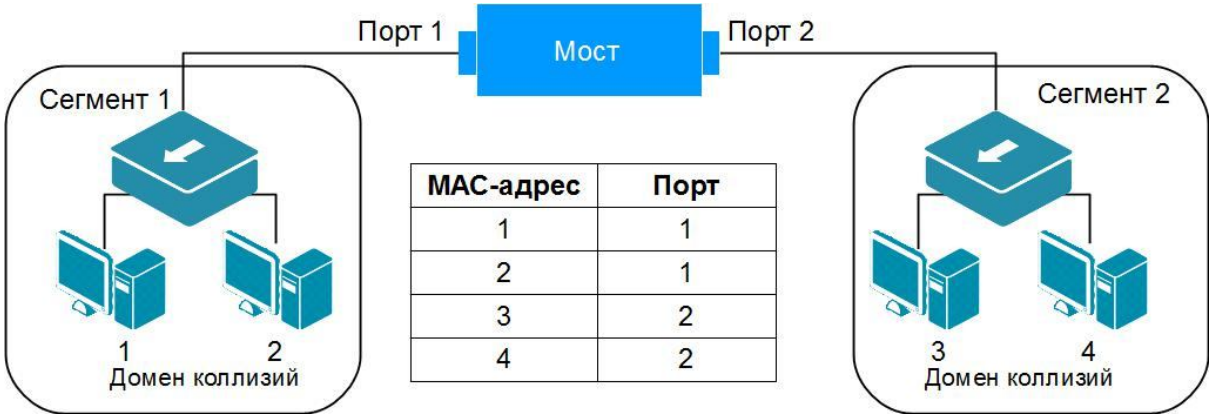
С увеличением количества сегментов сети и компьютеров в них, возрастало количество коллизий. Кроме того, общее количество концентраторов и соединяемых ими сегментов сети было ограничено из-за временных задержек и снижения пропускной способности сети. Помимо этого сеть, построенная с помощью концентраторов, характеризовалась низким уровнем сетевой безопасности, т. к. передача данных через все порты позволяла «прослушивать» информацию, передаваемую по сети. Невысокая

пропускная способность и слабый уровень сетевой защиты привели к тому, что в современных компьютерных сетях концентраторы не применяются, их вытеснили сначала мосты, а затем коммутаторы.

4.2.2 Мосты и коммутаторы

Мост *(bridge)* был разработан компанией Digital Equipment Corporation (DEC) в начале 1980-х годов и представлял собой устройство физического и **канального** уровней модели OSI, предназначенное для объединения двух локальных сетей или двух сегментов одной сети.

Мост в отличие от концентратора не просто усиливал и восстанавливал форму сигнала при его передаче с одного порта на другой, но и обладал некоторыми интеллектуальными функциями. Он пересылал через себя кадры (блок данных канального уровня) только в том случае, если такая передача действительно была необходима, то есть если физический адрес (MAC-адрес) узла назначения принадлежал другому сегменту сети или другой сети. Делал он это с помощью хранимой в памяти *таблицы коммутации* – таблицы соответствия своих портов и используемых в каждой сети (сегменте сети) MAC-адресов, которую формировал сразу после включения питания. Благодаря этому мост изолировал трафик одного сегмента сети (или сети) от трафика другого, уменьшая коллизии за счет деления одного большого домена коллизий на два небольших и повышая общую производительность сети. Также мост уменьшал возможность несанкционированного доступа к данным, так как кадры не выходили за пределы своего сегмента, и их сложнее было перехватить злоумышленнику.



MAC-адрес	Порт
1	1
2	1
3	2
4	2

Рис. 4.4 Соединение двух сегментов сети с помощью моста

Мосты являются устаревшими устройствами, на смену которым пришли **коммутаторы** (*switch*). Коммутатор представляет собой многопортовый мост и по принципу обработки данных ничем не отличается от него, однако в отличие от моста поддерживает множество дополнительных функций. Коммутатор функционирует на **канальном** (втором) **уровне** модели OSI и служит для объединения сетевых устройств в пределах одного или нескольких сегментов сети.

Сетевые устройства могут функционировать как на одном, так и на нескольких уровнях модели OSI. Обычно при описании сетевых устройств упоминают наивысший уровень модели OSI, протоколы которого они поддерживают. При этом подразумевается, что устройства могут работать и на нижележащих уровнях. Например, когда говорят, что коммутатор – это устройство второго или канального уровня модели OSI, имеется в виду, что он выполняет функции физического и канального уровней.

Коммутатор может быть оборудован большим количеством портов и *параллельно устанавливать несколько соединений* между разными парами портов, что обеспечивает одновременное взаимодействие подключенных к нему устройств.

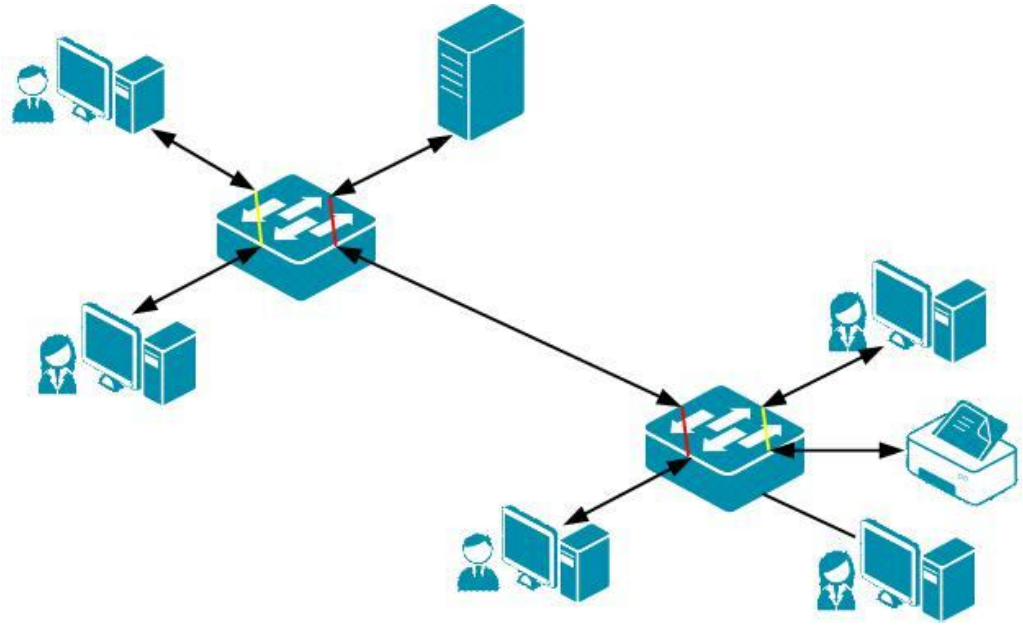


Рис. 4.5 Применение коммутаторов в сети

При передаче кадра через коммутатор в нем создается отдельный виртуальный или реальный (в зависимости от архитектуры) канал, по которому данные пересылаются напрямую от порта-источника к порту-получателю с максимально возможной для используемой технологии скоростью. Такой принцип работы получил название *«микросегментация»*.

Микросегментация (*microsegmentation*) – разбиение коммутатором локальной сети одного домена коллизий на меньшие домены для каждого порта.

Благодаря микросегментации, коммутаторы получили возможность функционировать в *режиме полного дуплекса* (full duplex), что позволило каждому узлу, непосредственно подключенному к порту коммутатора, одновременно передавать и принимать данные. Таким образом, благодаря появлению режима полного дуплекса, исчезло понятие домена коллизий. Узлам не приходится конкурировать за полосу пропускания с другими устройствами, в результате чего не происходят коллизии, и повышается производительность сети.

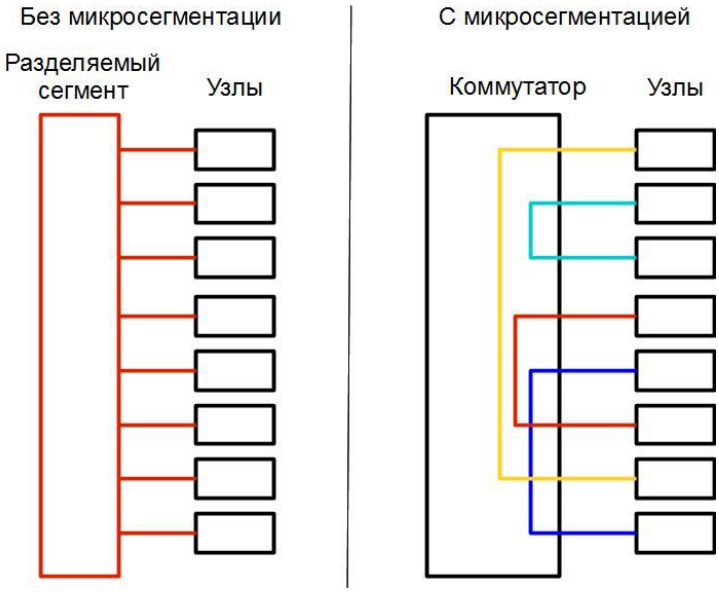


Рис. 4.6 Микросегментация

Передачу данных коммутатор, так же как мост осуществляет на основе таблицы коммутации, что позволяет ему локализовать трафик внутри сегмента сети. Когда коммутатор получает кадр, он извлекает из него MAC-адрес получателя и ищет этот MAC-адрес в таблице коммутации. Как только в таблице коммутации будет найдена запись, ассоциирующая MAC-адрес получателя с одним из портов коммутатора, кадр будет передан через соответствующий порт (Рис. 4.7).

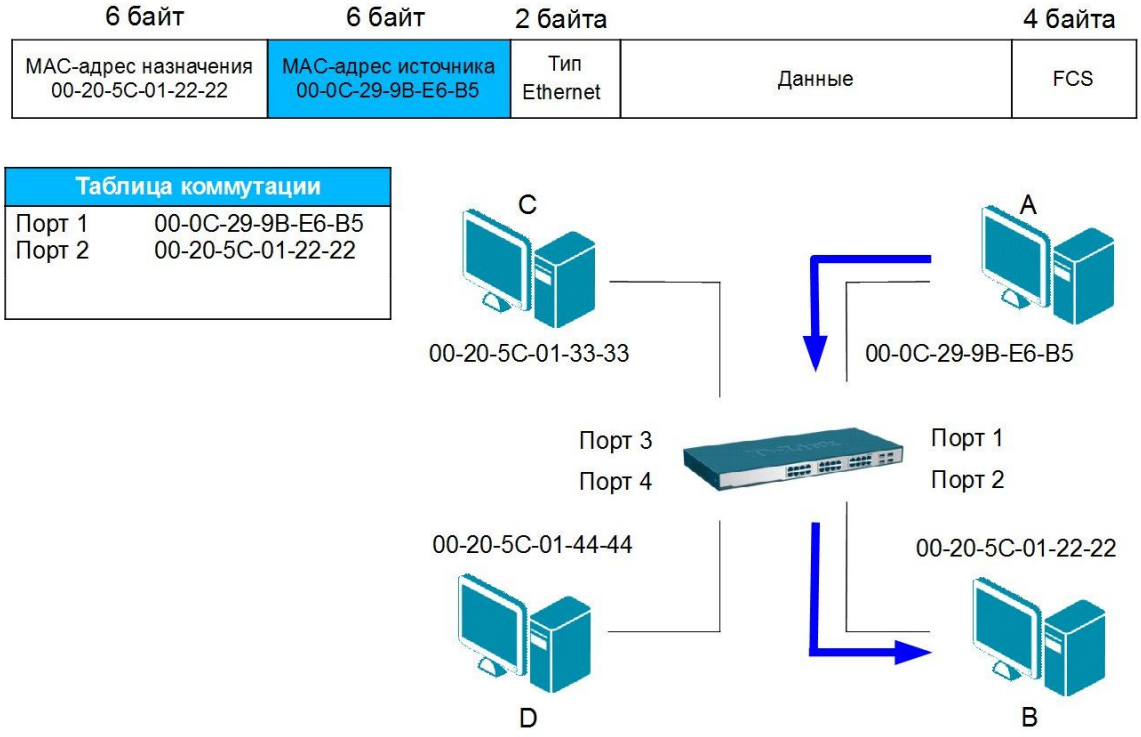


Рис. 4.7 Передача кадров через коммутатор

Если в таблице коммутации отсутствует запись соответствия MAC-адреса устройства и порта коммутатора или MAC-адрес назначения является широковещательным (кадр предназначен всем узлам сети), то коммутатор передает кадры через все порты, т. е. работает

как концентратор. В этом случае говорят, что коммутатор образует *широковещательный домен* (broadcast domain).

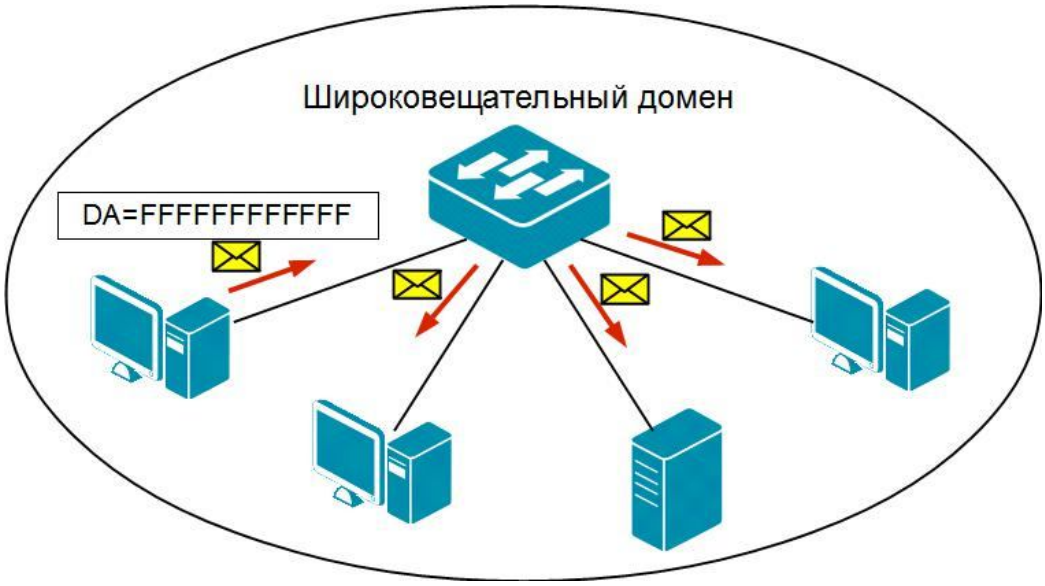


Рис. 4.8 Широковещательная рассылка через коммутатор

В настоящее время коммутаторы являются основным строительным блоком для создания локальных сетей. Современные коммутаторы Ethernet, кроме своего основного назначения могут выполнять ряд дополнительных функций, таких как организация резервирования и повышения отказоустойчивости сети, создание виртуальных локальных сетей (VLAN), определение и ограничение перегрузок в сети, обеспечение безопасности, фильтрации трафика и многих других.

Подробнее про коммутаторы и поддерживаемые ими технологии будет рассказано в главе 6.

4.2.3 Маршрутизаторы

Все рассмотренные выше устройства позволяют объединять узлы в локальную сеть, однако для организации взаимодействия между сетями и подключения локальных сетей к глобальным требуется специальное сетевое оборудование – *маршрутизаторы*.

Маршрутизатор *(router)* – это устройство **сетевого** (третьего) **уровня** модели OSI, основной задачей которого является анализ логических (сетевых) адресов (чаще всего IP-адресов) и определение наилучшего маршрута передачи пакета от источника к получателю.

Маршрутизатор выполняет функции физического, канального и сетевого уровней модели OSI. На первых двух уровнях он взаимодействует с локальными сетями или различными сегментами одной сети, на третьем – принимает решение о дальнейшем маршруте пакетов.

Маршрутизатор может соединять между собой как минимум две сети. Маршрутизаторы D-Link, в зависимости от модели, могут быть оборудованы от 1 до 8 интерфейсами LAN, которые используется для подключения локальных сетей, и 1 или 2 интерфейсами WAN, предназначенными для соединения локальных сетей с внешней сетью, как правило, сетью Интернет-провайдера, предоставляющего клиентам доступ в Интернет.

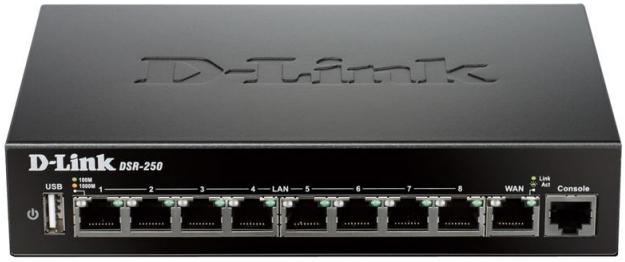


Рис. 4.9 Маршрутизатор D-Link DSR-250

Протоколы, используемые на физическом, канальном и сетевом уровнях разных сетей, могут быть различными. В отличие от коммутаторов, маршрутизаторы изменяют передаваемые пакеты данных. Они «разбирают» их до сетевого уровня, а затем вновь формируют по определенным правилам с учетом технологии, поддерживаемой интерфейсом, через который будут переданы данные. Другими словами они выполняют преобразование протоколов перед отправкой данных в другую сеть или другой сегмент сети. Поэтому маршрутизаторы используются в качестве **шлюза** *(gateway)* при объединении сетей, использующих разные протоколы.

По этой причине бюджетные маршрутизаторы, предназначенные для подключения домашних сетей и сетей небольших офисов к Интернет называют *Интернет-шлюзами.* Такие устройства могут объединять в себе функции коммутатора, беспроводной точки доступа, ADSL-модема, а также оснащены встроенным межсетевым экраном для предотвращения вторжения из внешней сети. В качестве примера Интернет-шлюза можно привести маршрутизатор D-Link DIR-615.

Рис. 4.10 Маршрутизатор DIR-615

Рис. 4.11 Подключение к Интернет с помощью Интернет-шлюза

Благодаря использованию логической (сетевой) адресации маршрутизаторы надежнее, чем коммутаторы изолируют трафик отдельных частей сети друг от друга, образуя *логические сегменты*.

В отличие от плоских физических адресов (MAC-адресов), в логических адресах (обычно IP-адресах) имеется поле номера сети, поэтому все узлы, у которых значение этого поля одинаково, принадлежат одному сегменту, называемому в данном контексте *подсетью* (subnetwork, subnet). К каждому интерфейсу маршрутизатора может быть подключена одна сеть (подсеть).

Без специальной настройки маршрутизаторы не передают через свои порты широковещательные пакеты, таким образом, они ограничивают область распространения широковещательного трафика, т.е. делят большой широковещательный домен на домены меньшего размера.

Подробнее про маршрутизаторы и поддерживаемые ими технологии будет рассказано в главе 11 «Протоколы сетевого уровня».

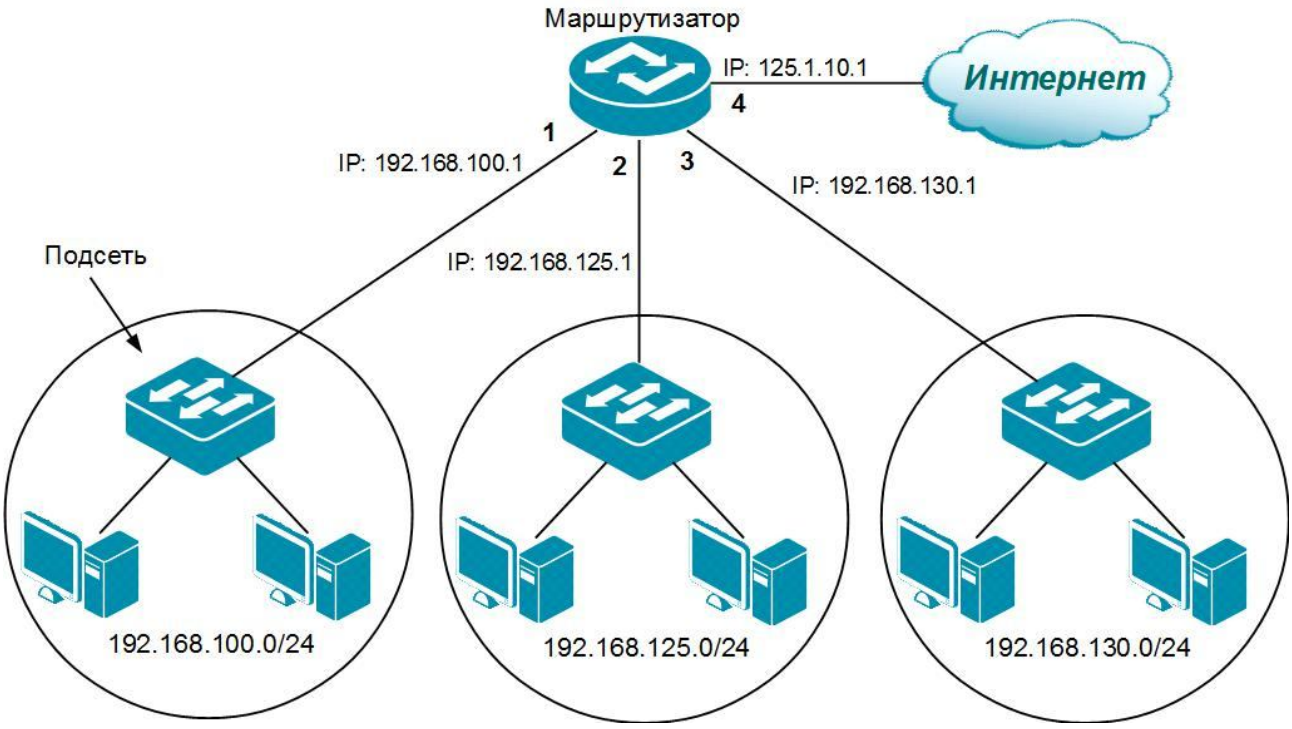


Рис. 4.12 Объединение разных сетей (подсетей) с помощью маршрутизатора

Следует отметить, что проблема распространения широковещательного трафика в сетях, построенных на коммутаторах, решается с помощью технологии *виртуальных локальных сетей* (Virtual LAN, VLAN).

Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса – индивидуального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с MAC-адресом назначения кадра.

Коммутатор, программное обеспечение которого поддерживает функцию виртуальных локальных сетей, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Благодаря этому можно объединять компьютеры в виртуальные рабочие группы (логические сегменты) независимо от их физического размещения в сети. Подробнее про технологию VLAN будет рассказано в главе 6.

В последнее время на магистралях сетей масштаба предприятия и провайдеров услуг маршрутизаторы преимущественно заменяются коммутаторами 3 уровня, которые осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI. Коммутаторы 3 уровня выполняют коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

4.2.4 Средства управления сетевыми устройствами

Логическую топологию можно динамически менять, выполняя различные настройки сетевого оборудования. Большинство современных устройств поддерживают различные функции управления и мониторинга. К ним относятся дружественный пользователю Web-интерфейс управления, интерфейс командной строки (Command Line Interface, CLI), Telnet, SNMP-управление.

Web-интерфейс управления позволяет осуществлять настройку и мониторинг параметров сетевых устройств, используя любой компьютер, оснащенный Web-браузером. Он имеется у точек доступа, Интернет-шлюзов, настраиваемых и управляемых коммутаторов, сетевых накопителей (NAS), IP-камер, шлюзов IP-телефонии, IP-телефонов. С помощью Web-интерфейса администратор может посмотреть статус устройства, статистику по производительности и т.д. и произвести необходимые настройки.

Следует отметить, что вид Web-интерфейса у разных устройств (и у разных аппаратных ревизий одной модели) может отличаться. Описание Web-интерфейса и работы с ним доступно в руководстве пользователя на соответствующее устройство.

В качестве примера рассмотрим Web-интерфейс точки доступа DAP-2310 (Рис. 4.13). Условно Web-интерфейс можно разделить на 3 области. Область 1 содержит список папок, объединяющих семейство функций, предназначенных для выполнения той или иной задачи. В области 3 отображаются текущие настройки устройства или поля для их изменения, в зависимости от выбранного в области 1 пункта меню. В области 2, в зависимости от модели и типа устройства, может осуществляется доступ к настройкам или отображаться графическое изображение передней панели устройства в режиме реального времени.

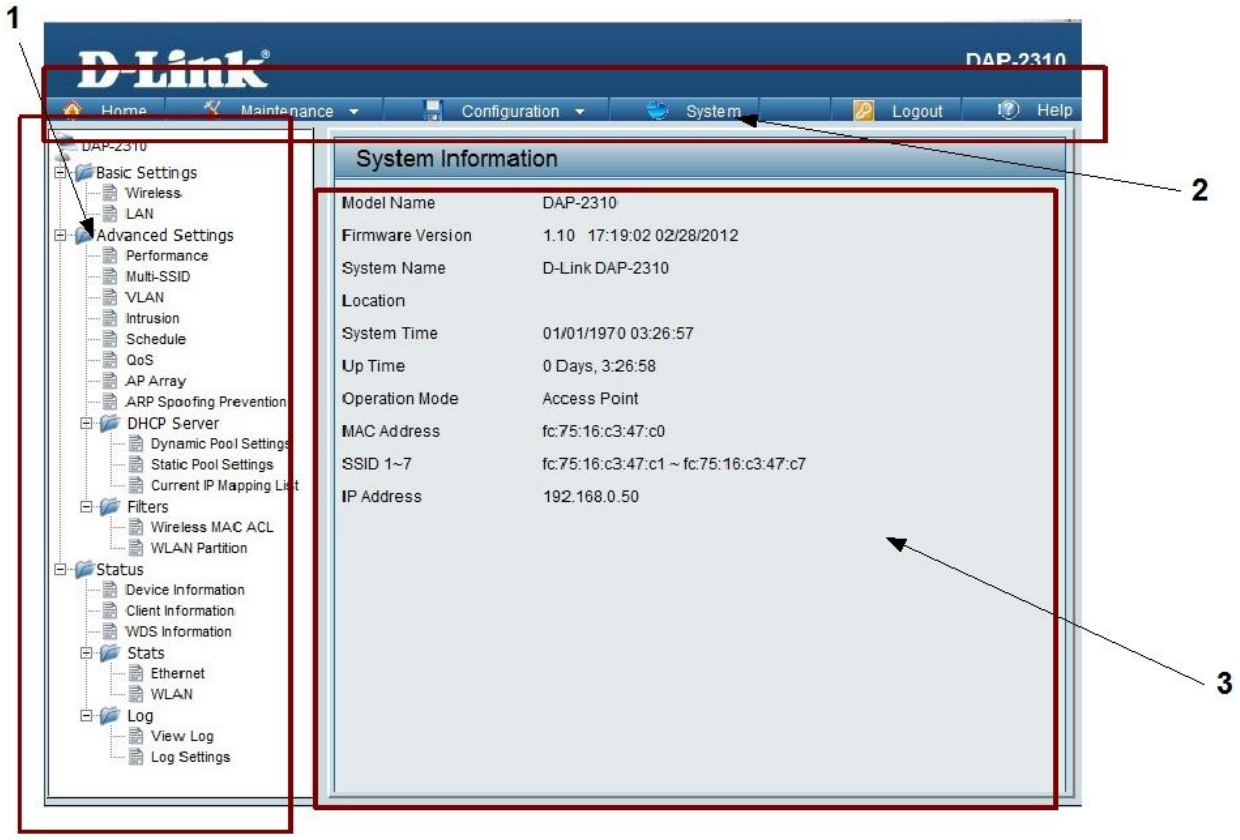


Рис. 4.13 Web-интерфейс управления точки доступа DAP-2310

Web-интерфейс управления состоит из пользовательского графического интерфейса (GUI), запускающегося на клиенте, и HTTP/HTTPS-сервера, запускаемого на устройстве.

Связь между клиентом и сервером обычно осуществляется через TCP/IP соединение с портом 80 протокола HTTP. При первом подключении к HTTP-серверу на сетевом устройстве необходимо выполнить следующие шаги:

Шаг 1. Подключить один конец кабеля Ethernet к порту Ethernet на компьютере, а другой – к любому LAN-порту Ethernet на устройстве.

Шаг 2. Назначить компьютеру статический IP-адрес из той же сети, что и IP-адрес интерфейса управления сетевого устройства (обычно указывается в руководстве пользователя). Например, если коммутатору присвоен IP-адрес 10.90.90.90, то компьютеру необходимо назначить IP-адрес вида 10.x.y.z (где x и y – числа от 0 до 254, z – число от 1 до 254) и маску подсети 255.0.0.0.

IP-адрес или **адрес третьего уровня** – это логический адрес, который не привязывается к конкретной аппаратуре (сетевой карте, порту и т. д.) и назначается администратором сети независимо от физических адресов (MAC-адресов).

Шаг 3. На компьютере запустить Web-браузер (Internet Explorer, Mozilla Firefox, Google Chrome), в адресной строке которого ввести IP-адрес интерфейса управления по умолчанию (обычно указывается в руководстве пользователя).

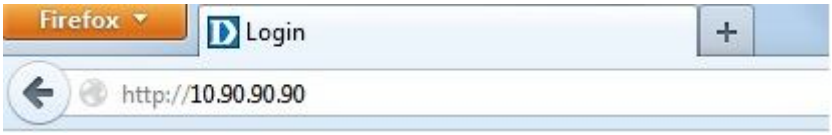


Рис. 4.14 IP-адрес интерфейса управления по умолчанию в адресной строке Web-браузера

Шаг 4. В появившемся окне аутентификации в поле Password необходимо ввести admin и нажать кнопку OK. После этого появится окно Web-интерфейса сетевого устройства.

Рис. 4.15 Окно аутентификации пользователя

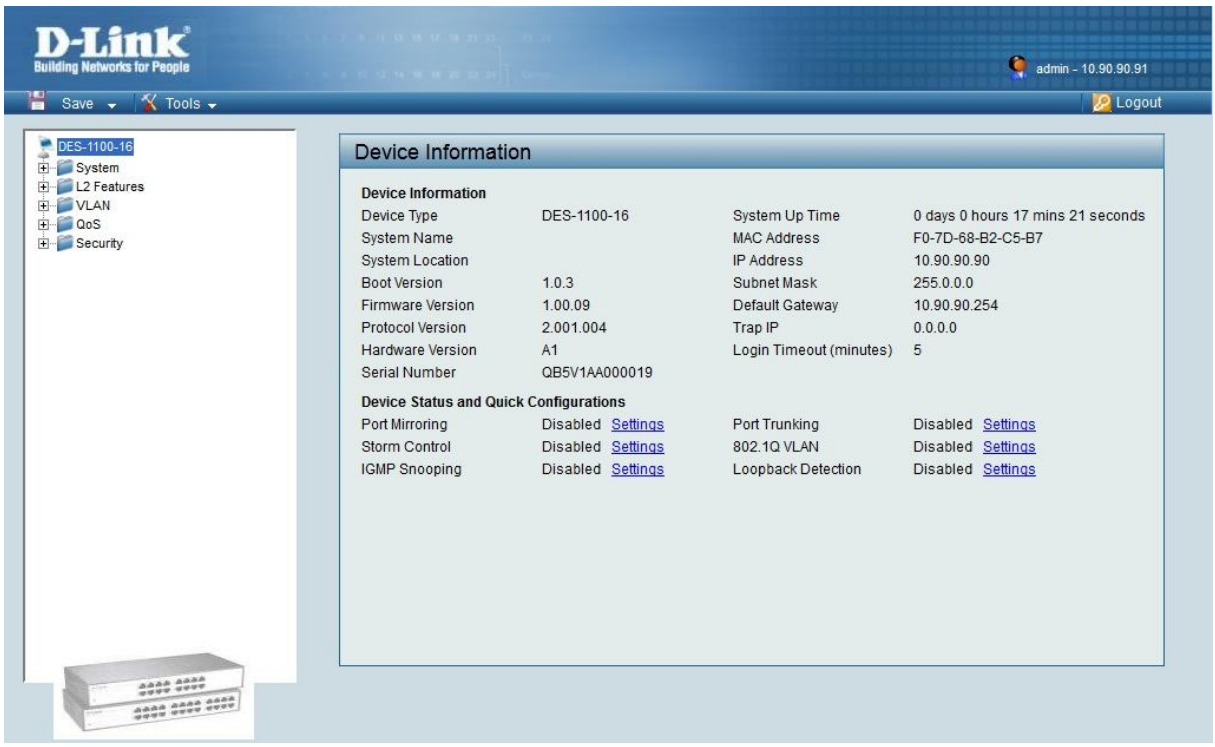


Рис. 4.16 Web-интерфейс управления коммутатора DES-1100-16

Внимание: программное обеспечение оборудования D-Link предлагает возможность выбора языка Web-интерфейса. Информацию о поддержке Web-интерфейсом устройства русского языка можно получить в технической поддержке компании.

Рис. 4.17 Выбор языка Web-интерфейса в маршрутизаторе DIR-300

Дополнительно к настройке параметров через традиционный Web-интерфейс, некоторые модели маршрутизаторов предоставляют возможность визуализации и интерактивной конфигурации. Все основные функции устройства (подключение к Интернет, беспроводная сеть, фильтрация и т.д.) представлены на одной странице в виде схемы. Каждой функции соответствует своя пиктограмма. Для ввода параметров не требуется долгого поиска функции в списке папок. Достаточно навести курсор мыши на нужную пиктограмму, и открыть диалоговое окно для ввода параметров функции. При активизации определенных функций маршрутизатора соответствующие пиктограммы на схеме выделяются цветом. Помимо этого, рядом с пиктограммами отображается информация о параметрах настройки. Например, в случае успешного соединения, пиктограмма *Интернет* (рисунок 4.18) загорается зеленым цветом, в левой части отображается название активного

соединения, полученный IP-адрес, а также MAC-адрес этого соединения. В правой части отображается текущая скорость передачи данных и общий объем принятых данных.

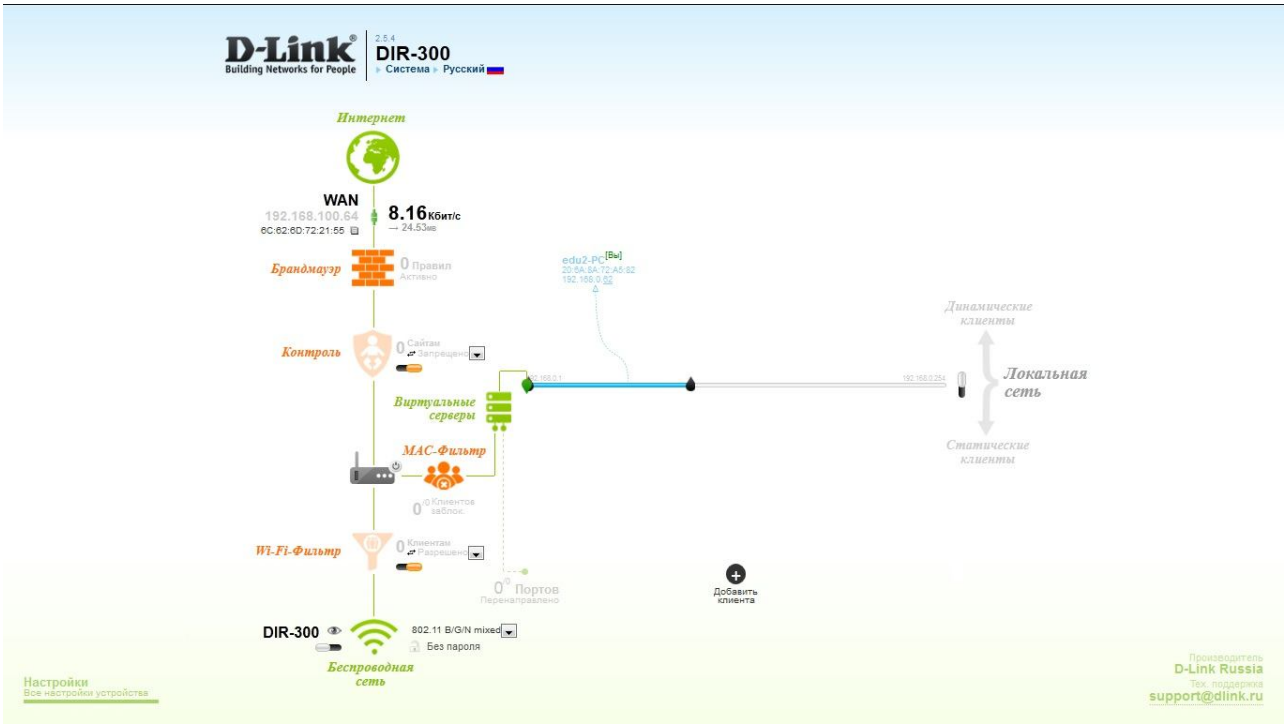


Рис. 4.18 Страница интерактивной конфигурации

Для упрощения управления несколькими сетевыми устройствами D-Link предлагает различные утилиты управления. Так, например, для управления несколькими коммутаторами D-Link серии EasySmart с одного компьютера можно использовать утилиту SmartConsole. Утилиту можно установить с компакт-диска, который входит в комплект поставки оборудования.

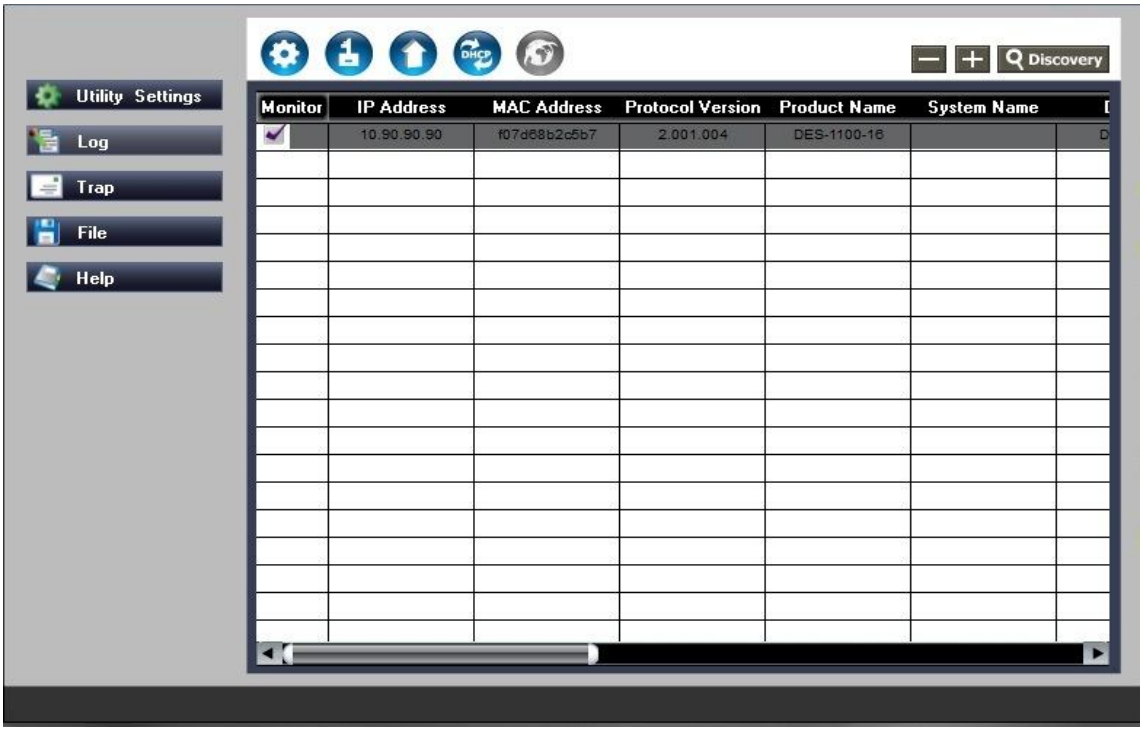


Рис. 4.19 Окно утилиты SmartConsole

Доступ к интерфейсу командной строки устройства осуществляется путем подключения к его консольному порту персонального компьютера с установленной программой эмуляции терминала. Надо отметить, что не все устройства имеют консольный порт. Обычно им оснащаются управляемые коммутаторы и маршрутизаторы, предназначенные для сетей SMB (Small-to-Medium Business). Этот метод доступа наиболее удобен при первоначальном подключении к коммутатору или маршрутизатору, когда IP-адрес не известен или не настроен, в случае необходимости восстановления пароля и при выполнении расширенных настроек устройства. Также доступ к интерфейсу командной строки может быть получен по сети с помощью протокола Telnet.

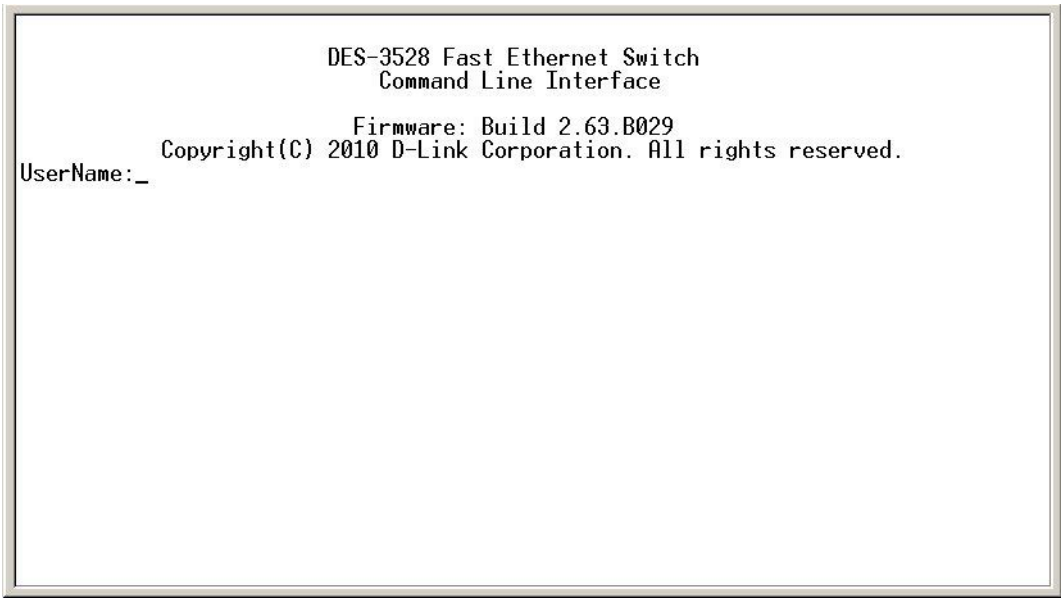


Рис. 4.20 Первоначальное окно интерфейса командной строки

Еще один способ управления сетевыми устройствами – использование протокола SNMP (Simple Network Management Protocol). Протокол SNMP является протоколом 7 уровня модели OSI и разработан специально для управления и мониторинга сетевых устройств путем обмена управляющей информацией между агентами, располагающимися на сетевых устройствах, и менеджерами, расположенными на станциях управления.

Следует отметить возможность обновления программного обеспечения сетевого оборудования. Благодаря этой функции обеспечивается длительный срок эксплуатации устройств, так как при обновлении ПО добавляются новые функции или устраняются имеющиеся ошибки. Компания D-Link распространяет новые версии ПО бесплатно. Они доступны на FTP-сервере компании ftp.dlink.ru.

4.3 Обзор сетевых топологий

4.3.1 Топология «шина»

В сети с **топологией «шина»** (*bus*) все узлы (компьютеры, серверы, периферийные устройства) подключаются к одному кабелю. Этот кабель называется *магистралью сети* или *сегментом*. Данные, отправленные в такую сеть узлом-отправителем, передаются по шине в обе стороны всем узлами сети, однако обрабатывает их только тот узел, чей адрес совпадает с адресом назначения, указанным в передаваемом сообщении. Остальные узлы сети сообщение отбрасывают.

Шина является разделяемой средой передачи, поэтому в каждый момент времени только один узел может осуществлять передачу данных. Прежде чем начать передачу

данных узел должен удостовериться, что линия связи свободна. Если она занята, узел должен отложить передачу до ее освобождения. В том случае, если два или более узла одновременно начнут передачу, возникнет коллизия, что приведет к повреждению передаваемых данных. Тогда узлы будут вынуждены приостановить передачу и повторно через разные промежутки времени передавать данные.

Сети топологии «шина» требуют обязательного наличия *терминаторов* на концах кабеля, которые предотвращают отражение сигналов от его концов, приводящее к возникновению коллизий.

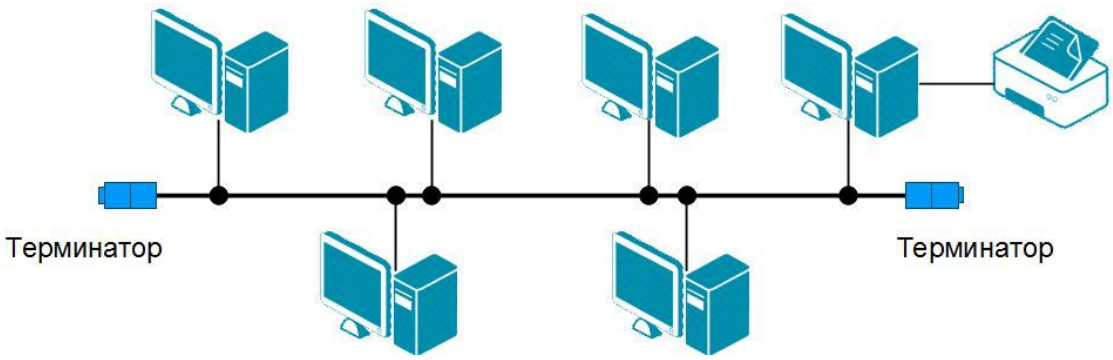


Рис. 4.21 Сеть с топологией «шина»

Несмотря на то, что топология «шина» характеризуется простотой реализации и дешевизной, она имеет ряд существенных недостатков:

- В сетях топологии «шина » существуют ограничения на длину кабеля и количество подключаемых к нему устройств.
- Поскольку шина используется совместно, при увеличении количества узлов, подключенных к ней, увеличивается количество коллизий, что уменьшает общую производительность сети и замедляет ее работу.
- Так как в сетях топологии «шина» используется один кабель, соединяющий узлы, то он является «единой точкой отказа». В случае обрыва любого участка кабеля нарушается работа всей сети.
- Для предотвращения отражения сигналов, передаваемых по шине, требуется использование терминаторов на концах кабеля.
- Существуют сложности при добавлении новых устройств, обнаружении неисправностей в сети.

Топология «шина» использовалась в сетях Ethernet 10BASE2 и 10BASE5 на основе коаксиального кабеля. В настоящее время шинную топологию имеют сети, построенные на основе электропроводки (PLC). Однако в традиционных локальных сетях топологии «шина» уже практически не используются.

4.3.2 Топология «кольцо»

В **топологии «кольцо»** (*ring*) каждый из узлов (рабочая станция, сервер, периферийное устройство) соединяется с двумя другими так, чтобы от одного он получал информацию, а второму передавал ее до тех пор, пока данные не будут получены узлом-приемником. Последний узел подключается к первому, замыкая кольцо. В сетях с топологией «кольцо» каждый узел выступает в роли повторителя, усиливая сигнал, что позволяет строить сети большой протяженности. В отличие от топологии «шина», в топологии «кольцо» передача данных осуществляется в одном направлении, последовательно от узла к узлу.

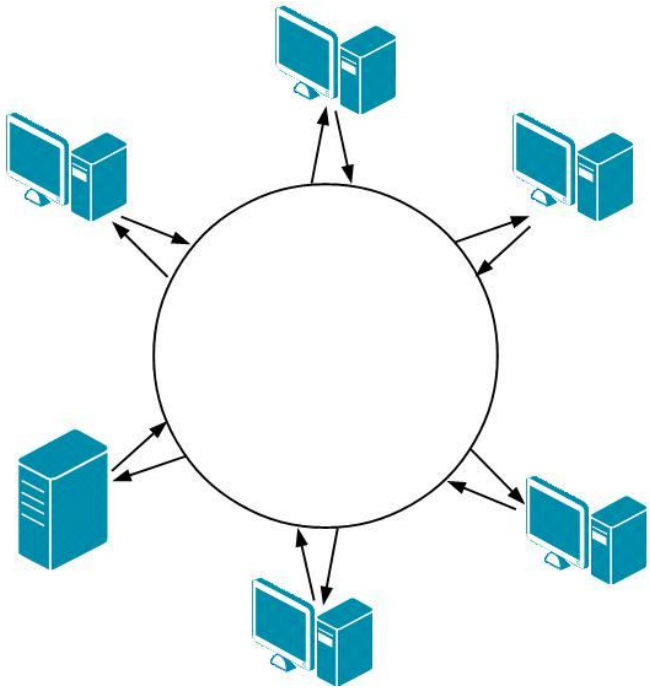


Рис. 4.22 Сеть с топологией «кольцо»

Топологии «кольцо» также как и топологии «шина» присущи достоинства и недостатки. К достоинствам можно отнести:

- Равные возможности доступа узлов к среде передачи, благодаря чему ни один из них не может ее монопольно захватить.
- Не требуются терминаторы.
- Не возникают коллизии.
- Можно строить сети большой протяженности.

К недостаткам этой топологии можно отнести:

- Низкая производительность сети. В зависимости от количества узлов в сети, время передачи данных может быть достаточно большим, поскольку сигнал должен пройти последовательно через все узлы, каждый из которых проверяет, не ему ли адресована информация.
- Невысокая надежность сети. Выход из строя хотя бы одного из узлов и/или обрыв кабеля приводит к полной неработоспособности сети. Чтобы избежать остановки работы сети при выходе из строя узла или обрыве кабеля, обычно используют двойное кольцо, что приводит к существенным финансовым затратам.
- Сложность расширения сети. Добавление в сеть нового узла часто требует ее остановки, что нарушает работу всех других узлов.

Для создания сетей с кольцевой топологией использовались такие технологии канального уровня как Token Ring и FDDI (Fiber Distributed Data Interface). Однако из-за значительных недостатков, сети на основе топологии «кольцо» в настоящее время практически не используются.

4.3.3 Последовательное соединение

Последовательное подключение (*daisy chain*) является одной из простейших топологий, если не считать топологию «шина». Существует два вида последовательного подключение: *линейное* (linear daisy chain) и *кольцевое* (ring daisy chain).

При **линейном** или **цепочечном подключении** (встречаются также названия «цепочка», «гирлянда») каждое устройство соединяется с предыдущим и следующим линией

связи «точка-точка» (т.е. отдельным кабелем), но самое первое и самое последнее устройства не соединяются.

Рис. 4.23 Линейное последовательное подключение

К достоинствам линейного подключения можно отнести простоту, небольшой расход кабеля и возможность использовать недорогого оборудования. Однако, несмотря на это оно имеет следующие недостатки:

- выход из строя любого устройства или обрыв кабеля приводят к разрыву цепочки и недоступности обслуживания пользователей из-за изоляции частей сети друг от друга;
- чем длиннее цепочка, тем больше времени требуется на доставку сообщений по ней, затрудняется поиск неисправностей и обслуживание сети.

Кольцевое подключение (или «кольцо») получается из линейного, если соединить самое первое и самое последнее устройство.

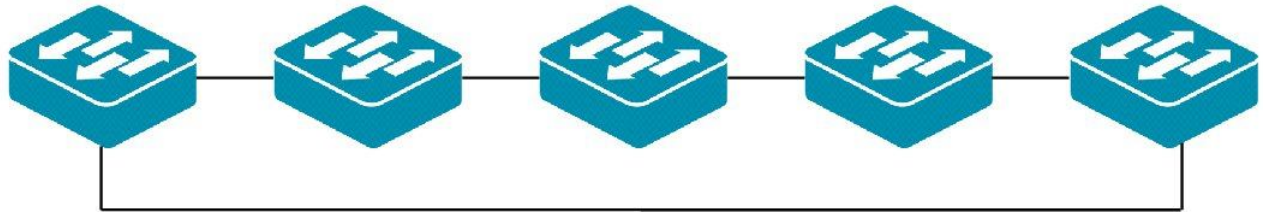


Рис. 4.24 Кольцевое последовательное подключение

Кольцевое подключение надежнее линейного, т.к. не имеет единой точки отказа. Даже если какое-то устройство выйдет из строя или будет поврежден кабель, сеть сохранит свою целостность и продолжит функционировать, т.к. до каждого устройства сети имеется два маршрута.

К недостаткам этой топологии можно отнести следующее:

- в сети требуется использование устройств, программное обеспечение которых поддерживает работу в замкнутых контурах;
- высокая стоимость и сложность настройки оборудования;
- сложность поиска неисправностей и обслуживания сети;
- при выходе из строя двух и более устройств, работоспособность сети будет нарушена.

Рассмотренные топологии часто применяются в сетях доступа провайдеров услуг, построенных на коммутаторах Ethernet. Линейную топологию используют в основном небольшие начинающие провайдеры, т.к. она не требует больших финансовых затрат, высокой квалификации персонала и хорошо адаптируется к городской застройке. Однако по мере роста сети и увеличения количества клиентов, сеть с линейным подключением будет неэффективна.

Кольцевое подключение является надежным благодаря избыточным связям между устройствами, поэтому оно часто используется в сетях доступа средних и крупных провайдеров.

При объединении коммутаторов в кольцо следует помнить, что *они не могут правильно функционировать в сетях с замкнутыми контурами*. Поэтому программное

обеспечение коммутаторов должно поддерживать специальные протоколы, обеспечивающие их работу в сетях с избыточными маршрутами. Это протоколы *Spanning Tree Protocol* (STP или его усовершенствованные версии RSTP и MSTP) и/или *Ethernet Ring Protection Switching* (ERPS). Задачей таких протоколов является логическое преобразование кольцевой топологии в линейную с возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода из строя активных каналов.

Подробнее работа протокола STP будет описана в главе 6.

4.3.4 Топология «звезда»

Топология «звезда» (*star*) – одна из самых распространенных топологий компьютерных сетей. Чаще всего она используется в локальных сетях небольших офисов или домашних сетях. В этой топологии все узлы подключаются отдельным кабелем к центральному устройству, в качестве которого в современных сетях может использоваться коммутатор или маршрутизатор. Обмен данными между узлами осуществляется через центральное устройство, которое выполняет и контролирует функции, реализованные в сети, а также усиливает проходящие через него сигналы.

В качестве основных преимуществ топологии «звезда» можно отметить:

- Простоту обслуживания и устранения неисправностей в сети, а также простоту подключения новых устройств.
- Защищенность сети. В качестве центрального устройства может использоваться сетевое оборудование с развитыми функциями безопасности, которое обеспечивает контроль потоков проходящего через него трафика. Помимо этого можно физически ограничить доступ к центральному устройству, поместив его в безопасное место.
- Возможность использования кабелей различных типов для подключения узлов к центральному устройству, если оно оборудовано портами различных типов (оптическими, медными).
- Возможность использования недорого оборудования.

Основными недостатками топологии является:

- Наличие единой точки отказа. Выход центрального устройства из строя приведет к неработоспособности всей сети.
- Для подключения устройств требуется большое количество кабеля.
- Количество устройств, которые могут быть объединены в сеть, ограничено количеством портов центрального устройства.

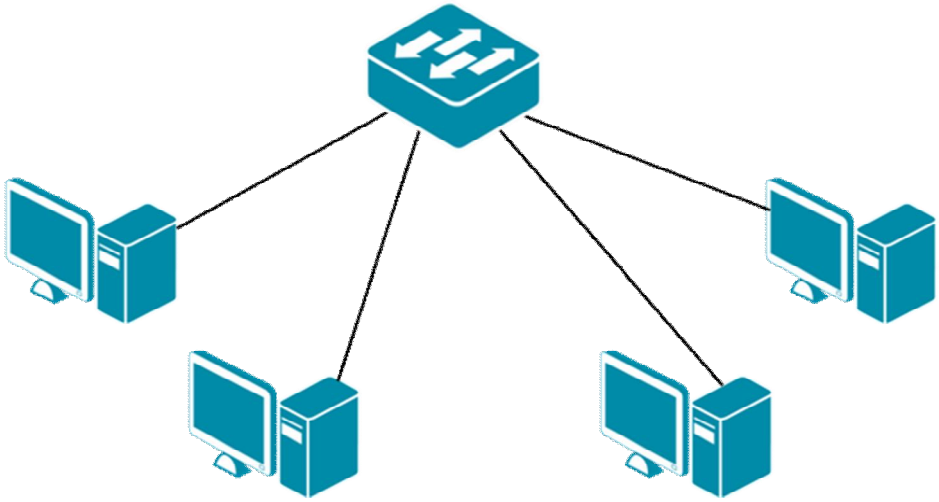


Рис. 4.25 Сеть с топологией «звезда»

Прежде чем дальше продолжить рассмотрение сетевых топологий сделаем небольшое отступление. Небольшие сети, как правило, создаются на основе одной из базовых топологий – линейного, кольцевого или звездообразного подключения. Для крупных сетей характерно наличие произвольных связей между узлами, т.к. они постоянно расширяются и модернизируются. В таких сетях можно выделить отдельные, произвольно связанные сегменты, имеющие одну из типовых топологий. Так как топология крупных сетей представляет собой комбинацию нескольких базовых топологий, то такие сети называют сетями со *смешанной* или *гибридной* топологией.

4.3.5 Топология «дерево»

Топология «дерево» *(tree)* или как ее еще называют **«расширенная звезда»** (*extended star*) создается на основе комбинации топологий «звезда» и линейного подключения. Эта топология реализует иерархию узлов. На самом верхнем уровне иерархии находится центральное устройство, которое объединяет между собой центральные устройства отдельных «звезд» линиями связи «точка-точка». Уровней иерархии может быть несколько.

Топология «дерево» является самой распространенной топологией современных компьютерных сетей. Наиболее часто она используется в сетях средних и крупных предприятий, сетях провайдеров услуг.

В качестве основных преимуществ этой топологии можно выделить:

- Возможность масштабируемости и расширяемости сети.
- Возможность деления большой сети на сегменты (отдельные «звезды»), что упрощает обслуживание и управление сетью.
- Неисправности в одном сегменте не влияют на работоспособность остальных сегментов.

Недостатки топологии «дерево» следующие:

- При увеличении количества сегментов сети усложняется ее обслуживание, и управление, а также поиск и устранение неисправностей.
- Высокая стоимость оборудования и необходимость большого количества кабеля.
- Требуется высококвалифицированный персонал.

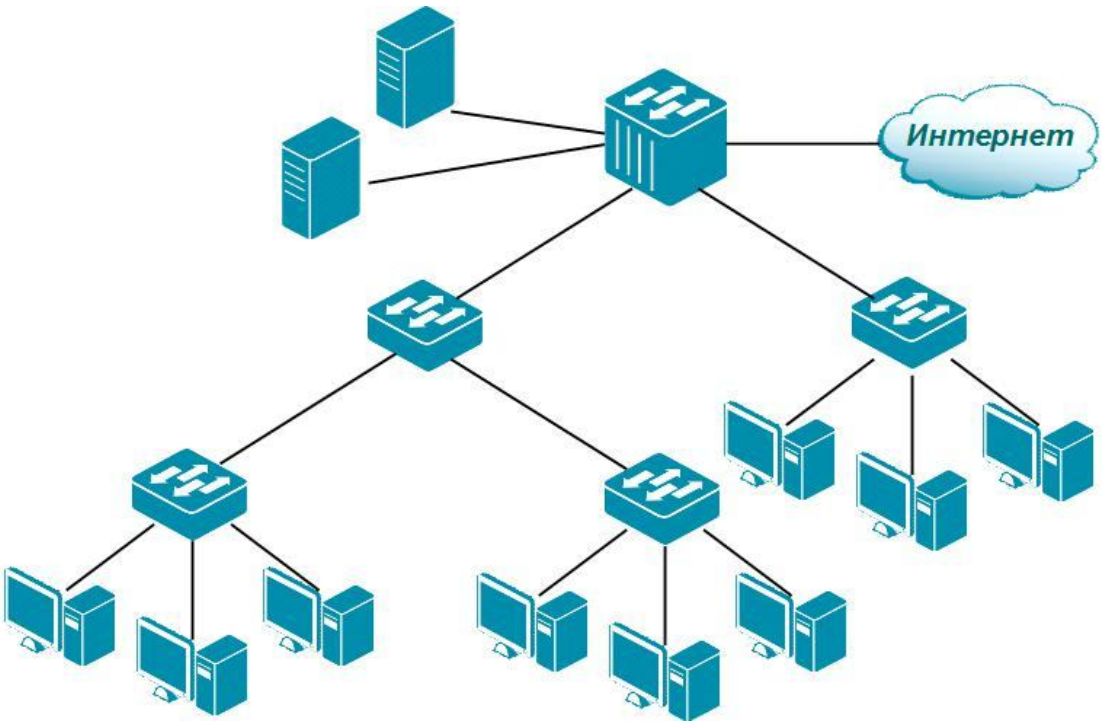


Рис. 4.26 Сеть с топологией «дерево»

4.3.6 Ячеистая топология

Ячеистая *(*также известна как *сетчатая, сеточная)* **топология** *(mesh)* – это тип сетевой топологии, в которой каждое устройство соединено с множеством других каналами связи «точка-точка», при этом устройство не только захватывает и обрабатывает свои данные, но и служит ретранслятором сообщений для других устройств. Эта топология характеризуется высокой надежностью и отказоустойчивостью, благодаря наличию множества резервных связей между узлами сети. Неисправность узла или обрыв линии связи не влияют на работоспособность сети (при обрыве одного из каналов связи возможна передача через другие). Для того чтобы найти наилучший путь передачи данных между узлами ячеистой сети используются маршрутизаторы или коммутаторы.

Существует два типа ячеистых топологий: **полносвязная топология** (*full connected*) и **топология неполной связности** *(partially connected)*.

В полносвязной топологии каждый узел напрямую связан со всеми остальными узлами сети. Эта топология отражает архитектуру Интернет, в котором имеется множество путей до любой точки. Полносвязная топология довольно дорогостоящая, т.к. требует большого расхода кабеля и большого количества портов для подключения, но в тоже время обеспечивает высокую отказоустойчивость. На практике она используется редко и применяется там, где требуется обеспечение высокой надежности и максимальной отказоустойчивости, например при построении магистральных сетей.

Топология неполной связности получается из полносвязной путем удаления некоторых возможных связей. В этой топологии количество соединений каждого устройства зависит, прежде всего, от его значимости в сети. Топология неполной связности менее дорогостоящая, чем полносвязная и характерна для большинства периферийных сетей, используемых для подключения к магистральным сетям с полносвязной топологией.

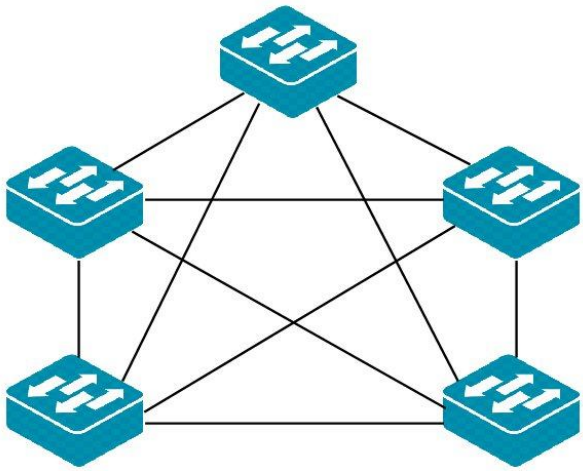


Рис. 4.27 Сеть с полносвязной ячеистой топологией

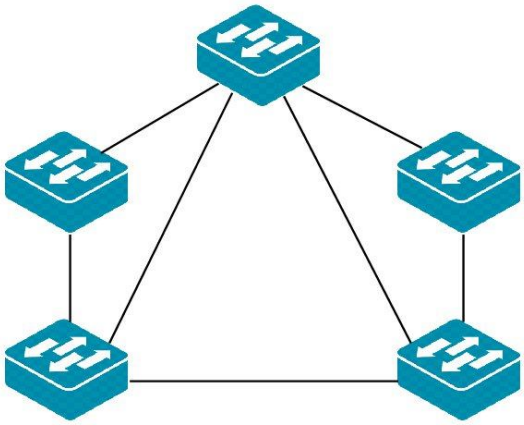


Рис. 4.28 Сеть с ячеистой топологией неполной связности

Несмотря на очевидное достоинство сетей с ячеистой топологией, основными их недостатками являются высокая стоимость, сложность подключения/отключения сетевого оборудования и его конфигурация.

Часто ячеистая топология используется совместно с другими топологиями («цепочка», «кольцо» и «звезда») и формирует сеть с гибридной топологией.

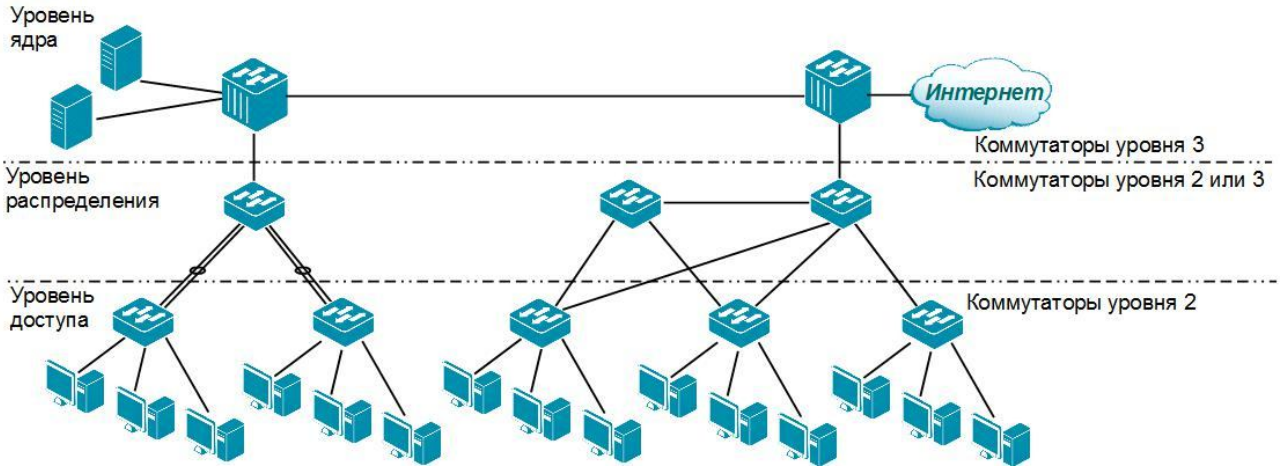


Рис. 4.29 Пример сети с гибридной топологией

Рассмотрев существующие сетевые топологии, обратим внимание на другие немаловажные вопросы, влияющие на выбор топологии сети. Топология должна обеспечивать:

- удобное управление потоками данных;
- устойчивость к неисправностям узлов, подключенных к сети и обрывам кабеля;
- возможность для дальнейшего расширения сети и перехода к новым высокоскоростным технологиям;
- низкую стоимость создания и сопровождения сети.

При этом надо учитывать:

- уже имеющуюся кабельную инфраструктуру и оборудование, если сеть требуется просто расширить;
- физическое размещение устройств;
- размеры планируемой сети;
- объем и тип информации для совместного использования.

5 Канальный уровень модели OSI

Канальный уровень *(Data link layer)* является вторым уровнем модели OSI, который расположен между физическим уровнем и сетевым уровнем. Он обеспечивает передачу данных, полученных от вышележащего сетевого уровня, через физический уровень между непосредственно подключенными устройствами.

Канальный уровень выполняет следующие функции:

- управление доступом к среде передачи;
- управление потоком данных;
- физическая (аппаратная) адресация;
- формирование кадров;
- достоверность принимаемых данных;
- адресация протокола верхнего уровня.

Функционирование канального уровня определяется его протоколом. Примерами протоколов канального уровня могут служить семейство протоколов Ethernet IEEE 802.3, протоколы беспроводных сетей IEEE 802.11.

На канальном уровне работают следующие устройства:

- сетевые адаптеры;
- медиаконвертеры с интеллектуальными функциями;
- коммутаторы;
- точки доступа.

5.1 Методы коммутации

В предыдущих главах разбирались вопросы, связанные с тем, как соединить множество устройств и организовать между ними взаимодействие, если они расположены в разных местах. Вы познакомились с основными сетевыми топологиями и узнали, что для того чтобы соединить каждый узел напрямую со всеми остальными узлами сети нужно использовать полносвязную ячеистую топологию. Однако, несмотря на максимальную отказоустойчивость, эта топология довольно дорогостоящая. На практике часто приходится выполнять передачу потоков данных от множества пользователей, используя общую среду передачи. Так в самой распространенной топологии локальных сетей «расширенная звезда» линии связи между абонентскими устройствами (компьютерами, серверами, принтерами) и устройством связи (коммутатором, маршрутизатором) являются индивидуальными, а между устройствами связи – разделяемыми, т.к. по ним передается трафик разных абонентских устройств. Для того чтобы по одному кабелю могло параллельно передаваться множество сигналов от разных пользователей используют методы мультиплексирования. Устройство связи в этом случае должно уметь определять направление передачи данных, т.е. выполнять *коммутацию (switching*).

Методы синхронного и асинхронного мультиплексирования с разделением по времени (TDM) легли в основу двух базовых принципов коммутации в компьютерных сетях:

- коммутации каналов (circuit switching);
- коммутации пакетов (packet switching).

5.1.1 Коммутация каналов

Коммутация каналов основана на синхронном TDM. Она предоставляет каждой паре взаимодействующих абонентов последовательность каналов (логических) для монопольного использования.

В сетях с коммутацией каналов абонентам могут быть предоставлены *коммутируемые* и *некоммутируемые* каналы.

Каналы связи, передача данных по которым возможна только после установления соединения между взаимодействующими системами, называются **коммутируемыми** или **временными**. При этом канал будет существовать только в течение сеанса связи, т.е. времени, требуемого для передачи данных. По окончании сеанса связи соединение разрывается, и канал освобождается. Коммутация выполняется только в начале сеанса связи. Для этого устройство-инициатор сеанса формирует и посылает ближайшему к ней узлу связи запрос на прокладку через сеть последовательности каналов, которая свяжет его с устройством-адресатом. Преимуществом коммутируемых каналов является небольшая стоимость. К их недостаткам можно отнести большое время ожидания соединения и возможность блокировки («занято»).

Классическим примером реализации коммутируемых каналов является телефонная связь, которая подразумевает, что абонент перед началом разговора набирает номер второго абонента, в результате чего последовательное переключение промежуточных коммутаторов позволяет образовать непрерывный канал связи между абонентами. При этом следует учесть, что канал остается занятым все время соединения, т.е. ни одному, ни другому абоненту дозвониться невозможно. После разговора соединение разрывается и канал освобождается.

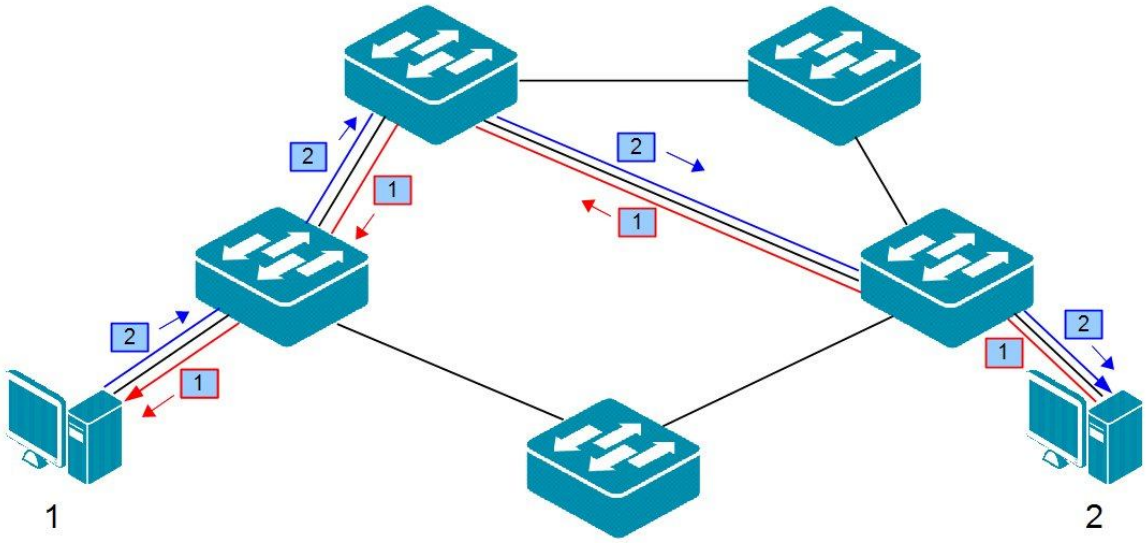


Рис. 5.1 Коммутация каналов

Каналы между конечными системами, которые доступны для передачи данных на длительное время за счет постоянно существующего соединения с заданными характеристиками, называются **выделенными** или **некоммутируемыми**. Выделенные каналы также называются *арендуемыми*. Эти каналы постоянно готовы к передаче данных. Однако их стоимость выше стоимости коммутируемых каналов.

Напомним, что в синхронном TDM время работы физического канала делится на повторяющиеся циклы, состоящие из кадров TDM. Каждый кадр TDM начинается с синхронизирующей последовательности и включает n тайм-слотов одинаковой длительности, по одному на каждый логический канал. Тайм-слоты назначаются всем, подключенным к устройству связи входным каналам, нумеруются и располагаются в кадре TDM в строго определенном порядке. Входные каналы по очереди передают блоки данных одинакового размера в течение выделенных им в каждом цикле тайм-слотов для того чтобы

устройство связи на другом конце канала могло корректно считать их и направить соответствующим адресатам.

Для этого устройство связи должно хранить в памяти таблицу коммутации, которая определяет отношения между:

- входящим абонентским портом и исходящим магистральным портом/тайм-слотом источника;
- входящим магистральным портом/тайм-слотом и исходящим магистральным портом/ тайм-слотом транзитного устройства связи (если передача ведется через транзитные узлы);
- входящим магистральным портом/тайм-слотом и исходящим абонентским портом приемника.

Т.к. взаимодействующие системы получают в каждом цикле тайм-слот с одним и тем же номером, передаваемые блоки данных появляются на приемной стороне через одинаковые промежутки времени и приходят с одним и тем же временем запаздывания. Поэтому сети с коммутацией каналов хорошо подходят для передачи голосового трафика или трафика видеоконференций.

Одним из основных недостатков сетей с коммутацией каналов является неэффективное использование полосы пропускания. Во время сеанса связи последовательность используемых каналов загружена потоками битов относительно небольшое время. Остальное время каналы простаивают.

5.1.2 Коммутация пакетов

Технология **коммутации пакетов** основана на использовании асинхронного или статистического TDM. Она позволяет конечным системам передавать данные через сеть без монопольного использования каналов, т.е. ни один из каналов не занимается парой абонентских систем даже на время сеанса связи. Передаваемые по сети сообщения разбиваются на небольшие блоки, называемые *пакетами* (*packet*). Пакеты передаются по одному и тому же каналу связи по мере их поступления независимо от их источников и адресатов. Взаимодействующие системы занимают канал только на время передачи пакета.

Напомним, что в отличие от синхронного TDM, в асинхронном TDM нет четкой привязки между тайм-слотом и устройством назначения, поэтому в сетях с коммутацией пакетов передаваемые блоки данных необходимо снабжать адресной информацией. Каждый пакет обычно состоит из двух частей – *заголовка*, содержащего служебные данные, необходимые для управления доставкой пакета (адресную информацию, порядковый номер и т.д.), и *данных*, подлежащих передаче. Порядок обмена пакетами, их размер, а также конкретный состав их заголовка определяется соответствующим сетевым протоколом, поэтому в отличие от синхронного TDM, асинхронный TDM не является прозрачным для протоколов. В сетях с коммутацией пакетов требуется, чтобы абонентские устройства и устройства связи (коммутаторы, маршрутизаторы) поддерживали одни и те же протоколы.

Термин «пакет» в данном случае дал название технологии и является общим термином, который используется для обозначения передаваемого блока данных. На канальном уровне блок данных называется кадром, на сетевом – пакетом или дейтаграммой, на транспортном – сегментом.

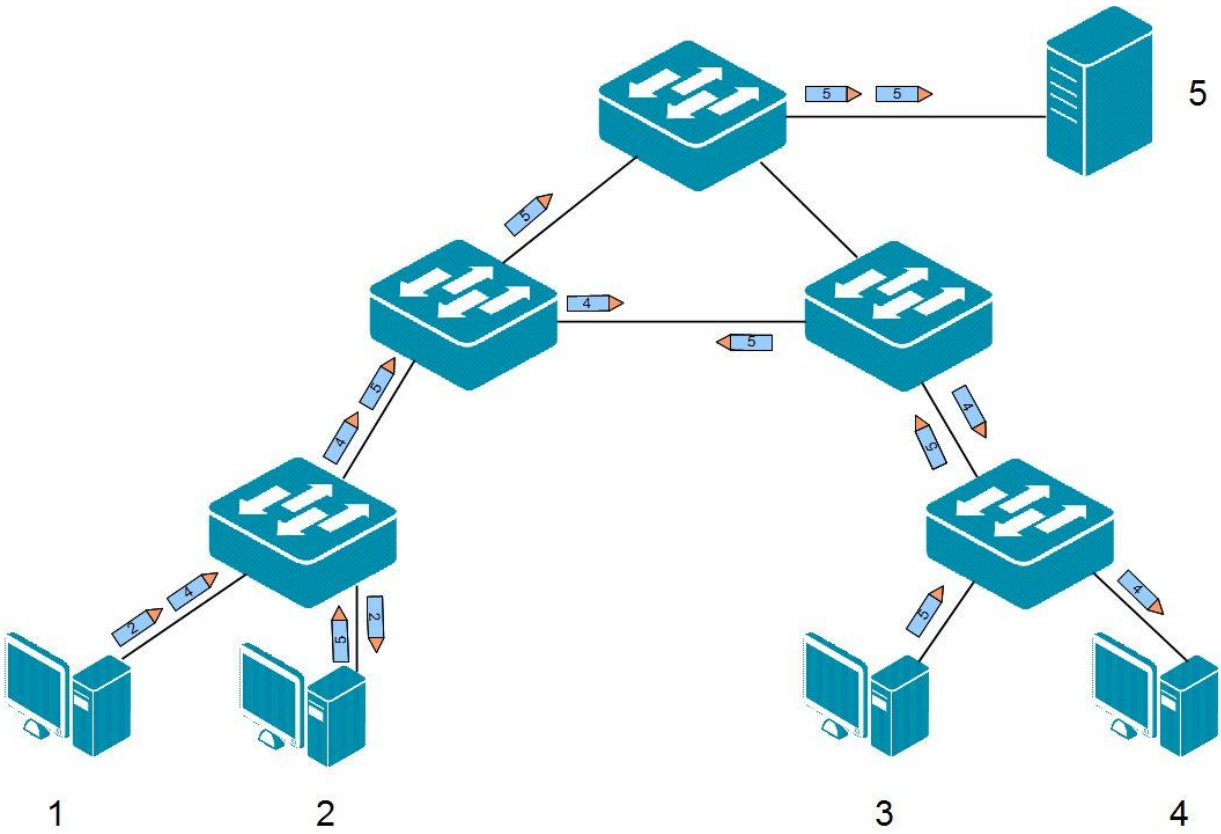


Рис. 5.2 Коммутация пакетов

Для повышения надежности сети с коммутацией пакетов, а также обеспечения распределения нагрузки, ее топология должна обеспечивать несколько путей передачи пакетов между взаимодействующими системами, т.е. между устройствами связи должны быть проложены резервные каналы. Устройства связи на основе адресной информации направляют пакеты по тем последовательностям каналов, которые в итоге позволяют достичь устройства-адресата. Устройство-адресат собирает поступившие пакеты в нужном порядке и формирует сообщение.

Устройства связи пакетной сети (коммутаторы, маршрутизаторы) отличаются от устройств сети с коммутацией каналов тем, что имеют внутреннюю буферную память. Она используется для временного хранения поступивших пакетов, когда их невозможно немедленно передать на выходной порт. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта и ожидает когда дойдет его очередь на передачу. Для предотвращения переполнения буферов коммутаторов или маршрутизаторов используются специальные *методы управления потоком* (*flow control*).

Обычно буферизированные пакеты передаются через выходной порт устройства в том порядке, в котором они поступили, т.е. «первым пришел, первым ушел» (FIFO, First Input, First Output). Однако можно применять приоритеты, обеспечивая *качество обслуживания* (*Quality of Service*, QoS). В этом случае пакеты с более высоким приоритетом будут передаваться первыми.

Прежде чем принять решение о передаче пакета, устройство связи получает и анализирует его содержимое. В современных устройствах используются следующие методы коммутации, определяющие их поведение при получении пакета:

- коммутация с промежуточным хранением (store-and-forward);
- коммутация без буферизации (cut-through).

Метод *коммутации с промежуточным хранением* исторически появился первым. Он заключается в том, что принятый пакет, прежде чем он будет передан, полностью копируется в буфер устройства и проверяется на наличие ошибок. Если имеются ошибки, пакет

отбрасывается. Если ошибок нет, устройство связи с помощью специальной таблицы определяет выходной порт, через который пакет будет передан.

При *коммутации без буферизации* устройство связи копирует в буфер только адрес назначения и сразу начинает передавать пакет (предварительно определив выходной порт с помощью специальной таблицы), не дожидаясь его полного приема. Устройство связи при работе в этом режиме не выполняет проверку пакета на наличие ошибок, но коммутация выполняется быстрее, что уменьшает задержку передачи блоков данных (особенно больших). Однако в некоторых случаях, метод cut-through теряет свои преимущества в скорости передачи. Это может произойти, например, при перегрузке сети (переполнении приемных буферов сетевых устройств).

Коммутация пакетов основана на таблицах, которые хранятся в памяти и содержат информацию, позволяющую определить путь до места назначения пакета.

В зависимости от используемой технологии можно выделить два типа таблиц:

- таблицы коммутации (*Forwarding DataBase, FDB*);
- таблицы маршрутизации (*Routing table*).

Таблицы маршрутизации хранятся на маршрутизаторах (коммутаторах 3 уровня) и позволяют им принимать решение о том, куда передавать пакет на основе его адреса назначения сетевого уровня. Этот процесс называется *маршрутизацией* (*routing*) и выполняется он на сетевом уровне модели OSI. Маршрутизация позволяет передавать данные узлам, находящимся в разных локальных сетях или подсетях одной локальной сети. Подробнее маршрутизация будет описана в главе 11.

Коммутаторы локальных сетей принимают решение о том, в каком направлении передавать кадр на основе *таблицы коммутации*. Для этого они анализируют адрес канального уровня, содержащийся в кадре. Построение таблицы коммутации будет описано в главе 6.

Так как коммутация выполняется быстрее маршрутизации, то коммутаторы 3 уровня могут выполнять маршрутизацию на основе таблиц коммутации 3 уровня (*L3 Forwarding DataBase*).

5.2 Сетевые протоколы и методы коммутации

Сетевые протоколы делятся на две категории по типу установления соединения:

- **Протоколы с установлением соединения** (*Connection-Oriented Protocol*): эти протоколы требуют установления логического соединения между двумя устройствами до начала передачи данных. Это обычно делается путем выполнения набора правил, которые определяют, как соединения должно инициироваться, управляться и завершаться. Обычно одно из устройств отправляет другому запрос на установление соединения. После получения ответа на запрос устройства начинают обмениваться управляющей информацией и определять параметры соединения. В случае успешного завершения этой фазы, между устройствами начинается передача данных. Когда данные будут переданы, устройства должны будут завершить соединение.
- **Протоколы без установления соединения** (*Connectionless Protocol*): эти протоколы не устанавливают соединение между устройствами. Как только у устройства появляются данные для передачи, оно сразу начинает их передавать.

Исходя из этой классификации, можно сделать вывод, что протоколы с установлением соединения используется только в сетях с коммутацией каналов, а протоколы без установления соединения в сетях с коммутацией пакетов. Этот вывод ошибочен. Несмотря на то, что сети с коммутацией каналов основываются на установлении соединения между взаимодействующими устройствами, в них используются не только протоколы с установлением соединения. Протоколы с установлением соединения обычно используются на верхних уровнях модели OSI в сетях с коммутацией пакетов и позволяют выполнять приложения, которые требуют установления логического соединения. В стеке протоколов

TCP/IP на транспортном уровне реализованы два важных протокола: TCP и UDP. Протокол TCP (Transmission Control Protocol) обеспечивает надежную доставку сегментов по сети за счет установления логического соединения между отправителем и получателем данных. Протокол UDP (User Datagram Protocol) не устанавливает соединение между отправителем и получателем сообщения и не гарантирует надежную доставку данных. Протокол TCP используется для приложений, которым требуется установка логического соединения, например, FTP (File Transfer Protocol) или Telnet. Протокол UDP используется приложениями, которым не требуется установка соединения, например, DNS (Domain Name System), IPTV, различные сетевые игры.

Однако, исходя из уровневой модели, не стоит думать, что протоколы с установлением соединения могут быть реализованы только поверх протоколов с установлением соединения и наоборот, протоколы без установления соединения могут быть реализованы только поверх протоколов без установления соединения.

На каждом уровне модели OSI могут быть реализованы как протоколы с установлением соединения, так и без установления соединения, поэтому возможны комбинации протоколов. Протокол с установлением соединения может быть реализован на основе протокола без установления соединения. Например, протокол TCP на сетевом уровне использует сервисы протокола IP, который является протоколом без установления соединения. Или протокол без установления соединения может быть реализован поверх протокола с установлением соединения на канальном уровне. Например, протокол IP поверх протокола ATM (Asynchronous Transfer Mode), который создает виртуальные каналы между отправителем и получателем перед передачей данных.

5.3 Протоколы канального уровня

Протоколы канального уровня определяют набор правил, позволяющих упорядочивать взаимодействие узлов, подключенных к одному сегменту сети.

Данные на канальном уровне рассматриваются как последовательный поток битов, и перед передачей по физическим каналам этот поток, в соответствии с принципом коммутации пакетов, разделяется на небольшие части, каждая из которых снабжается заголовком, содержащим некоторую служебную информацию, т.е. формируется *кадр* (*frame*). Структура заголовка кадра зависит от набора задач, которые решает данный конкретный протокол.

Протоколы канального уровня можно разделить на две группы:

- протоколы для соединений типа «точка-точка»;
- протоколы для сетей сложных топологий, к которым относятся локальные сети.

5.3.1 Структура кадра данных

Состав заголовка кадра зависит от многих факторов, определяемых набором функций, которые выполняет протокол. Можно выделить ряд информационных полей, которые обычно присутствуют в заголовке кадра.

Поле, определяющее начало кадра	Адрес отправителя и получателя	Информация о протоколе сетевого уровня	Данные (Data)	Контрольная сумма	Поле, определяющее конец кадра

Рис. 5.3 Структура кадра данных

1. Специальные поля, предназначенные для определения границ кадров. Поскольку в физической среде могут постоянно проходить какие-либо сигналы, то приемник должен уметь разбираться в том, когда начинается передача кадра и когда она заканчивается.

2. Поле, предназначенное для определения протокола сетевого уровня, которому необходимо передать данные. Так как на одном компьютере могут функционировать программные модули различных протоколов сетевого уровня, то протоколы канального уровня должны уметь распределять данные по этим протоколам.

3. Контрольная сумма (или специальный код) содержимого кадра, которая позволяет принимающей стороне определить наличие ошибок в принятых данных.

Для большинства протоколов канального уровня существует ограничение на максимально допустимый объем данных, передаваемых в одном кадре. Это ограничение вызвано различными техническими условиями. Характеристика, используемая для определения максимального размера блока данных (в байтах), который может быть передан на канальном уровне, называется *MTU (Maximum Transfer Unit, максимальная единица передачи данных)*.

Значение MTU может быть определено стандартом (например, для Ethernet), либо выбираться в момент установки соединения (обычно в случае подключений «точка-точка»).

5.4 Протоколы локальных сетей

Напомним, что локальная сеть (Local Area Network, LAN) – группа узлов, связанных друг с другом и расположенных на небольшом расстоянии друг от друга. Локальные сети были изобретены в 70-х годах 20 века. Первоначально среда передачи локальных сетей была общей (shared media). Все рабочие станции использовали для передачи одну и туже среду и имели равные права доступа к ней. Когда одна из станций отправляла данные, их получали все рабочие станции, подключенные к этой сети. Широковещательный характер передачи данных в локальной сети требовал управления доступом и адресации рабочих станций. В результате чего появились такие термины как «Media Access Conrol» (MAC, управление доступом к среде) и «MAC-адрес» (уникальный, но не структурированный адрес). Изначально не было необходимости в маршрутизации, поэтому для передачи данных в локальной сети было достаточно функционала 1 и 2 уровней модели OSI.

В 1980 г. в IEEE был организован комитет по стандартизации протоколов локальных сетей (IEEE 802 LAN/MAN Standards Committee, LMSC), в результате работы которого было принято семейство стандартов 802.x, которые содержат рекомендации по проектированию канального и физического уровней локальных сетей (LAN) и сетей мегаполисов (MAN).

За разработку каждого стандарта отвечает отдельная рабочая группа комитета. В настоящее время в комитете IEEE 802 активными являются следующие группы:

- 802.1 Higher Layer LAN Protocols
- 802.3 Ethernet
- 802.11 Wireless LAN
- 802.15 Wireless Personal Area Network (WPAN)
- 802.16 Broadband Wireless Access
- 802.18 Radio Regulatory TAG
- 802.19 Wireless Coexistence
- 802.21 Media Independent Handover Services
- 802.22 Wireless Regional Area Networks
- SG ECSG Smart Grid Executive Committee Study Group

Распущены группы:

- 802.2 Logical Link Control
- 802.4 Token Bus
- 802.5 Token Ring

Семейство стандартов IEEE 802 включает стандарты для сетей Ethernet, Token Ring, беспроводных сетей Wi-Fi, управления, безопасности, создания мостовых соединений.

Рис. 5.4 Уровневая модель IEEE 802

В спецификации IEEE 802 канальный уровень модели OSI был разбит на два подуровня:

- управление логическим каналом (Logical Link Control, LLC);
- управление доступом к среде передачи (Media Access Control, MAC).

Подуровень LLC обеспечивает взаимодействие с сетевым уровнем и предоставляет сервисы с установлением и без установления соединения. Этот подуровень не зависит от метода доступа к среде передачи.

Подуровень MAC описывает протоколы, реализующие различные методы доступа к среде передачи, отвечает за физическую адресацию, формирование кадров и обнаружение ошибок.

Физический уровень определяет электрические/оптические спецификации, механические интерфейсы, кодирование и синхронизацию битов и зависит от протокола подуровня MAC.

Рабочая группа IEEE 802.1 определяет стандарты, относящиеся к архитектуре сетей LAN/MAN, их взаимодействию, сетевому управлению и протоколам, расположенным выше подуровней MAC и LLC. Например, для сетей Ethernet, IEEE 802.1 определяет дополнительные функции, такие как мостовые соединения и Spanning Tree Protocol, включенные в стандарт IEEE 802.1D, виртуальные локальные сети (VLAN), описанные в стандарте IEEE 802.1Q , аутентификацию, определяемую стандартом IEEE 802.1X и другие.

5.4.1 Протокол LLC

Протокол LLC определен стандартом IEEE 802.2 и занимает промежуточное положение между протоколами сетевого уровня и протоколами подуровня MAC. LLC предоставляет сервисы протоколам сетевого уровня и взаимодействует с множеством протоколов MAC-подуровня (семейством протоколов Ethernet, Wi-Fi и др.). Он обеспечивает нужное качество транспортной службы для технологий локальных сетей, передавая кадры либо без установления соединения и подтверждения между узлами сети, либо с установлением соединения и подтверждением приема кадров.

Протокол LLC участвует в процессе инкапсуляции. Он помещает пакет сетевого уровня в свой кадр и добавляет адресную информацию спецификации IEEE 802.2:

- *адрес точки входа сервиса назначения* (Destination Service Access Point, DSAP) – указывает протокол верхнего уровня, которому надо передать данные для обработки;

- *адрес точки входа сервиса источника* (Source Service Access Point, SSAP) – указывает протокол верхнего уровня, данные которого пересылаются в кадре.
  В качестве примера можно привести следующие значения SAP:
  – 0x42 – Spanning Tree Protocol (IEEE 802.1D);
  – 0xAA – SNAP;
  – 0xE0 – Novell;
  – 0x06 – IP.

Поле управления служит для определения типа сервиса, используемого протоколами сетевого уровня: с установлением соединения и подтверждением приема; с установлением соединения и без подтверждения приема; без установления соединения и подтверждения приема; без установления соединения и с подтверждением приема.

Кадр LLC помещается в кадр MAC-подуровня, при этом флаги удаляются.

Флаг 01111110	Адрес точки входа сервиса назначения (DSAP)	Адрес точки входа сервиса назначения (SSAP)	Поле управления (Control)	Данные (Data)	Флаг 01111110

Рис. 5.5 Формат кадра LLC

Следует отметить, что реализация протокола LLC зависит от конкретного стека протоколов. В современных сетях функции протокола LLC обычно выполняются протоколами транспортного уровня, такими как TCP и UDP.

В настоящее время протокол LLC служит для идентификации протоколов верхнего уровня, пакеты которых пересылаются с помощью кадров протоколов MAC-подуровня семейства IEEE 802.

5.4.2 Подуровень MAC

Как было сказано ранее, *подуровень MAC* описывает протоколы, реализующие различные методы доступа к разделяемой среде, отвечает за физическую адресацию, формирование кадров и обнаружение ошибок.

На MAC-подуровне реализованы следующие протоколы локальных и городских сетей, которые получили широкое распространение:

- 802.3 – семейство протоколов Ethernet;
- 802.11 – семейство протоколов беспроводных локальных сетей;
- 802.15 – беспроводные персональные сети (WPAN), Bluetooth;
- 802.16 – беспроводная городская сеть, WiMAX.

Каждый протокол LAN/MAN семейства IEEE 802 содержит в кадре заголовок подуровня LLC.

5.4.3 Понятие MAC-адреса

Для обеспечения адресации узлов в локальной сети в заголовке кадров должны присутствовать адрес отправителя и адрес получателя. Большинство протоколов канального уровня семейства IEEE 802 для идентификации устройств используют физический адрес или *MAC-адрес* (MAC address).

MAC-адрес (Media Access Control) — это уникальный идентификатор, который присваивается каждому сетевому устройству во время изготовления. Он позволяет

уникально идентифицировать каждый узел сети и доставлять данные только этому узлу.

Стандарты IEEE определяют MAC-адрес, длиной 48 бит (6 октетов).

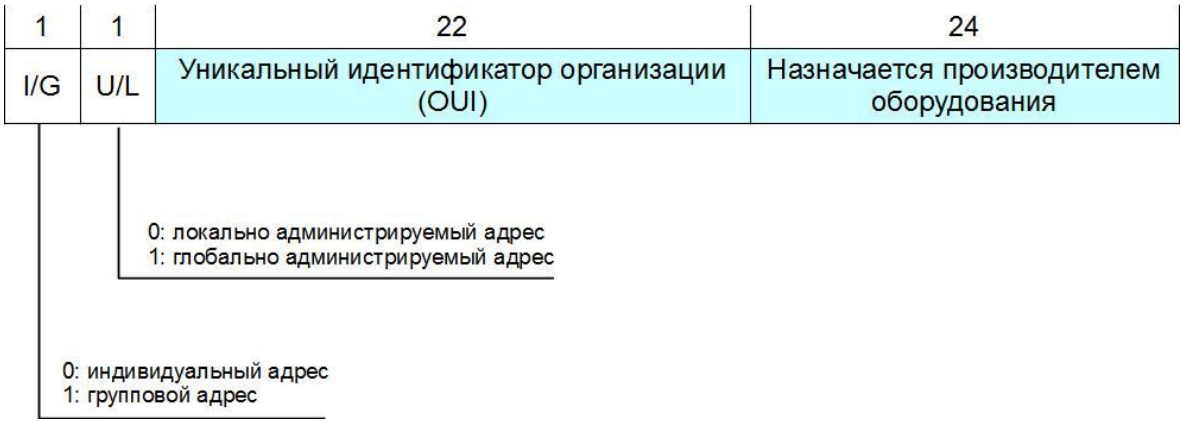


Рис. 5.6 Формат MAC-адреса

MAC-адрес можно разделить на две части. В первой части указывается *уникальный идентификатор производителя оборудования* (Organizationally Unique Identifier, OUI). Этот уникальный идентификатор присваивается производителю институтом IEEE. Старшие 24 бита MAC-адреса назначаются непосредственно производителем оборудования. Первый бит MAC-адреса (I/G) указывает, является ли адрес индивидуальным или групповым:

- 0 (индивидуальный) – адрес, ассоциированный с определенным сетевым устройством;
- 1 (групповой) – адрес, ассоциированный с несколькими или всеми узлами данной сети.

Существует два вида групповых адресов:

- *многоадресный* или *групповой* (*multicast*) – адрес, ассоциированный с группой узлов сети;
- *широковещательный* (*broadcast*) – адрес, ассоциированный со всеми узлами сети. Его значение – 0xFF-FF-FF-FF-FF-FF.

Второй бит MAC-адреса (U/L) указывает, является ли MAC-адрес глобально или локально администрируемым:

- 1 (глобально администрируемый MAC-адрес устройства) – он глобально уникален (администрируется IEEE) и обычно «зашит» в аппаратуру;
- 0 (локально администрируемый MAC-адрес) – он выбирается произвольно и может не содержать информации о производителе данного оборудования (OUI). Некоторые производители сетевых адаптеров поддерживают возможность изменять MAC-адрес устройства.

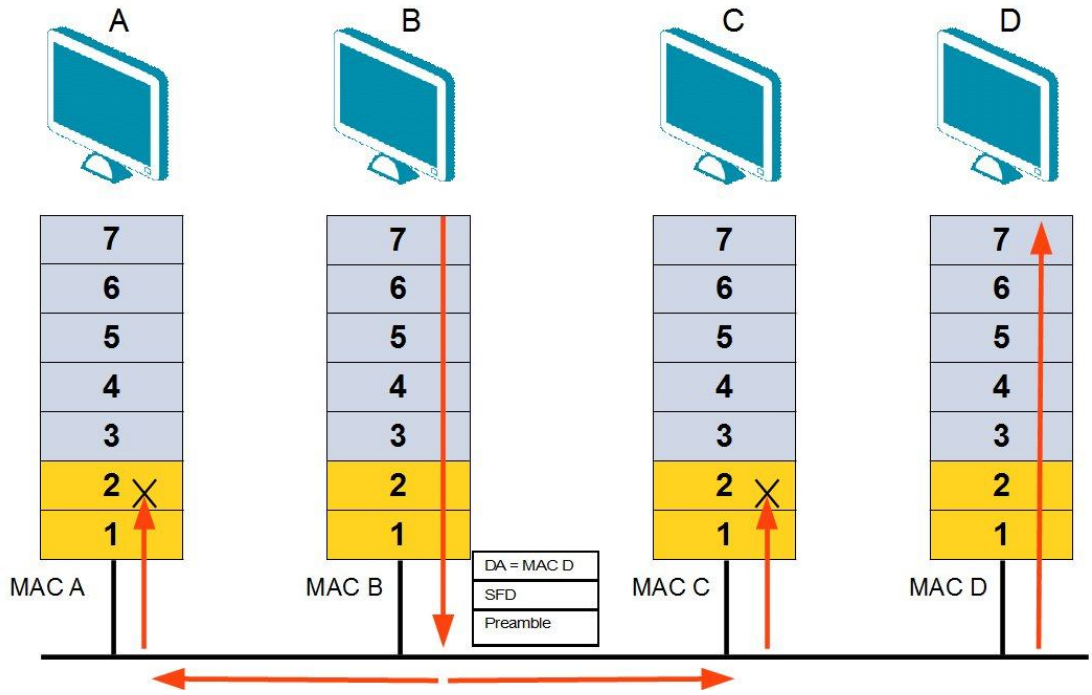


Рис. 5.7 Передача с использованием индивидуального MAC-адреса

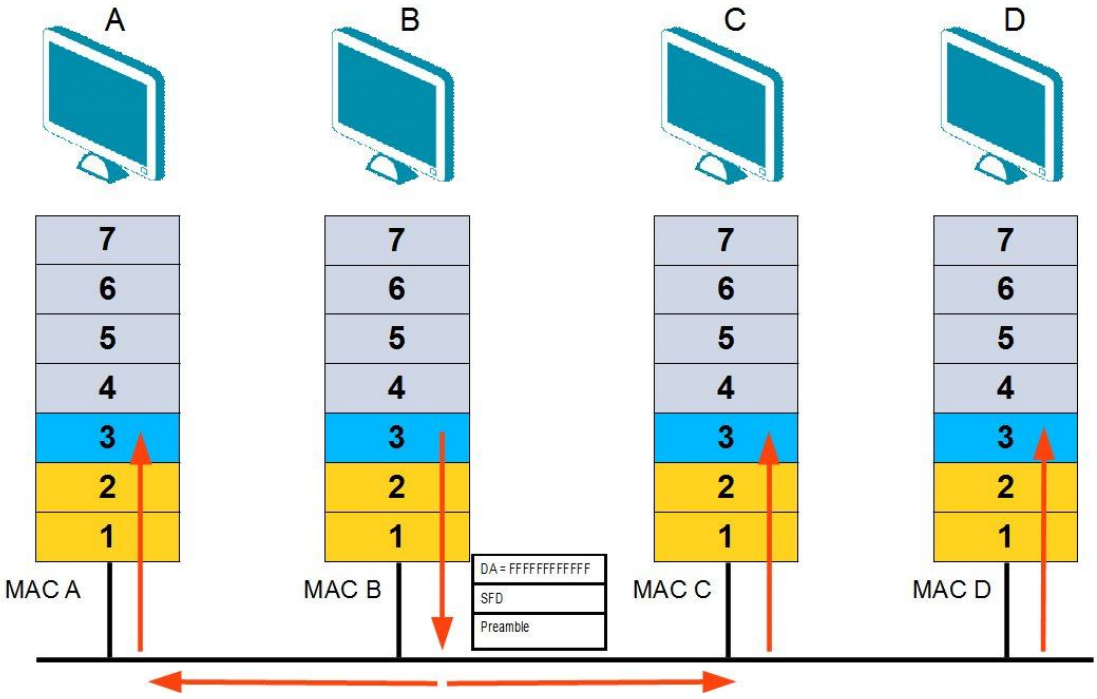


Рис. 5.8 Передача с использованием широковещательного MAC-адреса

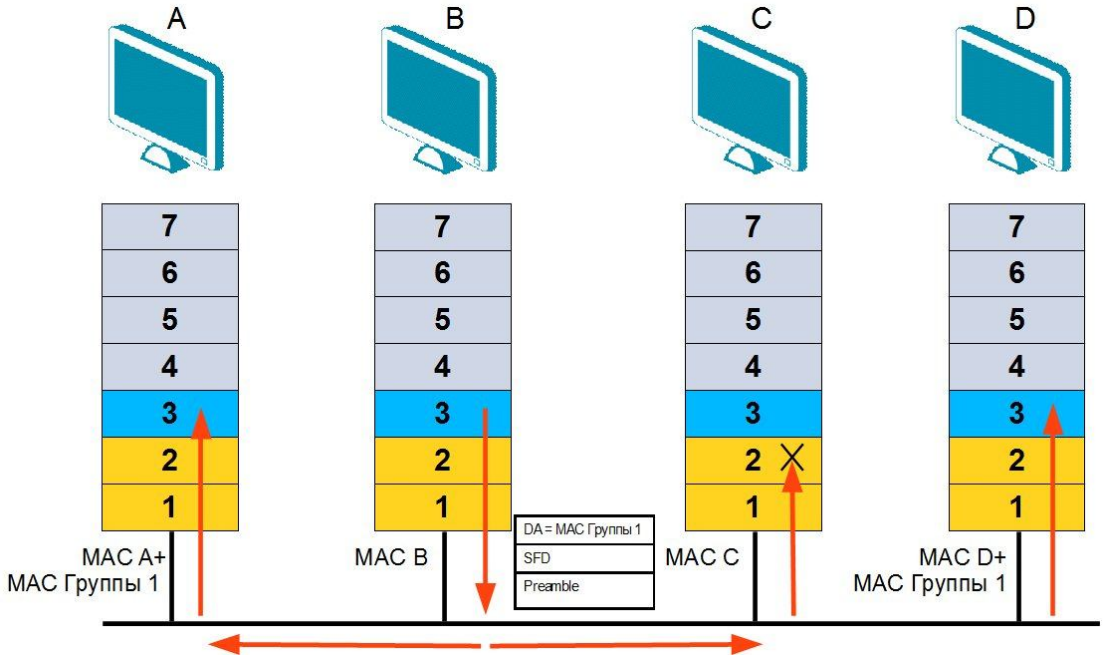


Рис. 5.9 Передача с использованием группового MAC-адреса

5.4.4 Сетевые адаптеры

Для подключения компьютера к сети и взаимодействия с другими сетевыми устройствами используется **сетевой адаптер** *(Network Interface Card, NIC)*. Сетевой адаптер, также известный как сетевая интерфейсная карта, сетевая карта, адаптер Ethernet, представляет собой периферийное устройство компьютера. В большинство современных компьютеров сетевые адаптеры интегрированы в материнскую плату.

По конструкторской реализации сетевые адаптеры делятся на:

- интегрированные в материнскую плату компьютера или ноутбука;
- внутренние, представляющие собой отдельную печатную плату, устанавливаемую в слот PCI, PCI Express, PCIe компьютера;
- внешние, подключающиеся к компьютеру или ноутбуку через интерфейс USB или CardBus (PCMCIA).

Для корректной работы сетевого адаптера на компьютере требуется установить его *драйвер*.

Драйвер – специальное программное обеспечение, позволяющее операционной системе работать с устройством.

Обычно драйвер входит в комплект поставки адаптера. Для устройств компании D-Link драйверы также можно бесплатно загрузить с FTP-сервера ftp.dlink.ru.

Сетевой адаптер и его драйвер реализуют на компьютере функции физического и канального уровней модели OSI (точнее подуровня MAC в соответствии со спецификацией IEEE 802) и выполняют две основные функции: прием и передачу кадров. Адаптер хранит уникальный 48-битный физический адрес (MAC-адрес), который позволяет однозначно идентифицировать компьютер в данном сегменте сети.

Для того чтобы узнать MAC-адрес сетевого адаптера компьютера в ОС Windows используется следующая команда: ipconfig/all

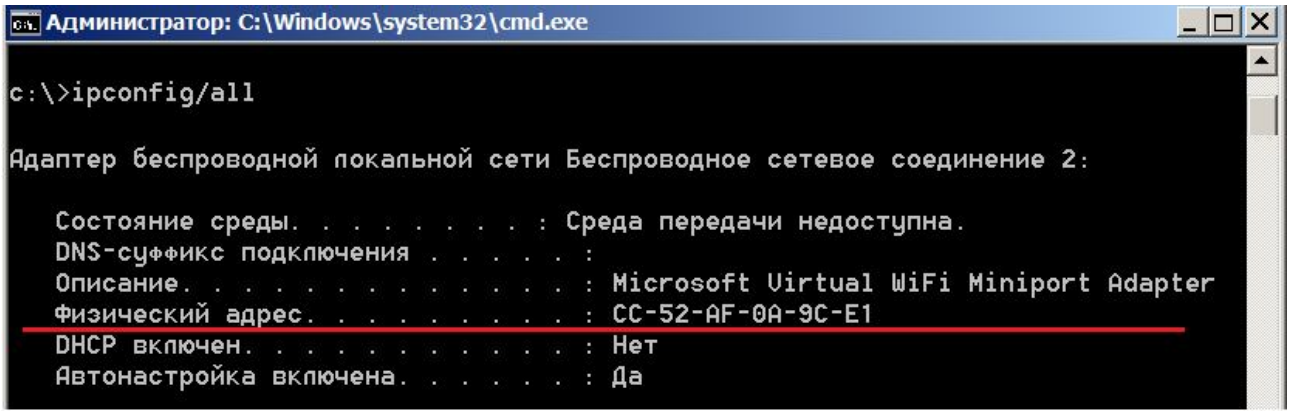


Рис. 5.10 Результат выполнения команды ipconfig

Остальные уровни модели OSI (от прикладного до сетевого) реализуются операционной системой, поэтому компьютер работает на всех семи уровнях модели OSI.

В зависимости от того, какой протокол на канальном уровне реализует адаптер, они делятся на Ethernet-адаперы, Wi-Fi-адаптеры, Bluetooth-адаптеры и т.д.

В сетевых адаптерах, предназначенных для подключения компьютеров к проводным сетям используются следующие, наиболее распространенные в настоящее время типы разъемов:

- медный 8P8C (ошибочное, но общепринятое название RJ-45) для подключения кабеля на основе витой пары;
- оптический разъем (LC, SC, ST, FC, MT-RJ) для подключения оптического кабеля.

Рис. 5.11 Сетевые адаптеры:
а) Сетевой адаптер Gigabit Ethernet для шины PCI DGE-528T;
б) Беспроводной адаптер для шины CardBus DWA-645;
в) Беспроводной адаптер для шины PCIe DWA-566;
г) Беспроводной адаптер для шины USB DWA-160.

В зависимости от сложности сетевого адаптера он может поддерживать различные функции, доступные для конфигурирования. Например, сетевой адаптер DGE-528T поддерживает такие функции как: Wake-On-LAN (WOL), позволяющую удаленно включать питание выключенного компьютера; технологию VLAN (Virtual LAN), позволяющую сделать компьютер частью виртуальной локальной сети, для повышения его безопасности; функцию управления потоком IEEE 802.3x, позволяющую предотвратить потерю данных в случае переполнения буфера принимающего устройства.

Характеристики и функции, поддерживаемые сетевым адаптером, обычно указываются в спецификации или руководстве пользователя на устройство.

Чтобы создать простейшую домашнюю сеть, т.е. объединить между собой два компьютера достаточно наличия в них совместимых сетевых адаптеров. В случае использования технологии Ethernet, сетевые адаптеры компьютеров соединяются между собой кабелем соответствующего типа (чаще всего на основе витой пары). При

использовании беспроводного соединения в сеть можно объединить более двух компьютеров, для этого их адаптеры надо переключить в режим Ad-Hoc. Правда, чем больше компьютеров будет объединено в такую беспроводную сеть, тем меньше будет скорость передачи данных.

5.5 Технологии локальных сетей

За годы развития сетевых технологий было разработано много сетевых архитектур. Многие из них уже вышли из употребления, а другие, такие как Ethernet, широко используются и постоянно развиваются. Для начала кратко рассмотрим технологии канального уровня Token Ring и FDDI, которые в настоящее время применяются довольно редко.

5.5.1 Технология Token Ring

Эта технология канального уровня была разработана компанией IBM в начале 1980 гг., а затем стандартизирована IEEE в проекте 802, как спецификация IEEE 802.5. Сети Token Ring относятся к сетям с маркерным методом управления доступом, в которых отсутствует конкуренция за доступ к среде передачи. Логически сеть Token Ring представляет собой кольцо, а физически – звезду. Сети Token Ring работают с двумя битовыми скоростями – 4 и 16 Мбит/с. Смешение станций, работающих на различных скоростях, в одном кольце не допускается.

Для объединения компьютеров в сетях Token Ring используются концентраторы – т.н. *устройства многостанционного доступа* (*MSAU, MultiStation Access Unit*). Рабочие станции отдельными кабелями подключаются к MSAU по топологии «звезда». Технология Token Ring позволяет использовать для соединения экранированную или неэкранированную витую пару.

Максимальная длина сегмента при использовании неэкранированной витой пары (UTP) – 150 м (при работе на скорости 4 Мбит/с) или 60 м (при работе на скорости 16 Мбит/с), при использовании экранированной витой пары (STP) – расстояние передачи увеличивается до 300 м (для 4 Мбит/с) или 100 м (для 16 Мбит/с).

В кольце на основе неэкранированных кабелей может работать не более 72 станций, в кольце на основе экранированных кабелей – максимум 260 станций.

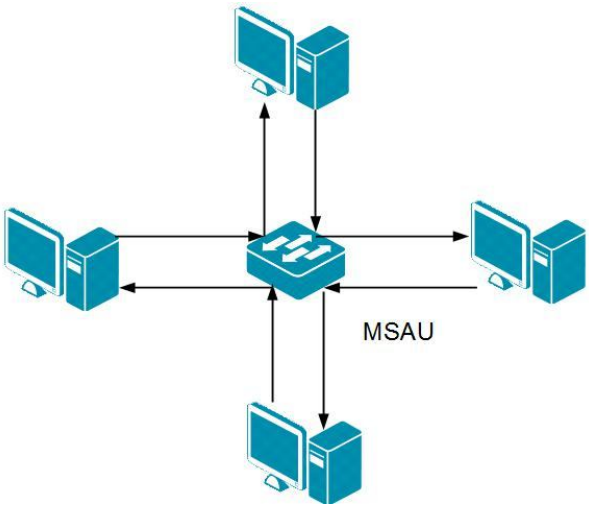


Рис. 5.12 Сеть Token Ring

В сетях с *маркерным методом доступа* право на доступ к среде передается циклически от станции к станции по логическому кольцу. Кольцо образуется отрезками кабеля, соединяющими все рабочие станции, и рассматривается как разделяемая среда передачи. Для обеспечения доступа станций к физической среде по кольцу циркулирует кадр специального формата и назначения – *маркер* или *токен (token)*.

Маркер представляет собой определенную последовательность битов и одновременно может быть использован только одной рабочей станцией или узлом. Получив маркер, рабочая станция анализирует его, при необходимости модифицирует, а при отсутствии у нее данных для передачи обеспечивает его продвижение к следующей станции. Станция, которая имеет данные для передачи, при получении маркера, извлекает его из кольца, что дает ей право доступа к физической среде и передачи своих данных. Затем эта станция преобразует маркер в кадр установленного формата и начинает передавать его по кольцу. Кадр снабжен адресом назначения и адресом источника (каждая рабочая станция имеет уникальный 48-битный MAC-адрес).

Передаваемые данные проходят по кольцу всегда в одном направлении от одной станции к другой, поэтому их получают все рабочие станции сети. Каждая станция проверяет, не ей ли предназначен кадр. Если нет, то станция выступает в роли ретранслятора и передает полученный кадр следующей станции сети. Когда станция - адресат распознает кадр, она копирует его в свою память, затем модифицирует некоторые биты в формате кадра (признак подтверждения приема) и возвращает его по кольцу обратно станции-отправителю. Последняя изымает этот кадр из кольца и проверяет, нормально ли принято сообщение. После этого она выдает новый маркер для обеспечения возможности другим станциям сети передавать данные.

Время владения разделяемой средой в сети Token Ring ограничивается *временем удержания маркера (token holding time)*, после истечения которого станция обязана прекратить передачу собственных данных (текущий кадр разрешается завершить) и передать маркер далее по кольцу. Станция может успеть передать за время удержания маркера один или несколько кадров в зависимости от размера кадров и величины времени удержания маркера.

Сети Token Ring, работающие со скоростью 16 Мбит/с, имеют отличный от сетей со скоростью 4 Мбит/с алгоритм доступа к кольцу, называемый алгоритмом *раннего освобождения маркера (Early Token Release)*. В соответствии с ним станция передает маркер следующей станции сразу же после окончания передачи последнего бита кадра, не дожидаясь возвращения по кольцу этого кадра с битом подтверждения приема. В этом случае пропускная способность кольца используется более эффективно, так как по кольцу одновременно продвигаются кадры нескольких станций. Тем не менее, свои кадры в каждый момент времени может генерировать только одна станция – та, которая в данный момент владеет маркером. Остальные станции в это время только ретранслируют чужие кадры, так что принцип разделения кольца во времени сохраняется, ускоряется только процедура передачи владения кольцом.

Технология Token Ring обладает свойствами отказоустойчивости. Для контроля работы сети и обработки ошибок в сетях Token Ring одна из станций выполняет роль *активного монитора,* который изучает кадры, циркулирующие по сети, удаляет все дефектные кадры, выдает новый маркер и обеспечивает правильную работу сети.

К достоинствам технологии Token Ring можно отнести:

- простоту расчета задержки передачи между любыми двумя устройствами, что особенно важно в автоматизированных системах управления, требующих обработки процессов в реальном режиме времени;
- отсутствие коллизий.

Недостатки:

- высокая стоимость, низкая совместимость оборудования;
- невысокая скорость передачи.

5.5.2 Технология FDDI

Стандарт **FDDI** (*Fiber Distributed Data Interface* – волоконно-оптический интерфейс передачи данных), разработанный в середине 80-х годов комитетом X3T9.5 ANSI, определяет кольцевую сеть с маркерным доступом и скоростью передачи до 100 Мбит/с на основе волоконно-оптического кабеля, способною охватить очень большую площадь (до 100 км).

Стандарт FDDI во многом основывается на технологии Token Ring (стандарт IEEE 802.5) и обеспечивает совместимость с ней, т.к. у обеих технологий одинаковые форматы кадров. Однако у этих технологий имеются существенные различия.

Стек FDDI определяет физический уровень и подуровень доступа к среде передачи (MAC). Физический уровень разбит на протокол физического уровня (Physical Layer Protocol, PHY), который отвечает за работу схем кодирования данных, и на подуровень физического уровня, зависящий от среды передачи (Physical Medium Dependent, PMD), на котором реализованы спецификации передачи. Особенностью стека FDDI является наличие уровня управления станциями (Station Management, SMT). Он отвечает за удаление и подключение рабочих станций, обнаружение и устранение неисправностей, сбор статистической информации о работе сети.

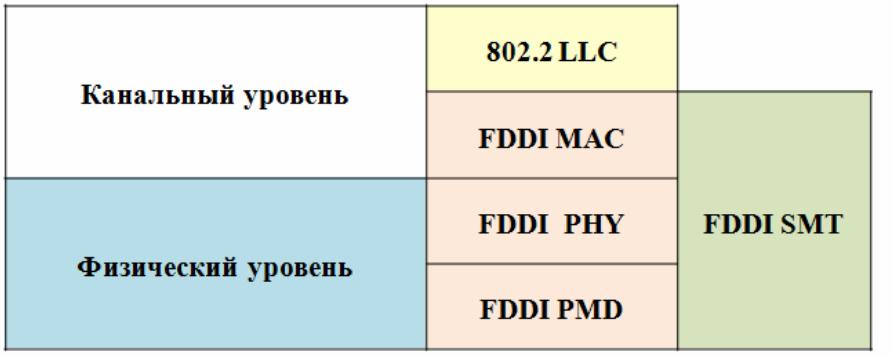


Рис. 5.13 Стек FDDI

Сети FDDI характеризуются встроенной избыточностью, что обеспечивает их высокую отказоустойчивость. Сеть FDDI строится на основе двух колец, которые образуют основной и резервный пути передачи данных между узлами сети. Данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным (первичным). По нему данные передаются при нормальной работе. Второе кольцо (вторичное) – вспомогательное, по нему данные передаются в случае обрыва в первом кольце. В случае какого-либо вида отказа, когда часть первого кольца не может передавать данные (например, обрыв кабеля или отказ узла), сеть выполняет «свертывание» колец – объединяет первое кольцо со вторым, образуя единое кольцо.

Основными компонентами сети FDDI являются станции и концентраторы. Для подключения станций и концентраторов к сети может быть использован один из двух способов:

- **Одиночное подключение** (Single Attachment, SA) – подключение только к первичному кольцу. Станция и концентратор, подключенные данным способом, называются соответственно станцией одиночного подключения (Single Attachment Station, SAS) и концентратором одиночного подключения (Single Attachment Concentrator, SAC).

- **Двойное подключение** (Dual Attachment, DA) – одновременное подключение к первичному и вторичному кольцам. Станция и концентратор, подключенные таким способом, называются соответственно станцией двойного подключения (Dual Attachment Station, DAS) и концентратором двойного подключения (Dual Attachment Concentrator, DAC).

В качестве среды передачи в сетях FDDI используется одномодовый и многомодовый волоконно-оптический кабель. Максимальное количество станций в кольце – 500. Максимальное расстояние между узлами может составлять 2 км при использовании многомодового кабеля и 20 км – при использовании одномодового. Максимальная протяженность сети – 100 км.

К преимуществам технологии FDDI можно отнести высокую отказоустойчивость. К недостаткам – двойной расход кабеля.

В настоящее время эта технология считается устаревшей.

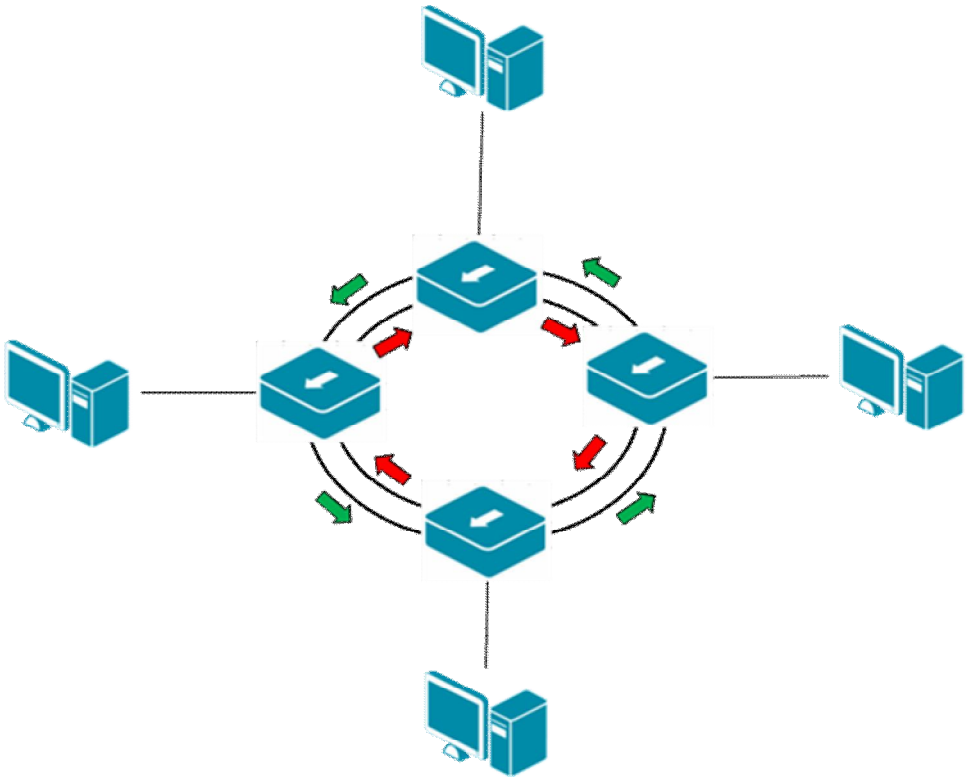


Рис. 5.14 Сеть FDDI

5.6 Технология Ethernet

Технология Ethernet является самой распространенной на сегодняшний день технологией локальных сетей благодаря своей простоте и универсальности. Ее теоретические основы были сформулированы в 1973 году в кандидатской диссертации аспиранта Гарвардского университета Роберта Меткалфа (Robert Melancton Metcalfe), озаглавленной «Пакетные сети».

Главные события в истории Ethernet развернулись в Пало-Альто, в исследовательском центре компании Xerox (PARC). В 1972 году сотрудники центра трудились над созданием прототипа персонального компьютера с названием Alto и одновременно разрабатывали высокоскоростной лазерный принтер. Всех сотрудников центра в Пало-Альто планировалось снабдить персональными компьютерами, каждый из которых будет подключен к одному и тому же лазерному принтеру. Задача создания сети была возложена на Роберта Меткалфа.

Основными требованиями, которые предъявлялись к новой сети, были высокое быстродействие, необходимое для нормальной работы лазерного принтера, и возможность объединения нескольких сотен компьютеров.

К концу 1972 года Меткалф и несколько других сотрудников исследовательского центра закончили работу над созданием экспериментальной сети, способной передавать данные от одного компьютера к другому со скоростью 2,94 Мбит/с.

Сначала Меткалф назвал свою сеть Alto Aloha Network, а затем переименовал в Ethernet.

22 мая 1973 года Роберт Меткалф составил докладную записку для главы PARC о потенциале технологии Ethernet. В том же году Xerox выпустил первую интерфейсную сетевую плату Ethernet для своих компьютеров Alto.

В 1976 году Роберт Меткалф и его ассистент Дэвид Боггс (David Boggs) издали брошюру под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks».

Меткалф ушел из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных сетей.

Ему удалось убедить компании Digital Equipment, Intel и Xerox, что Ethernet должна стать стандартом передачи пакетов по сети персональных компьютеров. Компании начали работать совместно и 30 сентября 1980 года опубликовали спецификацию на сеть Ethernet для передачи данных со скоростью 10 Мбит/с, которая называется Ethernet версии 1. В 1982 г. Digital Equipment, Intel и Xerox выпустили новую спецификацию Ethernet версии 2. Эту версию стандарта называют Ethernet DIX или Ethernet II.

Первый стандарт IEEE 802.3 был основан на спецификации Ethernet версии 1. Проект стандарта был одобрен группой 802.3 в 1983 году и в 1985 опубликован как официальный стандарт. В исходном стандарте Ethernet предусматривалось использование только коаксиального кабеля (стандарты 10BASE5 и 10BASE2). В начале 1990-х годов появились спецификации на основе витой пары (10BASE-T) и оптоволокна (10BASE-FL).

- В 1995 г. был опубликован стандарт Fast Ethernet (IEEE 802.3u).
- В 1998 г. был опубликован стандарт Gigabit Ethernet (IEEE 802.3z и 802.3ab).
- В 2002 г. был опубликован стандарт 10 Gigabit Ethernet (IEEE 802.3ae).
- В 2010 г. был опубликован стандарт 40 и 100 Gigabit Ethernet (IEEE 802.3ba).

В настоящее время стандарты Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 и 100 Gigabit Ethernet объединены в один стандарт IEEE 802.3-2012. Это гигантский документ, состоящий из 6 секций, который включает версию 2008 г., 2005 г., 2002 г. и всех последующих дополнений.

5.6.1 Форматы кадров Ethernet

В процессе стандартизации в формате оригинального кадра Ethernet произошли изменения. Поле «EtherType» было заменено на поле «Length», также стандарт в соответствии со спецификацией IEEE 802 требовал, чтобы в поле данных инкапсулировался заголовок LLC, который позволял бы определять тип протокола сетевого уровня. Однако, несмотря на принятие стандарта, Ethernet II продолжал широко использоваться. Поэтому через несколько лет в стандарте IEEE 802.3-1997 формально было одобрено использование форматов кадра Ethernet II и IEEE 802.3. Стандарт IEEE 802.3-2012 определяет следующую структуру кадра, обязательную для всех MAC-реализаций (рисунок 5.15):

7 байт	1 байт	6 байт	6 байт	2 байта	46 – 1500, 1504 или 1982 байта		4 байта	
Preamble	**SFP**	**Destination Address**	**Source Address**	**Length/Type**	**Data**	**PAD**	**FCS**	**Extension**
		64-2000 байта						

Рис. 5.15 Формат кадра IEEE 802.3-2012

Кадр содержит семь обязательных полей:

- *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 – это начало заголовка кадра.
- *Destination Address* (DA, адрес назначение) – MAC-адрес получателя кадра.
- *Source Address* (SA, адрес источника) – MAC-адрес отправителя кадра.
- *Length/Type* (длина/тип) – а) если значение меньше или равно 0x05DC (1500 в десятичной системе счисления), то поле указывает на длину поля данных в кадре (интерпретируется как длина); б) если значение больше или равно 0x0600 (1536 в десятичной системе счисления), то поле указывает на тип протокола, вложившего пакет в поле данных кадра (интерпретируется как тип).
- *Data* (данные) – поле данных переменной длины. Минимальная длина поля 46 байт, максимальная длина поля – 1500 байт (для стандартных кадров), 1504 байт (для кадров, содержащих тег протокола IEEE 802.1Q), 1982 байт (для расширенных (envelope) кадров).
- *Pad* (Padding, заполнение) – состоит из такого количества байт заполнителей, которое обеспечивает минимальную длину поля данных в 46 байт. Это обеспечивает корректное распознавание коллизий при работе протокола CSMA/CD. 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, Length/Type, поля данных и заполнения с помощью 32-разрядного циклического избыточного кода (Cyclic Redundancy Code, CRC).

Поле *Extension* (расширение) следует за полем FCS и состоит из последовательности битов, которые отличаются от битов данных и используются для выполнения процедур сетевого управления. Если эти процедуры не требуются, длина поля будет равна нулю. Это поле не используется при вычислении контрольной суммы кадра.

Минимальная длина кадра Ethernet составляет 64 байта, максимальная длина: стандартного кадра Ethernet – 1518 байт, кадра Ethernet с тегом стандарта IEEE 802.1Q – 1522 байта, расширенного кадра Ethernet – 2000 байт.

На практике существует четыре формата кадров Ethernet:

- кадр Ethernet II (Ethernet версии 2 или Ethernet DIX);
- кадр IEEE 802.3 /LLC;
- кадр Ethernet SNAP;
- кадр Raw 802.3 (Novell 802.3).

Разные типы кадра имеют некоторые отличия в формате, но могут сосуществовать в одной физической среде. При этом станция-отправитель и станция-получатель должны использовать один и тот же формат кадра. Наибольшее распространение получил кадр Ethernet II.

Кадр IEEE 802.3/LLC

Заголовок кадра IEEE 802.3/LLC является результатом объединения полей заголовков кадров, определенных в стандартах IEEE 802.3 и IEEE 802.2. Кадр IEEE 802.3 является кадром MAC-подуровня, поэтому в соответствии со стандартом IEEE 802.2 в его поле данных вкладывается кадр подуровня LLC с удаленными флагами начала и конца кадра.

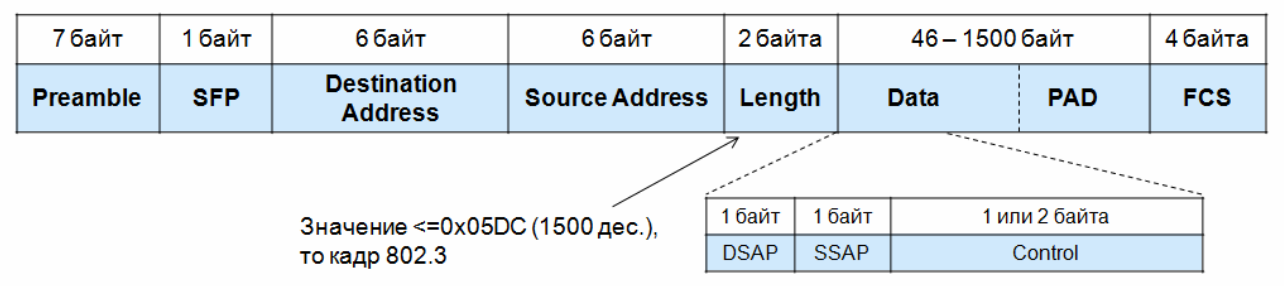


Рис. 5.16 Кадр IEEE 802.3/LLC

Поскольку в кадр IEEE 802.3/LLC вкладывается кадр подуровня LLC, то тип протокола верхнего уровня, передающего данные, берется из поля SAP кадра LLC. Поэтому в кадре IEEE 802.3/LLC после поля Source Address (адрес источника) расположено двухбайтовое поле Length (длина), которое указывает число байтов в поле данных. Поле данных имеет переменную длину от 46 до 1500 байтов, поэтому значение поля Length может быть меньше или равно 0x05DC (1500 в десятичной системе счисления).

Кадр Ethernet II

Кадр Ethernet II является наиболее распространенным типом кадра Ethernet. Он отличается от кадра IEEE 802.3/LLC тем, что после поля Source Address (адрес источника) следует поле Type (тип), которое используется для указания типа протокола верхнего уровня, вложившего пакет в поле данных кадра. Поле Length в кадре отсутствует. Для правильной интерпретации, значения в поле Type больше или равны 0x0600 (1536 в десятичной системе счисления).

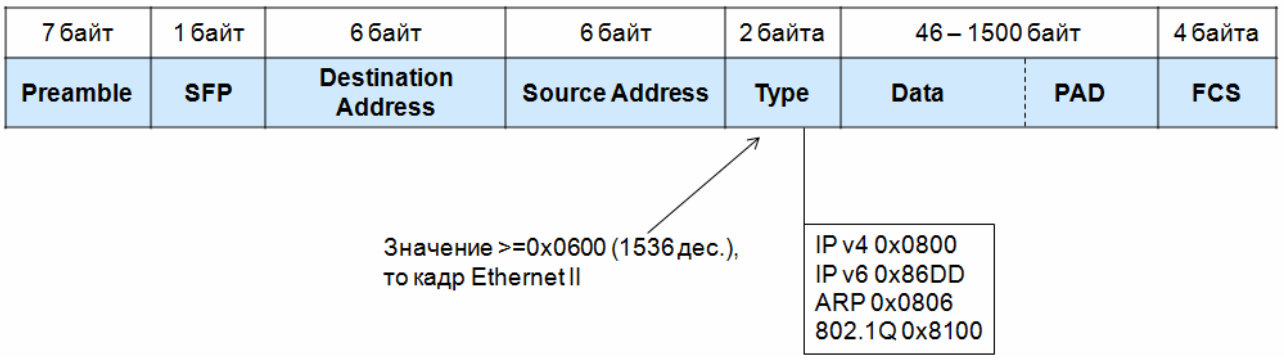


Рис. 5.17 Кадр Ethernet II

В отличие от поля SAP в заголовке LLC, поле Type имеет дину 2 байта, поэтому один и тот же протокол в полях SAP и Type будут кодироваться в общем случае разными числовыми значениями.

Кадр Ethernet SNAP

Для устранения разнобоя в кодировках типов протоколов верхнего уровня, комитет IEEE 802.2 провел дальнейшую работу по стандартизации кадров Ethernet. В результате появился кадр Ethernet SNAP.

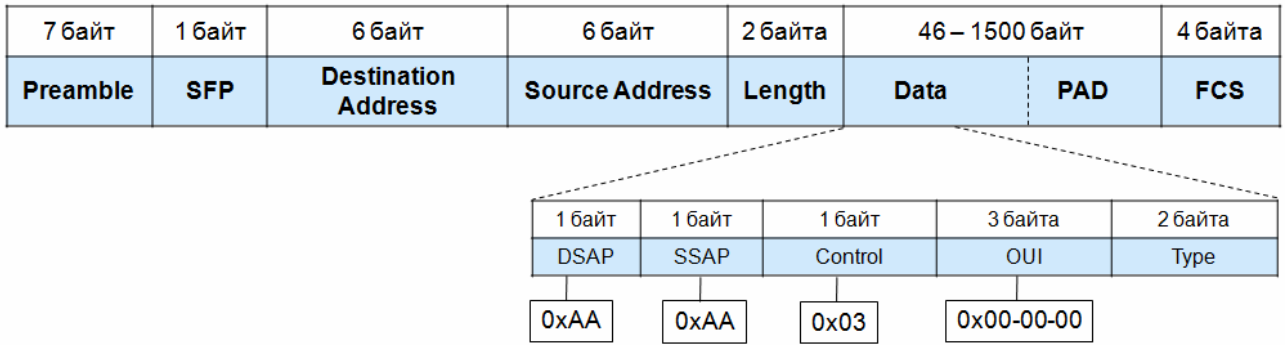


Рис. 5.18 Кадр Ethernet SNAP

Кадр Ethernet SNAP является расширением кадра IEEE 802.3/LLC за счет введения дополнительного заголовка протокола SNAP, состоящего из двух полей:

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

Так как SNAP представляет собой протокол, вложенный в протокол LLC, то в полях DSAP и SSAP записывается код 0xAA, отведенный для протокола SNAP.

С помощью заголовка SNAP достигнута совместимость с кодами протоколов в кадре Ethernet II, а также создана универсальная схема кодирования протоколов.

Этот тип кадра часто используется производителями сетевого оборудования при реализации собственных протоколов. Для этих целей поле OUI используется для указания производителя, а значение в поле Type выбирается производителем самостоятельно.

Кадр Raw 802.3 (Novell 802.3)

Кадр Raw 802.3 (Novell 802.3) представляет собой внутреннюю модификацию IEEE 802.3 без заголовка LLC. Компания Novell долгое время не использовала поле идентификации протокола верхнего уровня в своей ОС Novell Netware, т.к. в сетях Novell единственным протоколом сетевого уровня был IPX. В настоящее время Novell использует кадр IEEE 802.3/ LLC.

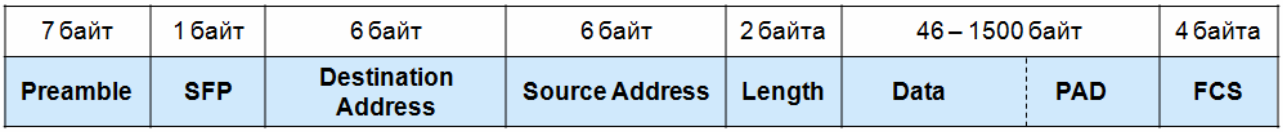


Рис. 5.19 Кадр Raw 802.3

Автоматическое распознавание формата кадра сетевым оборудованием происходит в соответствии со схемой, приведенной на рисункеРис. 5.20.

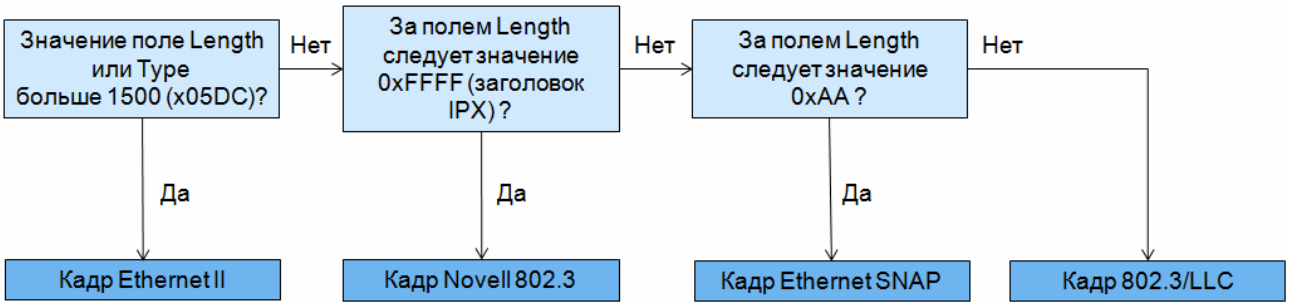


Рис. 5.20 Процедура распознавания формата кадров

В компьютерных сетях **Jumbo-фреймы** (*Jumbo-frame*) – это кадры Ethernet, размер поля данных которых может достигать 10 000 байт. Jumbo-фреймы не являются частью стандарта IEEE 802.3.

Использование Jumbo-фреймов позволяет передавать больше информации с меньшими усилиями, т.к. уменьшается нагрузка на центральный процессор и повышается пропускная способность канала связи, за счет уменьшения количества передаваемых кадров и сокращения служебной информации, добавляемой к ним.

Jumbo-фреймы поддерживают многие модели коммутаторов и сетевых адаптеров Fast/Gigabit Ethernet/10 Gigatit Ethernet.

5.6.2 Дуплексный и полудуплексный режимы работы

Стандарт IEEE 802.3-2012 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*) – позволяет паре узлов, имеющих соединение «точка-точка», одновременно принимать и передавать данные. Для этого каждый узел должен быть подключен к выделенному порту коммутатора.

5.6.3 Метод доступа CSMA/CD

Основная идея Ethernet состояла в использовании шинной топологии на основе коаксиального кабеля. Кабель использовался как разделяемая среда передачи, по которой рабочие станции, подключенные к сети, выполняли широковещательную двунаправленную (во всех направлениях) передачу. На обоих концах кабеля устанавливались терминаторы (заглушки).

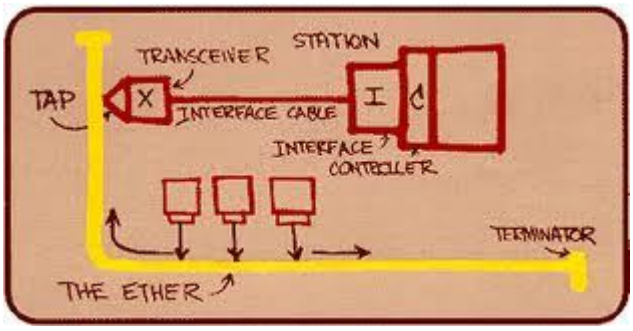


Рис. 5.21 Сеть Ethernet

Поскольку использовалась общая среда передачи, то требовался контроль над доступом узлов к физической среде. Для организации доступа узлов к разделяемой среде

передачи был использован *метод множественного доступа с контролем несущей и обнаружением коллизий* (Carrier Sense Multiple Access With Collision Detection, CSMA/CD).

Метод CSMA/CD основан на *конкуренции* (contention) узлов за право доступа к сети и включает следующие процедуры:

- контроль несущей;
- обнаружение коллизий.

Перед тем, как начать передачу, сетевое устройство должно удостовериться, что среда передачи данных свободна. Это достигается путем прослушивания несущей. Если среда свободна, то устройство начинает передавать данные. Во время передачи кадра, устройство продолжает прослушивать среду передачи. Делается это для того, чтобы гарантировать, что никакое другое устройство не начало передачу данных в то же самое время. После окончания передачи кадра все устройства сети должны выдержать технологическую паузу (Inter Packet Gap), равную 9,6 мкс. Эта пауза называется *межкадровым интервалом* и нужна для приведения в исходное состояние сетевых адаптеров и для предотвращения монопольного захвата среды одним сетевым устройством. После окончания технологической паузы устройства имеют право начать передачу своих кадров, т.к. среда свободна.

Сетевые устройства могут начинать передачу данных в любой момент, когда они определят, что канал свободен. Если устройство попыталось начать передачу кадра, но обнаружило, что сеть занята, оно вынуждено ждать, пока передающий узел не закончит передачу.

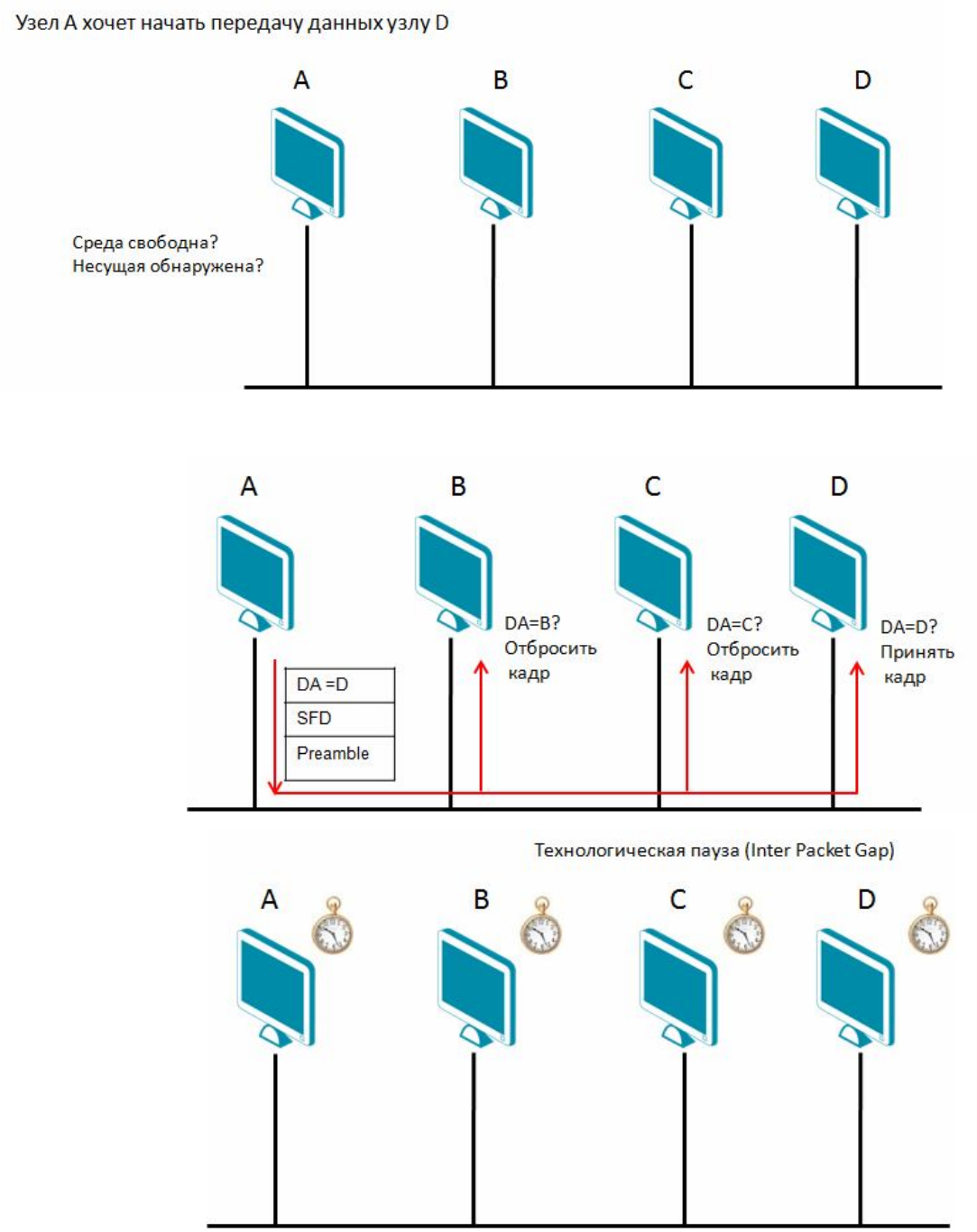


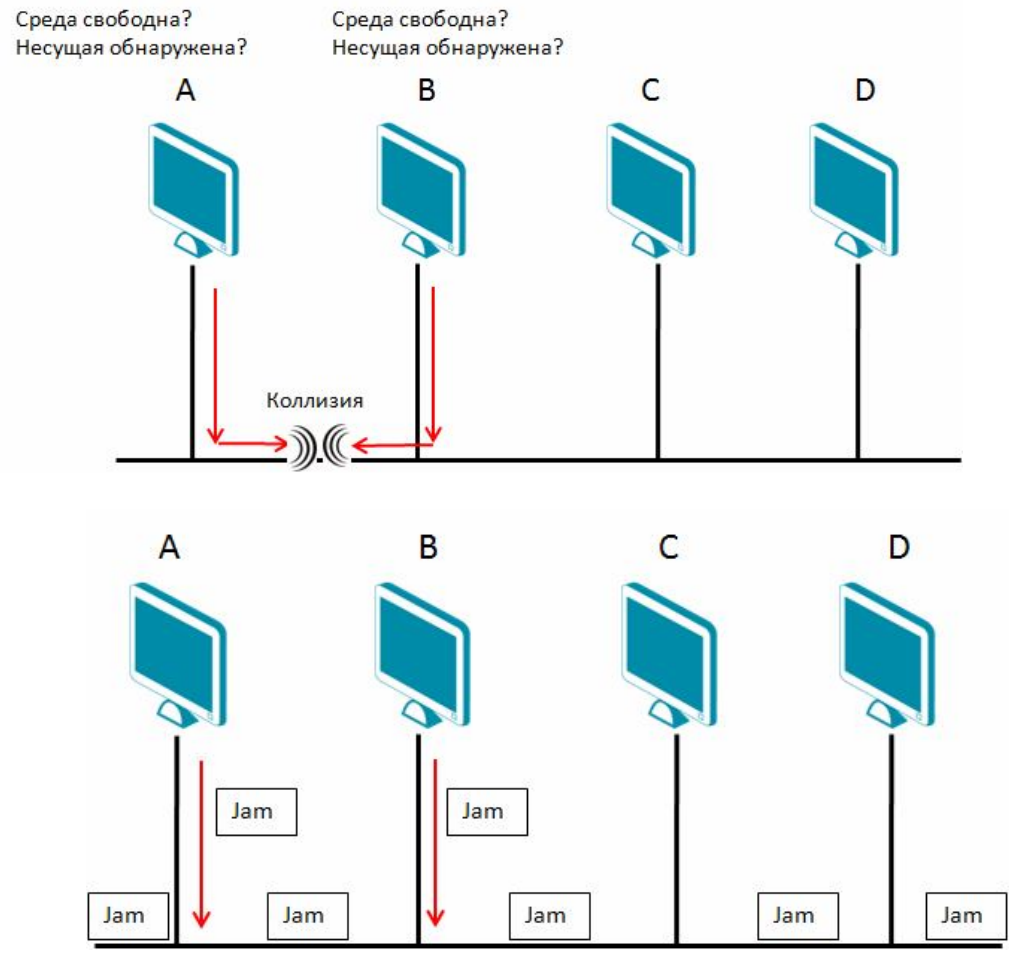
Рис. 5.22 Передача кадра в сети Ethernet

Ethernet – это широковещательная среда, поэтому все станции получают все кадры, передаваемые по сети. Однако не все устройства будут обрабатывать эти кадры. Только то устройство, MAC-адрес которого совпадает с MAC-адресом назначения, указанным в заголовке кадра, копирует содержимое кадра во внутренний буфер. Затем устройство проверяет кадр на наличие ошибок, и если их нет, передает полученные данные вышележащему протоколу. В противном случае, кадр будет отброшен. Устройство отправитель не уведомляется, успешно доставлен кадр или нет.

В сетях Ethernet неизбежны конфликты (*коллизии*), т.к. возможность их возникновения заложена в самом алгоритме CSMA/CD. Это связано с тем, что между моментом передачи, когда сетевое устройство проверяет, свободна ли сеть, и моментом начала фактической передачи проходит какое-то время. Возможно, что в течение этого времени какое-нибудь другое устройство сети начнет передачу.

Если несколько устройств в сети начали передачу примерно в одно и то же время, битовые потоки, поступающие от разных устройств, сталкиваются друг с другом и искажаются, т.е. происходит коллизия. В этом случае каждое из передающих устройств должно быть способно обнаружить коллизию до того, как закончит передачу своего кадра. Обнаружив коллизию, устройство прекращает передачу кадра и усиливает коллизию посылкой в сеть специальной последовательности из 32 бит, называемой *jam*-последовательностью. Это делается для того, чтобы все устройства сети смогли распознать коллизию. После того, как все устройства распознали коллизию, каждое устройство отключается на некоторый случайно выбранный интервал времени (свой для каждой станции сети). Когда время истечет, устройство опять может начать передачу данных. Когда передача возобновится, устройства, вовлеченные в коллизию, не имеют приоритета по передаче данных над остальными устройствами сети.

Если 16 попыток передачи кадра вызывают коллизию, то передатчик должен прекратить попытки и отбросить этот кадр.



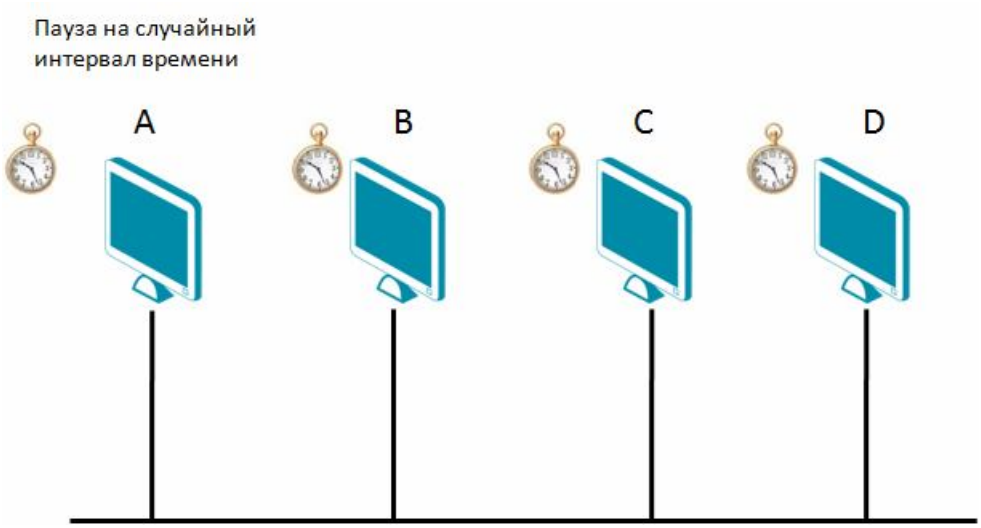


Рис. 5.23 Обнаружение коллизий в сети Ethernet

5.6.3.1 Домен коллизий

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

Домен коллизий (collision domain) – это часть сети Ethernet, все узлы которой распознают коллизию независимо от того, в какой части сети она возникла.

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

Напомним, что повторитель представлял собой устройство физического уровня модели OSI, используемое для соединения сегментов среды передачи данных с целью увеличения общей длины сети.

В сетях Ethernet (спецификации 10BASE2 и 10BASE5) на основе коаксиального кабеля применялись двухпортовые повторители, связывающие два физических сегмента. Работал повторитель следующим образом: он принимал сигналы из одного сегмента сети, усиливал их, восстанавливал синхронизацию и передавал в другой. Повторители не выполняли сложную фильтрацию и другую обработку трафика, т.к. не являлись интеллектуальными устройствами. Также общее количество повторителей и соединяемых ими сегментов было ограничено из-за временных задержек и других причин.

Позже появились многопортовые повторители, к которым рабочие станции подключались отдельным кабелем. Такие многопортовые повторители получили название «концентраторы». Причина появления многопортовых повторителей была следующей. Поскольку оригинальная технология Ethernet использовала в качестве среды передачи коаксиальный кабель и шинную топологию, то было сложно прокладывать кабельную систему здания. Позже международный стандарт на структурированную кабельную систему зданий определил использование топологии «звезда», в которой все устройства подключались к единой точке концентрации с помощью кабелей на основе витой пары. Под эти требования отлично подходила технология Token Ring и поэтому, чтобы выжить в конкурентной борьбе, технологии Ethernet пришлось адаптироваться к новым требованиям. Так появилась спецификация 10BASE-T Ethernet, которая использовала в качестве среды передачи кабели на основе витой пары и топологию «звезда».

Концентраторы работали на физическом уровне модели OSI. Они повторяли сигналы, поступившие с одного из портов на все остальные активные порты, предварительно восстанавливая их, и не выполняли никакой фильтрации трафика и другой обработки данных. Поэтому логическая топология сетей, построенных с использованием концентраторов, всегда оставалась шинной.

В один момент времени в сетях, построенных на повторителях и концентраторах, мог передавать данные только один узел. В случае одновременного поступления сигналов в общую среду передачи возникала *коллизия*, которая приводила к повреждению передаваемых кадров. Таким образом, все подключенные к таким сетям устройства находились в одном домене коллизий.

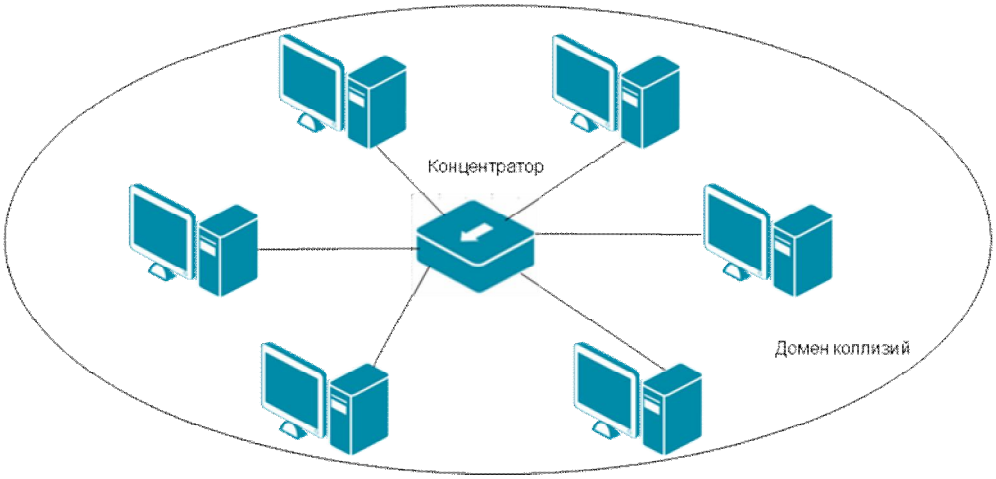


Рис. 5.24 Домен коллизий

С увеличением количества сегментов сети и компьютеров в них, возрастало количество коллизий, и пропускная способность сети падала. Помимо этого, полоса пропускания сегмента делилась между всеми подключенными к нему устройствами. Например, при подключении к сегменту с пропускной способностью 10 Мбит/с десяти рабочих станций, каждое устройство могло передавать в среднем со скоростью не более 1 Мбит/с. Встала задача *сегментации сети*, т.е. разделения пользователей на группы (сегменты) в соответствии с их физическим размещением с целью уменьшения количества клиентов, соперничающих за полосу пропускания.

5.6.4 Коммутируемая сеть Ethernet

Задача сегментации сети и повышения ее производительности была решена с помощью устройства, называемого *мостом* (bridge). Мост был разработан инженером компании Digital Equipment Corporation (DEC) Радьей Перлман (Radia Perlman) в начале 1980-х годов и представлял собой устройство канального уровня модели OSI, предназначенное для объединения сегментов сети. Мост был изобретен немного позже маршрутизаторов, но так как он был дешевле и прозрачен для протоколов сетевого уровня (работал на канальном уровне), то стал широко применяться в локальных сетях. Мостовые соединения (*bridging*) являются фундаментальной частью стандартов для локальных сетей IEEE.

Мост работал по алгоритму *прозрачного моста* (*transparent bridge*), который определен стандартом IEEE 802.1D. Прежде чем переслать кадры из одного сегмента в другой, он анализировал их и передавал только в том случае, если такая передача действительно была необходима, то есть MAC-адрес рабочей станции назначения принадлежал другому сегменту. Таким образом, мост изолировал трафик одного сегмента от трафика другого и делил один большой домен коллизий на несколько небольших, что повышало общую производительность сети. Однако мост передавал широковещательные кадры (например, необходимые для работы протокола ARP) из одного сегмента в другой, поэтому все устройства сети находились в одном *широковещательном домене* (*Broadcast domain*).

Подробнее алгоритм прозрачного моста будет рассмотрен в главе 6.

Коммутируемая сеть Ethernet (*Ethernet switched network*) – сеть Ethernet, сегменты которой соединены мостами или коммутаторами

MAC-адрес	Порт
1	1
2	1
3	2
4	2

Рис. 5.25 Соединение двух сегментов сети в помощью моста

Так как мосты были обычно двухпортовыми устройствами, то их эффективность сохранялась лишь до тех пор, пока количество рабочих станций в сегменте оставалось относительно невелико. Как только оно увеличивалось, в сетях возникала перегрузка, которая приводила к потере пакетов данных.

Увеличение количества устройств, объединяемых в сети, повышение мощности процессоров рабочих станций, появление мультимедийных приложений и приложений клиент-сервер требовали большей полосы пропускания. В ответ на эти растущие требования фирмой Kalpana в 1990 г. на рынок был выпущен первый *коммутатор* (*switch*), получивший название EtherSwitch.

Коммутатор представляет собой многопортовый мост и также функционирует на канальном уровне модели OSI. Основное отличие коммутатора от моста заключается в том, что он производительнее, может устанавливать одновременно несколько соединений между разными парами портов и поддерживает развитый функционал.

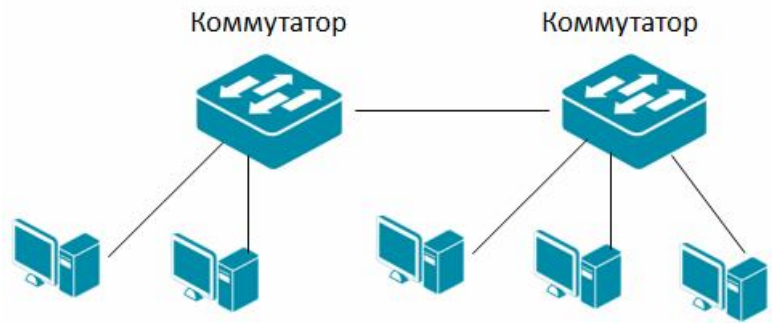


Рис. 5.26 Локальная сеть, построенная на коммутаторах

В 1993 году фирма Kalpana внедрила полнодуплексную технологию Ethernet (Full Duplex Ethernet Switch, FDES) в свои коммутаторы. Через какое-то время, при разработке технологии Fast Ethernet полнодуплексный режим работы стал частью стандарта IEEE 802.3.

Работа в полнодуплексном режиме обеспечивает возможность одновременного приема и передачи информации, т.к. к среде передачи подключены только два устройства. Прием и передача ведутся по двум разным физически каналам «точка-точка». Например, по разным парам кабеля на основе витой пары, или разным волокнам оптического кабеля.

Благодаря этому исключается возникновение коллизий в среде передачи (больше не требуется метод CSMA/CD, т.к. отсутствует конкуренция за доступ к среде передачи),

увеличивается время, доступное для передачи данных, и удваивается полезная полоса пропускания канала. Каждый канал обеспечивает передачу на полной скорости. Например, для спецификации 10BASE-T каждый канал передает данные со скоростью 10 Мбит/с. Для спецификации 100BASE-TX – со скоростью 100 Мбит/с. На концах дуплексного соединения скорость соединения удваивается, т.к. данные могут одновременно передаваться и приниматься. Например, в спецификации 1000BASE-T, в которой данные передаются по каналам со скоростью 1000 Мбит/с, суммарная пропускная способность будет равна 2000 Мбит/с.

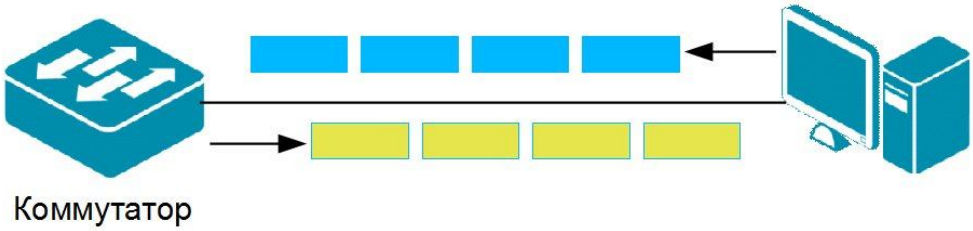


Рис. 5.27 Передача данных в дуплексном режиме

Также благодаря полнодуплексному режиму исчезло ограничение на общую длину сети и количество устройств в ней. Осталось только ограничение на длину кабелей, соединяющих соседние устройства.

Работа в полнодуплексном режиме возможна только при соединении сетевых устройств, порты которых его поддерживают. Если к порту устройства подключается сегмент, представляющий собой разделяемую среду, то порт будет работать в полудуплексном режиме и распознавать коллизии. Порты современных сетевых устройств поддерживают функцию автоопределения полудуплексного или дуплексного режима работы.

При работе порта в полнодуплексном режиме, интервал отправки между последовательными кадрами не должен быть меньше технологической паузы, равной 9,6 мкс. Для того чтобы исключить переполнение приемных буферов устройств при работе в полнодуплексном режиме требуется использовать механизм управления потоком кадров.

Следует отметить, что спецификации 10, 40 и 100 Gigabit Ethernet поддерживают только полнодуплексный режим работы. Это связано с тем, что современные сети стали полностью коммутируемыми и коммутаторы при взаимодействии с другими коммутаторами или высокоскоростными сетевыми адаптерами практически всегда используют режим полного дуплекса.

5.6.5 Управление потоком в полудуплексном и полнодуплексном режимах

Механизм управления потоком (Flow Control) позволяет предотвратить потерю данных в случае переполнения буфера принимающего устройства.

Для управления потоком в полудуплексном режиме обычно используется метод «*обратного давления*» (*backpressure*), т.е. принимающее устройство (например, порт коммутатора) в случае переполнения его буфера, посылает сигнал обнаружения коллизии (jam-последовательность) или обратно отправляет устройству-отправителю его кадры.

Для управления потоком в *полнодуплексном режиме* используется стандарт IEEE 802.3x, который в настоящее время является частью стандарта IEEE 802.3-2012 (Annex 31B). Согласно этому стандарту управление потоком осуществляется между MAC-подуровнями с помощью специального кадра-паузы, который автоматически формируется MAC-подуровнем принимающего устройства. В случае переполнения буфера, принимающее устройство отправляет кадр-паузу с указанием периода времени, на который требуется остановить передачу данных либо на уникальный MAC-адрес соответствующей станции, либо на специальный групповой MAC-адрес 0x01-80-C2-00-00-01. Если переполнение

буфера будет ликвидировано до истечения периода ожидания, то для восстановления передачи, принимающая станция отправляет второй кадр-паузу с нулевым значением времени ожидания.

Общая схема управления потоком показана на рисунке 5.28.

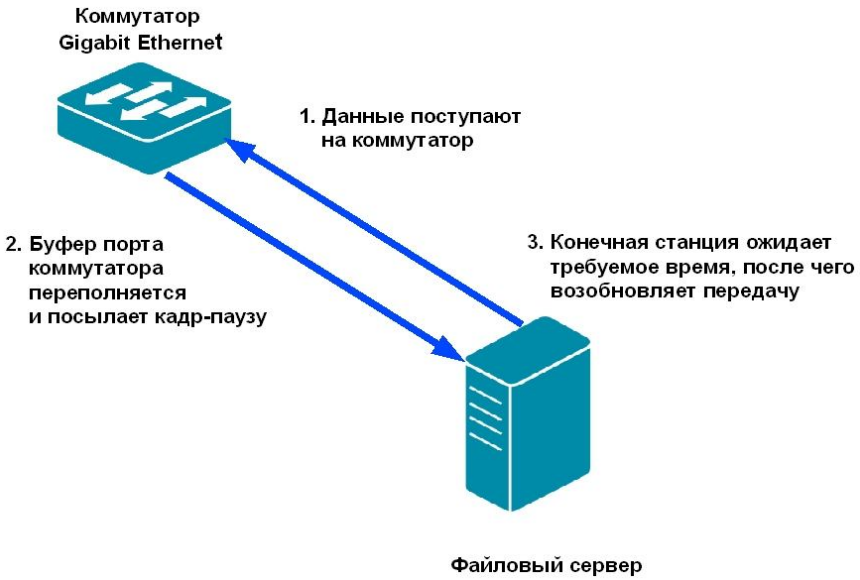


Рис. 5.28 Последовательность управления потоком IEEE 802.3x

Полнодуплексный режим работы и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи. Кадры-паузы идентифицируются как управляющие MAC-кадры по уникальным значениям полей «Длина/тип» (88-08) и «Код операции управления MAC» (00-01).

Преамбула	Начальный ограничитель кадра	Адрес назначения	Адрес источника	Длина/ тип	Код операции управления MAC (00-01)	Время паузы (от 00-00 до FF-FF)	Зарезер-вировано	Контрольная сумма кадра
7 байт	1 байт	6 байт	6 байт	2 байта	2 байта	2 байта	42 байта	4 байта

Рис. 5.29 Формат кадра-паузы

Правильно сконфигурированная функция управления потоком на устройствах позволяет повысить общую производительность сети за счет уменьшения потери данных и повторных передач. Управление потоком данных IEEE 802.3x большинства сетевых интерфейсных карт и встроенных сетевых карт включено по умолчанию. Коммутаторы D-Link имеют разные настройки функции IEEE 802.3x по умолчанию:

- неуправляемые коммутаторы – управление потоком IEEE 802.3x включено;
- коммутаторы серии Smart – управление потоком IEEE 802.3x отключено;
- управляемые коммутаторы – управление потоком IEEE 802.3x отключено.

5.7 Физический уровень технологии Ethernet

Все технологии семейства Ethernet имеют одинаковую реализацию MAC-подуровня – форматы кадров и способы доступа к среде передачи. Однако эти технологии отличаются

реализацией физического уровня, который определяет различные скорости передачи сигналов и типы среды передачи.

В настоящее время стандарт IEEE 802.3-2012 определяет спецификации физического уровня для скоростей передачи 10 Мбит/с, 100 Мбит/с (технология Fast Ethernet), 1000 Мбит/с (технология Gigabit Ethernet), 10 Гбит/с (технология 10 Gigabit Ethernet), 40 Гбит/с (технология 40 Gigabit Ethernet) и 100 Гбит/с (технология 100 Gigabit Ethernet).

Следует отметить, что ранее спецификации Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, 40 Gigabit Ethernet и 100 Gigabit Ethernet описывались в отдельных стандартах.

Архитектура физического уровня IEEE 802.3-2012 представляет собой набор интерфейсов и подуровней, каждый из которых выполняет определенную функцию.

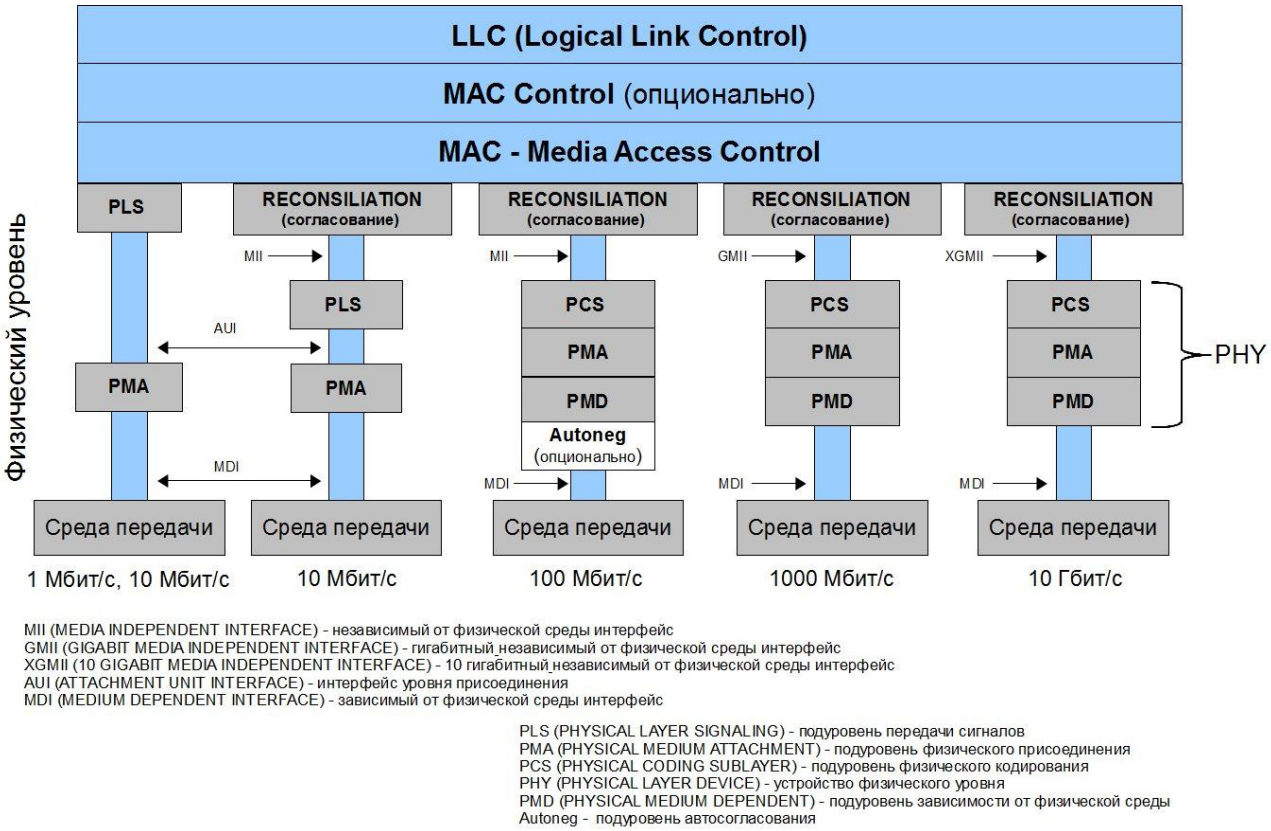


Рис. 5.30 Архитектура физических уровней Ethernet 10 Мбит/с, 100 Мбит/с, 1000 Мбит/с, 10 Гбит/с

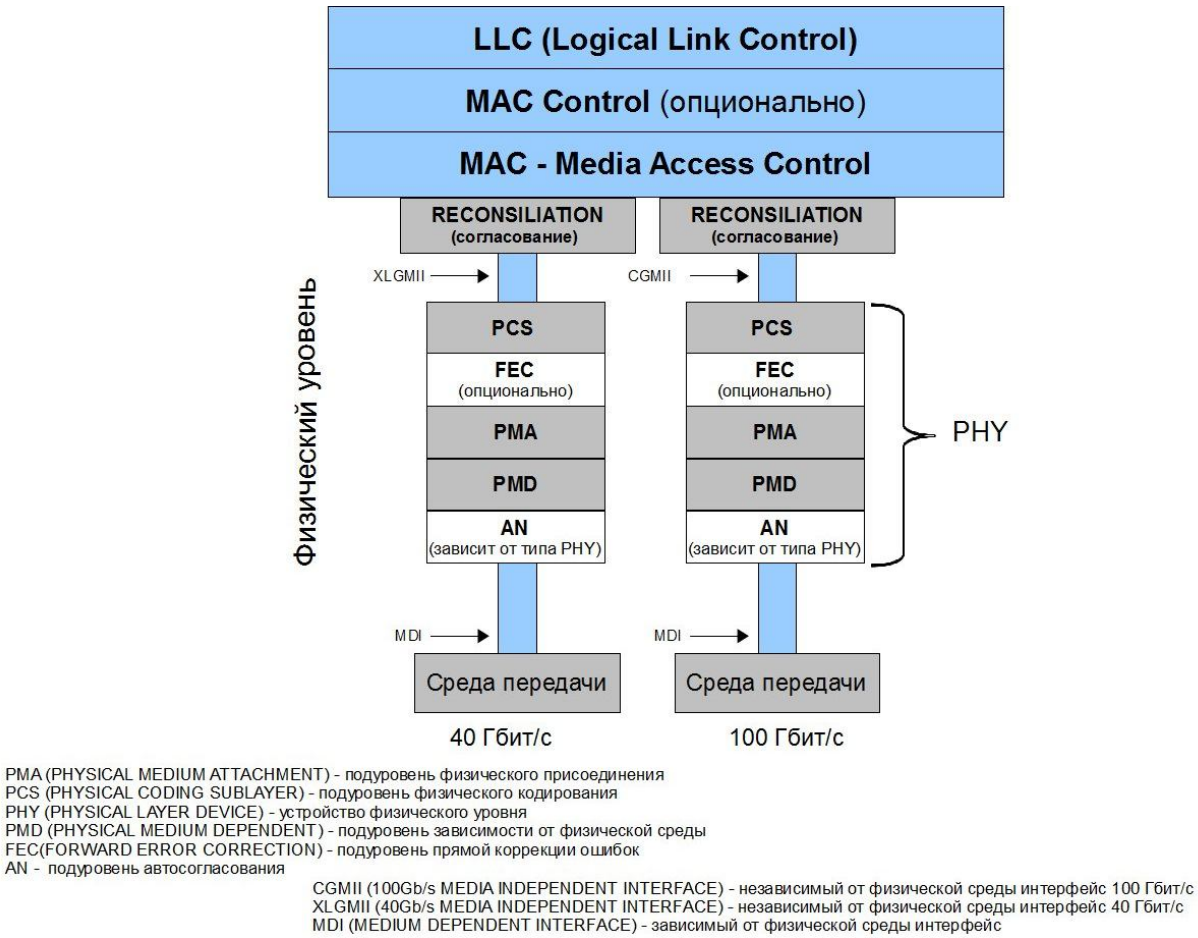


Рис. 5.31 Архитектура физических уровней Ethernet 40 Гбит/с и 100 Гбит/с

Физический уровень технологий Ethernet 100 Мбит/с, 1000 Мбит/с, 10 Гбит/с, 40 Гбит/с и 100 Гбит/с включает следующие элементы:

- подуровень согласования (Reconciliation sublayer);
- независимый от физической среды интерфейс (xMII):
  Media Independent Interface (MII) – интерфейс, независимый от физической среды для технологии Fast Ethernet;
  Gigabit Media Independent Interface (GMII) – гигабитный интерфейс, независимый от физической среды для технологии Gigabit Ethernet;
  10 Gigabit Media Independent Interface (XGMII) – 10-гигабитный интерфейс, независимый от физической среды для технологии 10 Gigabit Ethernet;
  40Gb/s Media Independent Interface (XLGMII) - независимый от физической среды интерфейс 40 Гбит/с;
  100Gb/s Media Independent Interface (CGMI) - независимый от физической среды интерфейс 100 Гбит/с.
- устройство физического уровня (Physical layer device, PHY);
- зависимый от физической среды интерфейс (Medium Dependent Interface, MDI).

Интерфейсы xMII поддерживают независимый от физической среды способ обмена данными между подуровнем MAC и устройством физического уровня (PHY).

Устройство физического уровня (PHY) состоит, в свою очередь, из нескольких подуровней:

- подуровня физического кодирования (Physical Coding Sublayer, PCS), зависящего от среды передачи и выполняющего кодирование данных (например, 4B/5B или 8B/10B), поступающих с MAC - подуровня;

- подуровня физического присоединения (Physical Medium Attachment, PMA), который является интерфейсом между подуровнями PCS и PMD и выполняет преобразование данных при их передаче между этими подуровнями;
- подуровня зависимости от физической среды (Physical Medium Dependent, PMD), который обеспечивает интерфейс со средой передачи. Он преобразует закодированные данные, полученные от подуровня PMA в сигналы, предназначенные для передачи через соответствующую физическую среду. Интерфейс MDI, который логически относится к PMD, фактически является средством физического присоединения к различным поддерживаемым стандартом средам передачи. Другими словами он является портом сетевого устройства с соответствующим разъемом (RJ-45, SC, LC и др.), служащим для подключения кабеля.
- подуровня автосогласования (Auto-Negotiation), который позволяет портам двух взаимодействующих устройств автоматически выбрать наиболее эффективный общий режим работы. В технологии Fast Ethernet этот подуровень является опциональным; в технологиях Gigabit Ethernet и 10 Gigabit Ethernet обязательным; в технологиях 40 Gigabit Ethernet и 100 Gigabit Ethernet наличие этого подуровня зависит от типа устройства физического уровня.

Опционально в спецификациях 10 Gigabit Ethernet, 40 Gigabit Ethernet и 100 Gigabit Ethernet, предназначенных для работы с медными кабелями имеется подуровень прямой коррекции ошибок (FEC, Forward Error Correction), который выполняет помехоустойчивое кодирование.

5.7.1 Спецификации физической среды Ethernet (10 Мбит/с)

Стандарт IEEE 802.3-2012 определяет следующие спецификации физического уровня технологии Ethernet со скоростью передачи 10 Мбит/с:

- **10BASE5**: используется коаксиальный кабель диаметром 0,5 дюйма (известен как «толстый Ethernet»), Манчестерское кодирование, топология «шина». Максимальная длина сегмента – 500 метров. Поддерживает работу только в полудуплексном режиме (метод CSMA/CD).
- **l0BASE2**: используется коаксиальный кабель диаметром 0,25 дюйма (известен как «тонкий Ethernet»), Манчестерское кодирование, топология «шина». Максимальная длина сегмента – 185 метров. Поддерживает работу только в полудуплексном режиме (метод CSMA/CD).
- **10BASE-T**: используются две пары проводников с диаметром от 0,4 до 0,6 мм (от 26 AWG до 22 AWG) кабеля на основе неэкранированной витой пары (UTP); интерфейс MDI поддерживает разъем 8P8C (RJ-45); метод физического кодирования - Манчестерское кодирование. Образует топологию «звезда». Максимальная длина сегмента – не более 100 м. Поддерживает работу в полудуплексном (метод CSMA/CD) и полнодуплексном режимах.
- **10BASE-F**: используется многомодовый волоконно-оптический кабель 62.5/125 мкм, Манчестерское кодирование и топология «звезда». Имеется несколько вариантов этой спецификации: 10BASE-FP (расстояние до 1000 м), 10BASE-FB (расстояние до 2000 м), 10BASE-FL (расстояние до 2000 м). 10BASE-FL поддерживает работу в полудуплексном (метод CSMA/CD) и полнодуплексном режимах. 10BASE-FP и 10BASE-FB работают только в полудуплексном режиме.

5.7.2 Спецификации физической среды Fast Ethernet (100 Мбит/с)

Fast Ethernet – общий термин, объединяющий спецификации Ethernet, обеспечивающие передачу данных на скорости до 100 Мбит/с. Технология Fast Ethernet является развитием технологии Ethernet.

Общее с технологией Ethernet:

- форматы кадров;
- временные параметры (межкадровый интервал (IPG), битовый интервал, интервал отсрочки, время передачи кадра минимальной длины и т. п);
- полудуплексный режим работы с методом доступа CSMA/CD и полнодуплексный режим для работы с коммутаторами;
- поддержка всех основных видов кабеля.

Отличием является то, что признаком свободного состояния среды в Fast Ethernet является передача по ней символа Idle соответствующего избыточного кода, а не отсутствие сигналов, как в спецификациях Ethernet 10 Мбит/с.

Стандарт IEEE 802.3-2012 определяет следующие спецификации физического уровня технологии Fast Ethernet со скоростью передачи 100 Мбит/с:

- **100BASE-T4:** используются четыре пары проводников кабеля на основе неэкранированной витой пары (UTP) категорий 3, 4, 5 (одна пара используется для обнаружения коллизий, три остальных пары – для передачи данных); разъем 8P8C (RJ-45); используется кодирование 8B6T. Поддерживает работу только в полудуплексном (метод CSMA/CD). Максимальная длина сегмента – не более 100 м. Для совместимости со спецификацией 10BASE-T поддерживает функцию *автосогласования (Auto-Negotiation)*, которая обеспечивает механизм обмена информацией между двумя устройствами, подключенными к одному каналу связи с целью выбора наилучшего общего режима работы.
- **100BASE-TX:** используются две пары проводников кабеля на основе неэкранированной витой пары (UTP) категории 5 или экранированной (STP) витой пары; разъем 8P8C (RJ-45); алгоритм логического кодирования данных 4B/5B и метод физического кодирования MLT-3; сигнальная скорость составляет 125 Мбод. Поддерживает работу в полудуплексном (метод CSMA/CD) и полнодуплексном режимах. Максимальная длина сегмента – не более 100 м. Для совместимости со спецификацией 10BASE-T поддерживает функцию автосогласования. Также поддерживается функция автоматического определения полярности кабеля на основе витой пары, режим уменьшенного потребления электроэнергии в то время, когда канал связи не используется (технология *энергоэффективный Ethernet* (Energy-Efficient Ethernet, EEE)).
- **100BASE-FX:** используется два волокна многомодового волоконно-оптического кабеля 50/125 мкм и 62.5/125 мкм; интерфейс MDI поддерживает разъемы SC, MIC, ST; алгоритм логического кодирования данных 4B/5B, метод физического кодирования NRZI; сигнальная скорость составляет 125 Мбод. Поддерживает работу в полудуплексном (метод CSMA/CD) и полнодуплексном режимах. Максимальная длина сегмента – не более 400 м (полудуплекс) и 2000 м (полный дуплекс).

Спецификации 100BASE-TX и 100BASE-FX известны также как 100BASE-X. Следующие спецификации используются для создания каналов связи «точка-точка» с расстоянием до 10 000 м.

- **100BASE-LX10**: используется два волокна одномодового волоконно-оптического кабеля; передача и прием ведутся на длине волны 1310 нм; алгоритм логического

кодирования данных 4B/5B, метод физического кодирования NRZI; сигнальная скорость составляет 125 Мбод. Длина сегмента – до 10 000 м.

- **100BASE-BX10**: используется одно волокно одномодового волоконно-оптического кабеля для одновременной передачи и приема сигналов на разных длинах волн (интерфейс для сетей WDM); передача ведется на длине волны 1310 нм (восходящий поток), прием – на длине волны 1550 нм (нисходящий поток); алгоритм логического кодирования данных 4B/5B, метод физического кодирования NRZI; сигнальная скорость составляет 125 Мбод. Длина сегмента – до 10 000 м.

5.7.3 Автосогласование

Автосогласование (*Auto-Negotiation*) – это функция Ethernet (IEEE 802.3-2012 Clause 28, Clause 37, Clause 73), позволяющая двум устройствам, подключенным к одному каналу связи выбрать общие параметры передачи, такие как скорость, режим работы (полнодуплексный/полудуплексный, энергосберегающий/обычный).

Автосогласование выполняется полностью на физическом уровне во время инициализации связи без дополнительного привлечения протоколов канального уровня или высших уровней. Автосогласование позволяет устройствам выполнить следующие операции:

- сообщить партнеру по связи о своей версии Ethernet и дополнительных возможностях;
- подтвердить прием и определить общие режимы работы;
- отказаться от режимов работы, не поддерживаемых вторым партнером;
- настроить каждое устройство на режим наивысшего уровня, поддерживаемый обоими партнерами по связи.

Автосогласование впервые появилось как дополнительная функция в спецификациях 100BASE-TX и 100BASE-T4 (в настоящее время описано в IEEE 802.3-2012 Clause 28). Целью его разработки было обеспечение обратной совместимости со спецификацией 10BASE-T. Другими спецификациями Fast Ethernet оно не поддерживается.

Процедура автосогласования выполняется следующим образом. Устройство, начавшее процесс автосогласования, посылает своему партнеру пачку специальных импульсов Fast Link Pulse burst (FLP), в которой содержится 8-битное слово, кодирующее предлагаемый режим взаимодействия, начиная с самого приоритетного, поддерживаемого данным узлом. Например, скорость 100 Мбит/с и полнодуплексный режим работы.

Если узел-партнер поддерживает функцию автосогласования, а также может поддерживать предложенный режим, он отвечает пачкой импульсов FLP, в которой подтверждает данный режим, и на этом переговоры заканчиваются. Если же узел-партнер может поддерживать менее приоритетный режим, то он указывает его в ответе, и этот режим выбирается в качестве рабочего. Таким образом, всегда выбирается наиболее приоритетный общий режим узлов.

Узел, который поддерживает только технологию 10BASE-T, периодически посылает импульсы проверки целостности линии (Normal Link Pulse, NLP), связывающей его с соседним узлом. Такой узел не понимает запросов FLP, который отправляет ему узел с функцией автосогласования, и продолжает посылать свои импульсы. Узел, получивший в ответ на запрос FLP только импульсы NLP, понимает, что его партнер может работать только по стандарту 10BASE-T, и устанавливает этот режим работы и для себя.

В спецификациях 1000BASE-X, 1000BASE-T и 10GBASE-T автосогласование является обязательной процедурой. Базовый механизм автосогласования в спецификации 1000BASE-X был дополнен функцией управления, которая обеспечивает дополнительный контроль над процедурой автосогласования (IEEE 802.3-2012 Clause 37). Спецификации 1000BASE-T и 10GBASE-T выполняют процессе автосогласования, описанный в IEEE 802.3-2012 Clause 28, но дополнительно требуют разделение устройств на ведущее (master) и

ведомое (slave) с целью синхронизации при передаче данных. Ведущим обычно является многопортовое устройство, ведомым – однопортовое.

Автосогласование для спецификаций 1000BASE-KX, 1000BASE-KX, 10GBASE-KX4, 10GBASE-KR, 40GBASE-KR4, 40GBASE-CR4 и 100GBASE-CR10 описано в разделе IEEE 802.3-2012 Clause 73. Эти спецификации определяют разные скорости передачи через медный кабель длиной не более 1 м и используются в объединительных платах (Backplane) модульных коммутаторов/маршрутизаторов. Процедура автосогласования этих спецификаций отличается от механизма обмена импульсами FLP и основана на дифференциальном манчестерском кодировании (Differential Manchester encoding, DME).

5.7.4 Спецификации физической среды Gigabit Ethernet (1000 Мбит/с)

Gigabit Ethernet – общий термин, объединяющий спецификации Ethernet, обеспечивающие передачу данных на скорости до 1000 Мбит/с (1 Гбит/с). Технология Gigabit Ethernet является развитием технологии Fast Ethernet.

Общее с предыдущими технологиями Ethernet:

- формат кадров;
- полудуплексный режим работы с методом доступа CSMA/CD и дуплексный режим для работы с коммутаторами;
- поддержка всех основных видов кабеля.

Для сохранения совместимости с технологиями Ethernet и Fast Ethernet были внесены изменения на физическом уровне и MAC - подуровне.

При работе в полудуплексном режиме возникают проблемы, связанные с максимальной протяженностью сети и ее пропускной способностью. При передаче данных на скорости 1000 Мбит/с диаметр сети составляет около 20 м. Это ограничение возникает из-за временных требований метода доступа CSMA/CD. Для увеличения диаметра сети при работе в полудуплексном режиме используются методы:

- *Carrier extension* (расширение несущей): используется MAC-подуровнем для увеличения времени, в течении которого может быть распознана коллизия. Для этого физический уровень устройства-отправителя увеличивает размер передаваемого кадра путем добавления в его конец битов расширения. Физический уровень устройства-получателя удаляет эти биты. Из-за большого количества битов расширения эффективная пропускная способность сети получается чуть больше, чем у Fast Ethernet.
- *Packet burst* (пакетная передача): используется MAC-подуровнем для минимизации издержек, связанных с добавлением битов расширения. Этот метод позволяет MAC-подуровню отправлять последовательность кадров, не прерывая при этом контроль над средой передачи. Для разделения кадров внутри пакета MAC - подуровень устройства-отправителя использует биты расширения, чтобы другие устройства видели, что сеть занята и не пытались передать данные, пока не закончится пакет.

При работе в полнодуплексном режиме эти методы не нужны.

Физическая спецификация технологии Gigabit Ethernet включает следующие среды передачи данных:

- **1000BASE-T:** используются четыре пары проводников кабеля на основе неэкранированной витой пары (UTP) категории 5, 5e; все четыре пары одновременно используются для полнодуплексной передачи; разъем 8P8C (RJ-45); кодирование выполняется с помощью 5-уровневого кода PAM; сигнальная скорость каждой пары проводников составляет 125 Мбод. Поддерживает работу в полудуплексном (метод CSMA/CD) и полнодуплексном режимах. Максимальная длина сегмента – не более 100 м. Поддерживается функция автоматического определения полярности кабеля на основе витой пары, энергоэффективный Ethernet (EEE). Функция автосогласования согласует три скорости передачи – 10, 100 и 1000 Мбит/с, два режима работы –

полнодуплексный и полудуплексный, возможность работы в режиме низкого энергопотребления (EEE) и роли master – slave.

Следующие спецификации объединены под общим названием 1000BASE-X.

- **1000BASE-SX (Short Wavelength)**: используется два волокна многомодового волоконно-оптического кабеля 50/125 мкм и 62.5/125 мкм; передача и прием ведутся на длине волны 850 нм; кодирование 8B/10B; сигнальная скорость составляет 1250 Мбод. Поддерживает работу в полу- и полнодуплексном режимах. Длина сегмента – до 550 м (кабель 50/125 мкм), до 275 м (кабель 62.5/125 мкм). Поддерживается автосогласование режимов работы (полнодуплексный/ полудуплексный).
- **1000BASE-LX (Long Wavelength)**: используется два волокна многомодового волоконно-оптического кабеля 50/125 мкм и 62.5/125 мкм или одномодового оптического кабеля; передача и прием ведутся на длине волны 1300 нм; кодирование 8B/10B; сигнальная скорость составляет 1250 Мбод. Поддерживает работу в полу- и полнодуплексном режимах. Длина сегмента – до 550 м (многомодовый кабель), до 5000 м (одномодовый кабель). Поддерживается автосогласование режимов работы (полнодуплексный/полудуплексный).
- **1000BASE-CX:** используется твинаксиальный кабель (высококачественный сбалансированный экранированный медный кабель 150 Ом) длиной до 25 м. Сигнальная скорость составляет 1250 Мбод. Используется разъем DE-9. Поддерживается автосогласование режимов работы (полнодуплексный/ полудуплексный).

Следующие спецификации используются для создания каналов связи «точка-точка» с расстоянием до 10 000 м. Основное приложение – организация магистральных каналов.

- **1000BASE-LX10**: используется два волокна одномодового или многомодового 50/125 мкм и 62.5/125 мкм волоконно-оптического кабеля; передача и прием ведутся на длине волны 1310 нм. Длина сегмента – до 550 м (многомодовый кабель), до 10 000 м (одномодовый кабель).
- **1000BASE-BX10**: используется одно волокно одномодового волоконно-оптического кабеля для одновременной передачи и приема сигналов на разных длинах волн (интерфейс для сетей WDM); передача ведется на длине волны 1310 нм (восходящий поток), прием - на длине волны 1490 нм (нисходящий поток). Длина сегмента – до 10 000 м.

Следующие спецификации являются собственной разработкой производителей и не входят в стандарт:

- **1000BASE-ZX**: используется два волокна одномодового волоконно-оптического кабеля; передача и прием ведутся на длине волны 1550 нм. Длина сегмента, обеспечиваемая оборудованием D-Link – до 80 000 м.
- **1000BASE-LH (Long Haul):** используется два волокна одномодового волоконно-оптического кабеля. Длина сегмента – до 100 000 м.

5.7.5 Спецификации физической среды 10 Gigabit Ethernet (10 Гбит/с)

10 Gigabit Ethernet (10GE, 10GbE или 10GigE) – общий термин, объединяющий спецификации Ethernet, обеспечивающие передачу данных на скорости до 10 Гбит/с. Технология 10 Gigabit Ethernet является развитием технологии Gigabit Ethernet.

В технологии 10GE остались прежними формат кадра, а также его минимальный и максимальный размер.

В отличие от предыдущих версий Ethernet, в 10 Gigabit Ethernet не поддерживается полудуплексный режим работы. Все спецификации 10 Gigabit Ethernet на MAC-подуровне поддерживают работу только в *полнодуплексном* режиме. На физическом уровне 10 Gigabit Ethernet появились две группы спецификаций: LAN PHY – для локальных сетей, работающих на скорости 10 Гбит/с и WAN PHY – для глобальных сетей, работающих на скорости SONET STS-192c/SDH VC-4-64c. Используются новые схемы кодирования, максимальная длина сегмента увеличена до 40 000 м.

Технология 10GE включает четыре семейства спецификаций: 10GBASE-W, 10GBASE-R, 10GBASE-X, 10GBASE-T.

Семейство 10GBASE-X состоит их трех спецификаций, использующих четырехпотоковую передачу (в формате 4 потока x 8 бит) с кодированием каждого потока кодом 8B/10B:

- **10GBASE-CX4:** используется твинаксиальный кабель длиной 15 м. Сигнальная скорость каждого из 4-х потоков составляет 3,125 Гбод.
- **10GBASE-LX4:** используется одномодовый или многомодовый 50/125 мкм и 62.5/125 мкм волоконно-оптический кабель и 4 длины волны с шагом 13,4 нм во втором окне прозрачности (1310 нм). Каждая длина волны передает один из четырех потоков данных. Потоки объединяются мультиплексором WDM на передающей стороне перед подачей в волоконно-оптический кабель и демультиплексируются на приемной стороне. Сигнальная скорость каждого из 4-х потоков составляет 3,125 Гбод. Длина сегмента – от 240 до 300 м в зависимости от полосы пропускания многомодового кабель, до 10 000 м при использовании одномодового кабеля.
- **10GBASE-KX4:** предназначен для объединительных плат (Backplane) модульных коммутаторов/ маршрутизаторов. Используется медный кабель длиной не более 1 м. Поддерживается энергоэффективный Ethernet (EEE) и автосогласование.

Семейство 10GBASE-R состоит из пяти спецификаций, которые могут использоваться самостоятельно после кодирования данных на подуровне PCS по схеме 64B/66B или превращаться в спецификации 10GBASE-W, если потоки данных после PCS передаются WAN-интерфейсу WIS, чтобы далее инкапсулироваться в кадры технологий SONET и SDH.

- **10GBASE-SR:** используется многомодовый 50/125 мкм и 62.5/125 мкм волоконно-оптический кабель; передача ведется на длине волны 850 нм. Сигнальная скорость составляет 3,125 Гбод. Длина сегмента – от 66 до 400 м (в зависимости от полосы пропускания многомодового кабель 50/125 мкм), от 26 до 33 м (в зависимости от полосы пропускания многомодового кабель 62,5/125 мкм).
- **10GBASE-LR:** используется одномодовый волоконно-оптический кабель; передача ведется на длине волны 1310 нм. Сигнальная скорость составляет 3,125 Гбод. Длина сегмента – до 10 000 м.
- **10GBASE-ER:** используется одномодовый волоконно-оптический кабель; передача ведется на длине волны 1550 нм. Сигнальная скорость составляет 3,125 Гбод. Длина сегмента – до 40 000 м.
- **10GBASE-LRM:** используется многомодовый 50/125 мкм и 62.5/125 мкм волоконно-оптический кабель; передача ведется на длине волны 1300 нм. Сигнальная скорость составляет 3,125 Гбод. Длина сегмента – до 220 м.
- **10GBASE-KR:** предназначен для объединительных плат (Backplane) модульных коммутаторов/маршрутизаторов. В отличие от 10GBASE-KX4 использует однопотоковую передачу и кодирование 64B/66B. Используется медный кабель длиной не более 1 м. Поддерживается энергоэффективный Ethernet (EEE) и автосогласование.

Семейство 10GBASE-W относится к WAN PHY и предназначено для адаптации скорости передачи и форматов Ethernet к скорости и форматам технологий SONET STS-192c

и SDH VC-4-64c. Для этого устройство физического уровня (PHY) семейства 10GBASE-W имеет дополнительный подуровень WAN-интерфейса (WIS, WAN Interface Sublayer), расположенный под подуровнем PCS. После кодирования в подуровне PCS кодом 64B/66B потоки данных Ethernet подключаются к WIS, чтобы далее инкапсулироваться в кадры технологий SONET и SDH для их транспорта через физический уровень. Без подуровня WIS семейство спецификаций 10GBASE-W не отличается от семейства спецификаций 10GBASE-R. При этом следует отметить, что интерфейс 10GBASE-W может взаимодействовать только с другим интерфейсом 10GBASE-W. В семейство 10GBASE-W входят следующие спецификации:

- **10GBASE-SW:** используется многомодовый 50/125 мкм и 62.5/125 мкм волоконно-оптический кабель; передача ведется на длине волны 850 нм. Сигнальная скорость составляет 9,953 Гбод. Длина сегмента – от 66 до 400 м (в зависимости от полосы пропускания многомодового кабель 50/125 мкм), от 26 до 33 м (в зависимости от полосы пропускания многомодового кабель 62,5/125 мкм).
- **10GBASE-LW:** используется одномодовый волоконно-оптический кабель; передача ведется на длине волны 1310 нм. Сигнальная скорость составляет 9,953 Гбод. Длина сегмента – до 10 000 м.
- **10GBASE-EW:** используется одномодовый волоконно-оптический кабель; передача ведется на длине волны 1550 нм. Сигнальная скорость составляет 9,953. Длина сегмента – до 40 000 м.

Спецификация **10GBASE-T** определяет передачу данных со скоростью 10 Гбит/с через 4-х парный кабель на основе сбалансированной витой пары Class E или Class F (как определено в ISO/IEC 11801:2002) или Category 6 или Category 6A (как определено в TIATSB-155-A) с номинальным сопротивлением 100 Ом. По каждой из четырех пар данные передаются одновременно в каждом направлении со скоростью 2500 Мбит/с. Метод логического кодирования – 64B/65B, метод физического кодирования – PAM2. Спецификация поддерживает топологию «звезда». Длина сегмента составляет 100 м. При использовании неэкранированной витой пары Category 6 длина сегмента ограничена 55 м. Интерфейс MDI требует использования 8-контактного разъема (8P8C), соответствующего требованиям IEC 60603-7-4 (unscreened) или IEC 60603-7-5 (screened), поддерживается функция автоматического определения полярности. Поддерживается энергоэффективный Ethernet (EEE). Автосогласование в 10GBASE-T выполняет согласование скоростей 100 Мбит/с, 1000 Мбит/с, 10000 Мбит/с, режимов работы дуплекс/полудуплекс, возможности работы в режиме низкого энергопотребления (EEE) и ролей master – slave.

5.7.6 Спецификации физической среды 40 и 100 Gigabit Ethernet (40 и 100 Гбит/с)

Технологии 40 и 100 Gigabit Ethernet на настоящий момент являются самыми высокоскоростными технологиями компьютерных сетей. Окончательные версии спецификаций этих технологий были утверждены к 2012 году и стали частью стандарта IEEE 802.3-2012.

40 Gigabit Ethernet – общий термин, объединяющий спецификации Ethernet, обеспечивающие передачу данных на скорости до 40 Гбит/с. **100 Gigabit Ethernet** – общий термин, объединяющий спецификации Ethernet, обеспечивающие передачу данных на скорости до 100 Гбит/с.

В технологиях 40 и 100 Gigabit Ethernet остались прежними формат кадра, а также его минимальный и максимальный размер. Также как и технология 10GE, эти технологии на MAC-подуровне поддерживают работу только в *полнодуплексном* режиме. Максимальная

длина сегмента составляет 40 000 м при использовании одномодового волоконно-оптического кабеля.

Одним из основных применений технологии 40 Гбит/с является организация ядра высокоскоростных сетей центров обработки данных, которым требуется большая полоса пропускания, а также создание магистральных каналов. Технологию 100 Гбит/с можно использовать в ядре сетей операторов связи или сетей Metro Ethernet.

В семейство 40GBASE-R в настоящий момент входит пять спецификаций:

- **40GBASE-KR4:** предназначен для объединительных плат (Backplane) модульных коммутаторов/маршрутизаторов. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Максимально расстоянием передачи по медному кабелю 1 м. Поддерживается автосогласование.
- **40GBASE-CR4:** используется твинаксиальный кабель; максимальная длина сегмента – 7 м. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Поддерживается автосогласование.
- **40GBASE-SR4**: используются четыре волокна многомодового волоконно-оптического кабеля 50/125 мкм класса OM3 или OM4; длина волны 850 нм. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Длина сегмента – до 100 м при использовании кабеля класса OM3 и до 150 м при использовании кабеля класса OM4.
- **40GBASE-FR**: используется одномодовый волоконно-оптический кабель; передача ведется на длине волны 1550 нм, прием может выполняться на длинах волн 1310 нм и 1550 нм. Выполняется однопотоковая передача и кодирование 64B/66B. Сигнальная скорость 41,25 Гбод. Максимальная длина сегмента – 2 000 м.
- **40GBASE-LR4**: используется одномодовый волоконно-оптический кабель. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Для передачи и приема используются 4 длины волны: 1271 нм, 1291 нм, 1311 нм, 1331 нм. Каждая длина волны передает один из четырех потоков данных. Потоки объединяются мультиплексором WDM на передающей стороне перед подачей в волоконно-оптический кабель и демультиплексируются на приемной стороне. Максимальная длина сегмента – 10 000 м.

В семейство 100GBASE-R в настоящий момент входит четыре спецификации:

- **100GBASE-CR10:** используется твинаксиальный кабель; максимальныя длина сегмента – 7 м. Выполняется десятипотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Поддерживается автосогласование.
- **100GBASE-SR10**: используются десять волокон многомодового волоконно-оптического кабеля 50/125 мкм класса OM3 или OM4; длина волны 850 нм. Выполняется десятипотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 10,3125 Гбод. Длина сегмента – до 100 м при использовании кабеля класса OM3 и до 150 м при использовании кабеля класса OM4.
- **100GBASE-LR4**: используется одномодовый волоконно-оптический кабель. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная скорость каждого потока 25,7812 Гбод. Для передачи потоков используется технология WDM. Передача и прием ведутся на длинах волн 1295,56 нм, 1300,05 нм, 1304,58 нм, 1309,14 нм. Максимальная длина сегмента – 10 000 м.
- **100GBASE-ER4**: используется одномодовый волоконно-оптический кабель. Выполняется четырехпотоковая передача и кодирование 64B/66B. Сигнальная

скорость каждого потока 25,7812 Гбод. Для передачи потоков используется технология WDM. Передача и прием ведутся на длинах волн 1295,56 нм, 1300,05 нм, 1304,58 нм, 1309,14 нм. Максимальная длина сегмента – 40 000 м.

5.8 Энергоэффективный Ethernet

В 2010 г. институт IEEE принял стандарт на энергоэффективный Ethernet IEEE 802.3az Energy-Efficient Ethernet (EEE), который являлся набором усовершенствований для MAC-подуровня и физических спецификаций на основе витой пары 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T, а также спецификаций для объединительных плат (Backplane) 1000BASE-KX, 10GBASE-KX4 и 10GBASE-KR. В настоящее время стандарт IEEE 802.3az является частью стандарта IEEE 802.3-2012 (Clause 78).

Технология EEE автоматически уменьшает потребление энергии в то время, когда по каналам связи не ведется передача данных. Также в ней предусмотрена возможность обмена информацией о поддержке EEE между партнерами по связи во время процедуры автосогласования. Если один из партнеров не поддерживает EEE, то перехода в режим низкого энергопотребления не будет.

Для сбережения энергии EEE использует сигнальный протокол, который позволяет передатчику сообщать о том, что существует пауза в передаче данных и канал не используется. Сигнальный протокол также служит для извещения о том, что в канале надо начать передачу после предопределенного периода «спящего режима».

Когда передатчик ожидает паузу в потоке данных, он передает партнеру по связи сигнал Low Power Idle (LPI), сообщая, что канал переходит в «спящий режим». Когда приемник получает этот сигнал, он отключает некоторый функционал для уменьшения энергопотребления. Через период времени, равный времени сна (T_s), передатчик может остановить передачу сигналов, таким образом, канал перейдет в состояние покоя (T_q). Периодически передатчик отправляет сигналы обновления, которые служат для извещения партнера по связи, что канал существует, и обрыва связи не произошло. Сигналы обновления отправляются до тех пор, пока передатчик не решит выйти из режима низкого энергопотребления. Время нахождения канала в «спящем режиме» не регулируется. Оно может быть различным. Когда передатчик решает начать передачу, он отправляет обычный сигнал Idle. После истечения времени, определяющего период выхода из «спящего режима» (T_w), канал становится активным и по нему могут передаваться данные.

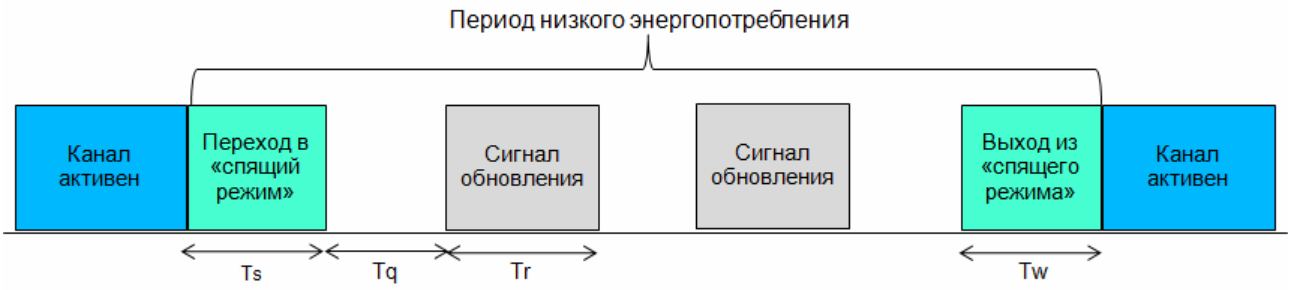


Рис. 5.32 Принцип работы передатчика с поддержкой EEE

Временные параметры T_s, T_q, T_r и T_w отличаются у разных спецификаций физического уровня. Минимальные и максимальные значения T_s, T_q, T_r определены в стандарте. Время T_w обычно равно времени, требуемому для передачи кадра максимальной длины через данную среду передачи. В некоторых случаях оборудованию может потребоваться более длительный период выхода из «спящего режима», чем среднее время T_w. Например, это относится к компьютеру, система которого находилась в «спящем режиме» и была «разбужена» сетевой активностью. EEE поддерживает дополнительную функцию, которая позволяет партнерами

по связи согласовывать время, определяющее период выхода из «спящего режима» с помощью протокола LLDP (Link Layer Discovery Protocol, описан в стандарте IEEE 802.1AB-2009). Протокол LLDP широко поддерживается сетевым оборудованием, поэтому у взаимодействующих устройств не должно возникать больших затруднений при согласовании времени T_w.

Оборудование D-Link поддерживает технологию EEE. Например, при использовании коммутаторов D-Link с поддержкой EEE на границе сети или при создании в сети, построенной на таких коммутаторах резервных маршрутов для повышения отказоустойчивости, можно добиться уменьшения потребление электроэнергии.

5.9 Сменные интерфейсные модули

В зависимости от выполняемых задач сетевые устройства могут быть оборудованы различным количеством и типом портов. Наиболее распространенными интерфейсами являются фиксированные интерфейсы с разъемом RJ-45 на основе витой пары, поддерживающие технологию Fast или Gigabit Ethernet, автосогласование скоростей, полудуплексного или полнодуплексного режима работы и автоматического определения полярности витой пары MDI/MDI-X. Эти интерфейсы, как правило, служат для подключения оборудования в локальных сетях. Магистральные сети обычно представляют собой волоконно-оптическую инфраструктуру.

Для обеспечения большей гибкости в выборе типа подключения к волоконно-оптической сети, многие коммутаторы, маршрутизаторы и медиаконвертеры оборудованы специальными слотами, в которые можно устанавливать компактные сменные интерфейсные модули. Сменные интерфейсные модули поддерживают режим «горячей замены», т.е. их можно устанавливать в устройство и извлекать из него без отключения питания. Модули обеспечивают прием и передачу сигналов при работе в сетях передачи данных, речи и видео, а также в сетях хранения данных. По сравнению с традиционными фиксированными портами они позволяют реализовывать сетевые решения с более гибкой конфигурацией, т.к. дают возможность подбирать оптимальные оптические интерфейсы (100BASE-FX, 1000BASE-SX, 1000BASE-BX10, 10GBASE-LR и т.д.) для каждого сетевого соединения и при этом экономить затраты.

Существует несколько видов сменных интерфейсные модулей:

- GBIC (Gigabit Interface Converter);
- SFP (Small Form Factor Pluggable);
- SFP+ (Enhanced Small Form Factor Pluggable);
- XFP (10 Gigabit Small Form Factor Pluggable);
- QSFP (Quad Small Form Factor Pluggable).

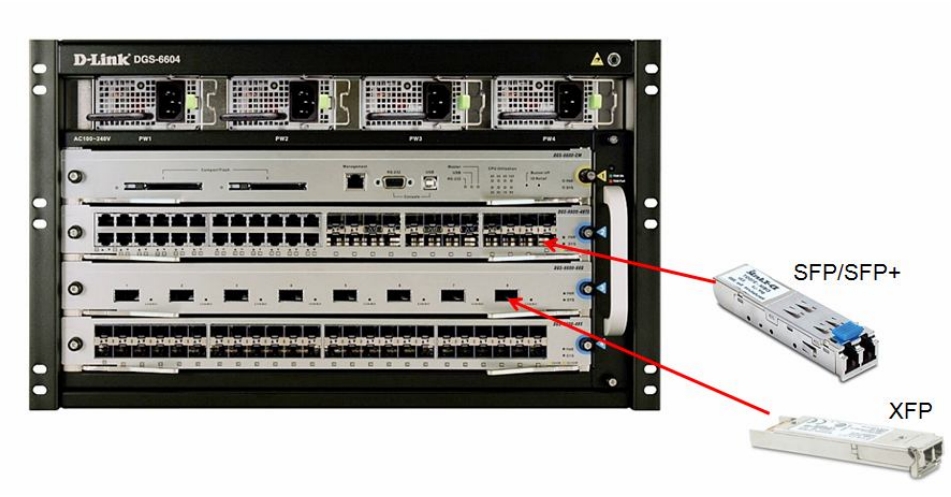


Рис. 5.33 Сменные интерфейсные модули

Самой первой спецификацией на компактные сменные интерфейсные модули была спецификация SFF-8053 комитета SFF, описывающая конвертеры гигабитного интерфейса (Gigabit Interface Converter, GBIC). Модули GBIC поддерживают стандарты Gigabit Ethernet или Fibre Channel для передачи данных, голоса и видео по медным или оптическим кабелям, но преимущественно представляют собой оптические трансиверы для приема или передачи сигнала по многомодовому или одномодовому волокну. Компания D-Link выпускает большой перечень модулей GBIC с поддержкой технологии Gigabit Ethernet с оптическими и медными интерфейсами.

Рис. 5.34 Модуль GBIC DGS-703 с 1 портом 1000Base-LX для одномодового оптического кабеля

Спустя несколько лет после появления спецификации GBIC разработчики предложили усовершенствованную, компактную модификацию сменного интерфейса (Small Form Factor Pluggable, SFP). Модули SFP в два раза меньше своих предшественников по габаритным размерам. Посадочный размер SFP (форм-фактор) определяется величиной медного разъема RJ-45. Интерфейсы SFP поддерживают практически любые существующие протоколы: Ethernet (на 10, 100, 1000 Мбит/с), SONET/SDH (OC3/ 12/48 и STM 1/4/16), Fibre Channel (1 и 2 Гбит/с). Модули SFP работают на длинах волн 850, 1310 и 1550 нм.

Компания D-Link выпускает модули SFP, поддерживающие стандарты Fast и Gigabit Ethernet и предназначенные для работы с разнообразным оптическим кабелем — одномодовым двухволоконным, одномодовым одноволоконным для систем с технологией WDM (Wavelength Division Multiplexing) и многомодовым. Модули снабжены дуплексными или симплексными разъемами типа LC для подключения оптического кабеля. В зависимости от используемой длины волны и типа оптического кабеля, модули обеспечивают разную дальность передачи – от 550 м до 80 км. Благодаря этому можно выбрать необходимый модуль SFP для конкретного соединения.

Рис. 5.35 Модуль SFP DEM-310GT с 1 портом 1000Base-LX для одномодового оптического кабеля

Рис. 5.36 Модули SFP DEM-331R и DEM-331T с 1 портом 1000BASE-BX10 с поддержкой технологии WDM

Модули SFP могут поддерживать важные функции цифровой диагностики (описанные в спецификации SFF-8472), позволяющие в реальном времени осуществлять мониторинг таких параметров как мощность передатчика, чувствительность приемника, напряжение питания и температура каждого оптического компонента. Информация о поддержке этой функции обычно указывается в спецификации на устройство.

Каждый модуль SFP выпускается с собственной электронной меткой, где содержатся сведения об идентификационном номере устройства и спецификации внешнего порта. Информация о внешнем порте может включать данные о длине волны, характеристиках волокна, скорости передачи данных, поддерживаемых протоколах, а также о длине канала. Идентификация SFP полезна при инвентаризации: с ее помощью отслеживается установка и замена компонентов и определяется местонахождение того или иного модуля.

Следующей ступенью эволюции сменных интерфейсов стала разработка оптических трансиверов XFP (10 Gigabit Small Form Factor Pluggable) для длин волн 850, 1310 и 1550 нм. Они поддерживают 10GE, 10 Gigabit SONET/SDH, Fibre Channel и еще некоторые высокоскоростные протоколы. XFP имеют несколько большие размеры, чем трансиверы SFP. Модули могут поддерживать систему цифровой диагностики для мониторинга состояния оптических линий.

В настоящее время компания D-Link выпускает трансиверы XFP 10GE, предназначенные для работы с одномодовым и многомодовым оптическим кабелем разной дальности передачи и для систем с технологией CWDM

Рис. 5.37 Модуль XFP DEM-423XT с 1 портом 10GE (10GBASE-ER) для одномодового оптического кабеля

Новым поколением оптических сменных интерфейсных модулей с поддержкой скоростей 10 Гбит/с стали трансиверы SFP+. Требования к модулям SFP+, которые являются расширенной версией SFP, определены в спецификации SFF-8431. Несмотря на то, что

модули SFP+ имеют ряд усовершенствований по сравнению с классическими модулями SFP, в коммутаторах D-Link слоты SFP+ поддерживают установку модулей SFP.

По сравнению с трансиверами XFP, модули SFP+ обладают меньшими габаритными размерами и тепловыделением, что позволяет повысить плотность размещения портов 10 Гбит/с на корпусе телекоммуникационных устройств.

Модули SFP+, также как и модули SFP могут поддерживать систему цифровой диагностики в соответствии со спецификацией SFF-8472.

Компания D-Link производит широкий спектр трансиверов SFP+ с поддержкой и без поддержки функции цифровой диагностики. Различают модули, предназначенные для работы как с одномодовым или многомодовым оптическим кабелем на длинах волн 850, 1310 и 1550 нм, с поддержкой технологий WDM, CWDM.

Рис. 5.38 Модуль SFP+ DEM-432XT-DD с 1 портом 10GE (10GBASE-LR) для одномодового оптического кабеля и поддержкой функции цифровой диагностики

Сменные интерфейсные модули QSFP/QSFP+ (Quad (4-channel) Small Form Factor Pluggable) представляют собой компактные оптические трансиверы с высокой плотностью компоновки, которые поддерживают четыре передающих и приемных канала. Первоначальная версия трансиверов поддерживала для каждого канала скорости 2,5 Гбит/с и 5 Гбит/с и называлась «QSFP». Последняя версия трансиверов называется «QSFP+». Скорость каждого канала в QSFP+ составляет 10 Гбит/с (в соответствии со спецификациями SFF-8635, SFF-8636) и 28 Гбит/с (в соответствии со спецификацией SFF-8665). Спецификация QSFP+ поддерживает стандарты 40 Gigabit Ethernet, Fibre Channel, InfiniBand and SONET/SDH. Модули QSFP+ могут поддерживать функции цифровой диагностики, которые позволяют отслеживать качество канала связи.

Один модуль QSFP+ способен заменить четыре стандартных модуля SFP+, а занимает на корпусе оборудования примерно столько же места, сколько занимает модуль XFP. Благодаря этому модули QSFP+ позволяет увеличить плотность портов на оборудовании в 3-4 раза по сравнению с модулями SFP+.

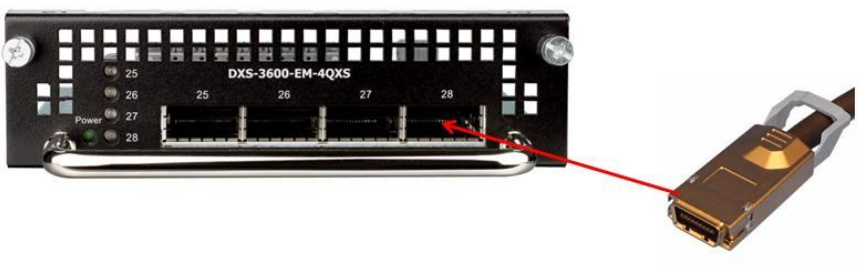


Рис. 5.39 Подключение модуля QSFP+ к разъему на коммутаторе

Рис. 5.40 Кабель DEM-CB300QXS с модулями QSFP+

6 Технологии коммутации

Мостовые соединения (*bridging*) являются фундаментальной частью стандартов для локальных сетей IEEE. Мост был разработан с целью уменьшения количества коллизий в локальных сетях, которые изначально использовали разделяемую среду передачи, увеличения диаметра сети, а также поддержки различных протоколов сетевого уровня. Мост делил локальную сеть на два (или более) сегмента и выполнял фильтрацию кадров на основе их MAC-адресов назначения. Прежде чем переслать кадры из одного сегмента в другой, он анализировал их и передавал только в том случае, если такая передача действительно была необходима, то есть MAC-адрес рабочей станции назначения принадлежал другому сегменту.

Стандарты IEEE определяют мостовые соединения для всех технологий локальных сетей. Например, в сетях Token Ring используется алгоритм *мостовой передачи с маршрутизацией от источника* (*source route bridging)*, определенный в Секции 9 стандарта IEEE 802.2, в сетях Ethernet используется алгоритм *прозрачного моста* (*transparent bridge*) , который определен стандартом IEEE 802.1D.

В настоящее время основным строительным блоком для создания локальных сетей являются коммутаторы (коммутаторы Ethernet, т.к. Ethernet является основной технологией локальных сетей). Коммутатор представляет собой многопортовый мост и также функционирует на канальном уровне модели OSI. Основное отличие коммутатора от моста заключается в том, что он производительнее, может устанавливать одновременно несколько соединений между разными парами портов и поддерживает множество дополнительных возможностей, отвечающих общепринятым стандартам. Наиболее распространенными и широко используемыми в настоящее время функциями коммутаторов являются:

- виртуальные локальные сети (VLAN);
- семейство протоколов Spanning Tree – IEEE 802.1D, 802.1w, 802.1s;
- статическое и динамическое по протоколу IEEE 802.1ad агрегирование каналов Ethernet;
- обеспечение качества обслуживания QoS;
- функции обеспечения безопасности, включая аутентификацию 802.1X, функции Port Security, IP-MAC-Port Binding и т.д.;
- SNMP-управление и др.

Помимо перечисленных функций коммутаторы могут поддерживать протоколы маршрутизации и играть роль маршрутизаторов локальной сети. В этом случае их называют коммутаторами 3-го уровня.

6.1 Алгоритм прозрачного моста

Коммутаторы локальных сетей обрабатывают кадры на основе *алгоритма прозрачного моста (transparent bridge*), который определен стандартом IEEE 802.1D. Процесс работы алгоритма прозрачного моста начинается с построения *таблицы коммутации* (Forwarding DataBase, FDB) или *таблицы MAC-адресов*. Напомним, что сети Ethernet являются сетями с коммутацией пакетов. Коммутация пакетов основана на таблицах, которые хранятся в памяти и содержат информацию, позволяющую определить путь до места назначения пакета.

```
DES-3528:5#show fdb
Command: show fdb

 Unicast MAC Address Aging Time  = 300

 VID  VLAN Name                         MAC Address       Port  Type
 ---- --------------------------------- ----------------- ----- ----------

 1    default                           1C-AF-F7-4C-5C-70 CPU   Self
 1    default                           20-6A-8A-72-A5-82 1     Dynamic
 1    default                           20-6A-8A-73-7C-8C 9     Permanent

Total Entries: 3
```

Рис. 6.1 Таблица коммутации

Изначально таблица коммутации пуста. При включении питания, одновременно с передачей данных, коммутатор изучает расположение подключенных к нему сетевых устройств путем анализа MAC-адресов источников получаемых кадров. Например, если на порт 1 коммутатора, показанного на **Ошибка! Источник ссылки не найден.**, поступает кадр от узла A, то он создает в таблице коммутации запись, ассоциирующую MAC-адрес узла A с номером входного порта. Записи в таблице коммутации создаются динамически, т.е. как только коммутатором будет прочитан новый MAC-адрес, то он сразу будет занесен в таблицу коммутации. Дополнительно к MAC-адресу и ассоциированному с ним порту в таблицу коммутации для каждой записи заносится время старения (aging time). Время старения позволяет коммутатору автоматически реагировать на перемещение, добавление или удаление сетевых устройств. Каждый раз, когда идет обращение по какому-либо MAC-адресу, соответствующая запись получает новое время старения. Записи, по которым не обращались долгое время, из таблицы удаляются. Это позволяет хранить в таблице коммутации только актуальные MAC-адреса, что уменьшает время поиска соответствующей записи и гарантирует, что она не будет использовать слишком много системной памяти.

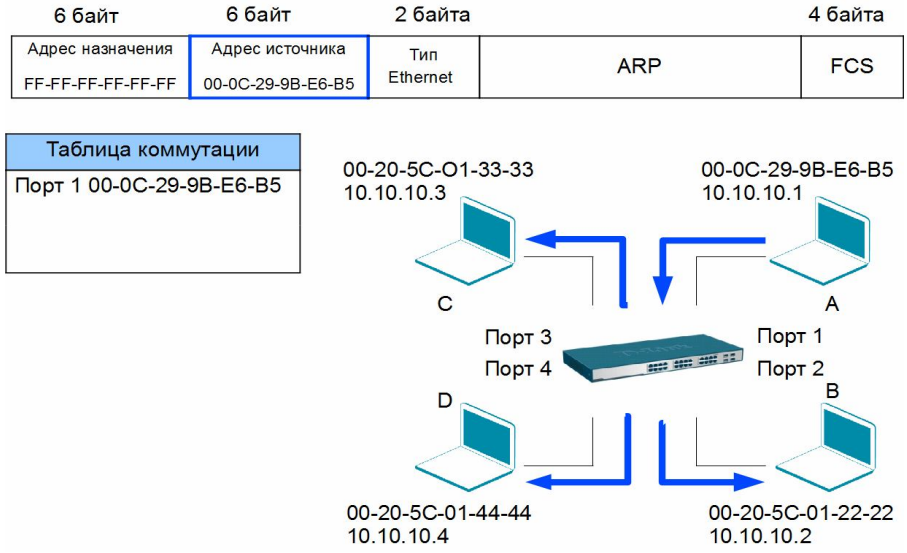


Рис. 6.2 Построение таблицы коммутации

Помимо динамического создания записей в таблице коммутации в процессе самообучения коммутатора, существует возможность создания статических записей таблицы коммутации вручную. Статическим записям в отличие от динамических не назначается время старения.

Статическую таблицу коммутации удобно использовать для повышения сетевой безопасности, когда необходимо гарантировать подключение к сети только устройств с определенными MAC-адресами. В этом случае необходимо отключить автоизучение MAC-адресов на портах коммутатора.

Внимание: как правило, размер статической таблицы коммутации меньше размера динамической. Размеры обеих таблиц также зависят от модели коммутатора. Обычно производители указывают размеры таблиц коммутации в спецификациях устройств.

Если в таблице коммутации появляется хотя бы одна запись, то коммутатор начинает использовать ее для пересылки кадров. Рассмотрим пример, показанный на **Ошибка! Источник ссылки не найден.**, описывающий процесс пересылки кадров между портами коммутатора.

Когда коммутатор получает кадр, отправленный компьютером A компьютеру B, он извлекает из него MAC-адрес назначения и ищет этот MAC-адрес в своей таблице коммутации. Как только в таблице коммутации будет найдена запись, ассоциирующая MAC-адрес назначения (компьютера B) с одним из портов коммутатора, за исключением порта-источника, кадр будет передан через соответствующий выходной порт (в приведенном примере – порт 2). Этот процесс называется продвижением (forwarding) кадра.

Если бы выходной порт и порт-источник совпали, то передаваемый кадр был бы отброшен коммутатором. Этот процесс называется *фильтрацией (filtering)*.

В том случае, если MAC-адрес назначения в поступившем кадре неизвестен (в таблице коммутации отсутствует соответствующая запись), коммутатор создает множество копий этого кадра и передает их через все свои порты, за исключением того, на который он поступил. Этот процесс называется *лавинной передачей (flooding)*. Несмотря на то, что процесс лавинной передачи занимает полосу пропускания, он позволяет коммутатору избежать потери кадров, когда MAC-адрес приемника неизвестен.

Помимо лавинной передачи одноадресных кадров, коммутаторы также выполняют лавинную передачу многоадресных и широковещательных кадров, которые генерируются сетевыми мультимедийными приложениями.

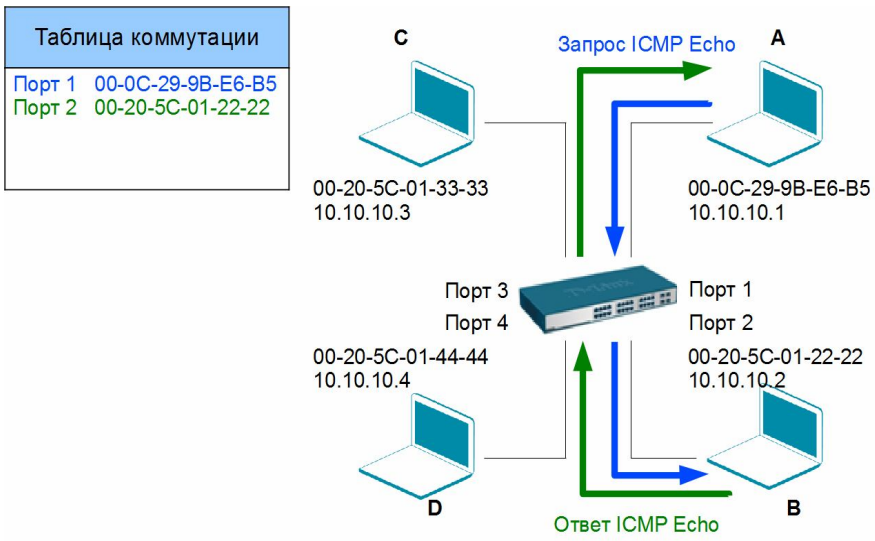


Рис. 6.3 Передача кадра с порта на порт коммутатора

6.2 Методы коммутации

Прежде чем принять решение о передаче кадра, коммутатор получает и анализирует его содержимое. В современных коммутаторах используются следующие методы коммутации пакетов, определяющие поведение устройства при получении кадра:

- коммутация с промежуточным хранением (store-and-forward);
- коммутация без буферизации (cut-through).

Оба метода коммутации пакетов принимают решение о продвижении кадров на основе MAC-адреса получателя, но отличаются последовательностью действий, которые коммутатор выполнит, прежде чем передать или отбросить поступивший на его порт кадр.

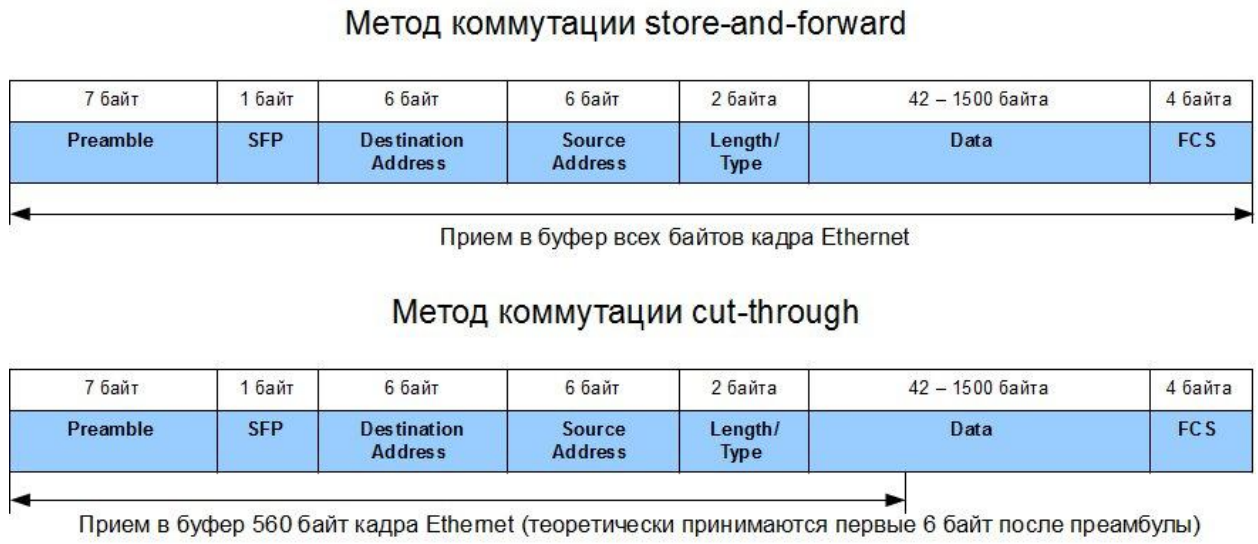


Рис. 6.4 Методы коммутации

Метод коммутации с промежуточным хранением (store-and-forward) исторически появился первым. Он характеризуется тем, что коммутатор, прежде чем передать кадр, полностью копирует его в буфер и производит проверку на наличие ошибок. Если кадр содержит ошибки (не совпадает контрольная сумма, или кадр меньше 64 байт или больше 1518 байт), то он отбрасывается. Если кадр не содержит ошибок, то коммутатор находит MAC-адрес приемника в своей таблице коммутации и определяет выходной порт. Затем, если не определены никакие фильтры, коммутатор передает кадр через соответствующий порт устройству назначения.

Несмотря на то, что этот способ передачи связан с задержками (чем больше размер кадра, тем больше времени требуется на его прием и проверку на наличие ошибок), он обладает двумя существенными преимуществами:

- коммутатор может быть оснащен портами, поддерживающими разные технологии и скорости передачи, например, 10/100 Мбит/с, 1000 Мбит/с и 10 Гбит/с;

- коммутатор может проверять целостность кадра, благодаря чему поврежденные кадры не будут передаваться в соответствующие сегменты.

В большинстве коммутаторах D-Link реализован этот метод коммутации. Благодаря использованию в устройствах высокопроизводительных процессоров и контроллеров ASIC (Application-Specific Integrated Circuit), задержка, вносимая коммутацией store-and-forward при передаче кадров, оказывается незначительной.

Коммутация без буферизации (cut-through) была реализована в первом коммутаторе Ethernet, разработанном фирмой Kalpana в 1990 г. При работе в этом режиме теоретически коммутатор копирует в буфер только MAC-адрес назначения (первые 6 байт после преамбулы) и сразу начинает передавать кадр, не дожидаясь его полного приема. Однако

современные коммутаторы не всегда реализуют коммутацию без буферизации в классическом варианте. В зависимости от реализации коммутатор дожидается приема в буфер определенного количества байтов кадра и, если на порте не определены никакие фильтры, принимает решение о его передаче. Так как при работе в режиме cut-through коммутатор не дожидается приема всего кадра, то он не выполняет проверку кадров на наличие ошибок. Проверка кадра на наличие ошибок возлагается на принимающий узел. Однако, современная сетевая инфраструктура, включающая оборудование и кабельную систему позволяет свести вероятность возникновения ошибочных кадров к минимуму.

Основным преимуществом коммутация без буферизации по сравнению с коммутацией с промежуточным хранением является уменьшение времени передачи кадров большого размера. Например, если приложение использует Jumbo-фреймы (кадры размером до 10 000 байт), то коммутатор, работающий в режиме cut-through, будет передавать данные на несколько микро или миллисекунд (в зависимости от скорости портов коммутатора) быстрее коммутатора, использующего режим store-and-forward.

Помимо этого, коммутаторы с поддержкой режима cut-through хорошо подходят для использования в сетях, например в центрах обработки данных, с приложениями критичными к задержкам.

Однако в некоторых случаях, метод cut-through теряет свои преимущества в скорости передачи. Это может произойти при перегрузке сети, использовании функций фильтрации, требующих обработки на ЦПУ, или когда порты коммутатора поддерживают разную скорость (если коммутационная матрица плохо спроектирована).

Коммутаторы D-Link серии DXS-3600-xx обеспечивают гибкость в выборе метода коммутации, т.к. поддерживают selectable store-and-forward/cut-through mode. По умолчанию в коммутаторах этой серии используется режим store-and-forward, поэтому для получения преимуществ от использования режима cut-through, администратор сети должен сначала его активизировать. Коммутатор будет копировать в буфер и изучать первые 560 байт кадра. Если размер кадра окажется больше 560 байт, коммутатор автоматически переключится в режим cut-through и начнет процесс продвижения кадра, не дожидаясь его полного приема. Соответственно для кадров, чей размер меньше или равен 560 байт будет использоваться режим коммутации store-and-forward.

6.3 Конструктивное исполнение коммутаторов

В зависимости от конструктивного исполнения (габаритных размеров), можно выделить три группы коммутаторов:

- настольные коммутаторы (Desktop switch);
- автономные коммутаторы, монтируемые в телекоммуникационную стойку (Rack mounted switch);
- коммутаторы на основе шасси (Chassis switch).

Как следует из названия, *настольные коммутаторы* не предназначены для размещения в стойках и иногда они могут оснащаться, входящими в комплект поставки скобами для крепления на стену. Обычно такие коммутаторы обладают корпусом обтекаемой формы с относительно небольшим количеством фиксированных портов (у коммутаторов D-Link количество портов варьируется от 5 до 16), внешним или внутренним блоком питания, ножками (обычно резиновыми) для обеспечения вентиляции нижней поверхности устройства. Чаще всего коммутаторы настольного форм-фактора используются в сетях класса *SOHO* (*Small Office, Home Office*), где не требуется высокая производительность и расширенные сетевые функции. В качестве примера коммутатора в настольном исполнении можно привести коммутатор D-Link модели DES-1005A.

Рис. 6.5 Коммутатор DES-1005A с 5 портами 10/100BASE-T

Автономные коммутаторы в стоечном исполнении высотой 1U (unit) имеют корпус для монтажа в 19” стойку, встроенным блоком питания и фиксированным количеством портов (у коммутаторов D-Link количество портов может достигать 52). По сравнению с настольными коммутаторы, монтируемые в стойку, обеспечивают более высокую производительность и надежность, а также предлагают широкий набор сетевых функций и интерфейсов. Как правило, такие коммутаторы используются на уровнях доступа и распределения сетей малых и средних предприятий (*Small to Medium Business, SMB*), корпоративных сетей и сетей провайдеров услуг (*Internet Service Provider, ISP*).

Рис. 6.6 Коммутатор DGS-1510-28 с 24 портами 10/100/1000BASE-T, 4 портами SFP и функцией энергосбережения

Среди коммутаторов в стоечном исполнении с фиксированным количеством портов можно выделить в отдельную группу *стековые коммутаторы*. Эти устройства представляют собой коммутаторы, которые могут работать как автономно, потому что выполнены в отдельном корпусе, так и совместно благодаря наличию специальных интерфейсов, позволяющих объединять коммутаторы в одно логическое устройство для увеличения количества портов, удобства управления и мониторинга. В этом случае отдельные коммутаторы образуют *стек*.

Коммутаторы на основе шасси содержат слоты, которые могут быть использованы для установки интерфейсных модулей расширения, резервных источников питания и процессорных модулей. Модульное решение обеспечивает гибкость применения, высокую плотность портов и возможность резервирования критичных для функционирования коммутатора компонентов. Модули такого коммутатора поддерживают технологию «*hot swap*» (горячая замена), т. е. допускают замену без выключения питания коммутатора. Коммутаторы на основе шасси предназначены для работы в крупных корпоративных магистральных сетях, городских сетях или сетях операторов связи.

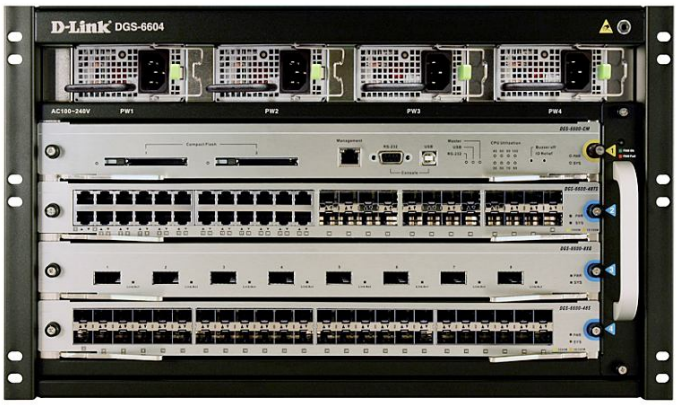
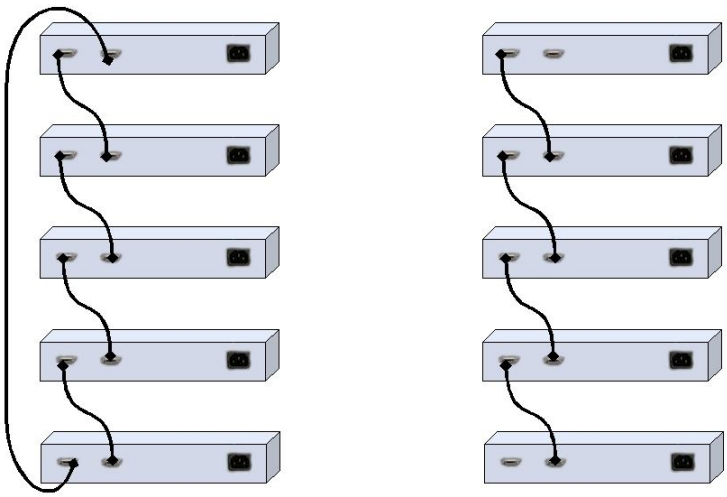


Рис. 6.7 Шасси 3 уровня DGS-6604 с 4 слотами расширения

6.4 Физическое стекирование коммутаторов

Под *физическим стекированием* понимается объединение нескольких коммутаторов в одно логическое устройство. Объединенные в стек коммутаторы имеют общие таблицы коммутации и маршрутизации (для коммутаторов 3 уровня).

В коммутаторах D-Link используются две топологии физического стекирования: «*кольцо*» (ring) и «*цепочка*» (chain).



Топология стекирования «кольцо» **Топология стекирования «цепочка»**

Рис. 6.8 Топологии стекирования «кольцо» и «цепочка»

Стек кольцевой топологии строится по следующей схеме: каждое устройство в стеке подключается к вышележащему и нижележащему, при этом самый нижний и самый верхний коммутатор в стеке также соединяются. При передаче данных кадр последовательно передается от одного устройства стека к другому до тех пор, пока не достигнет порта назначения. Система автоматически определяет оптимальный путь передачи трафика, что позволяет достичь полного использования полосы пропускания. Преимуществом кольцевой топологии является то, что при выходе одного устройства из строя или обрыве связи остальные устройства стека продолжат работу в обычном режиме.

В *стеке линейной топологии* каждое устройство также соединено с вышележащим и нижележащим, но самый верхний и самый нижний коммутаторы не соединяются.

Физическое стекирование по линейной и кольцевой топологии реализовано в следующих сериях коммутаторов D-Link. Коммутаторы серии DGS-3120-xx позволяют объединить в стек до 6 устройств, коммутаторы серии DGS-3610-xx – до 8 устройств, а коммутаторы серий DGS-3420-xx , DGS-36xx, DGS-3620-xx – до 12 устройств, используя интерфейсы 10 Gigabit Ethernet (10GE). Коммутаторы серии DGS-31xx объединяются в стек через интерфейсы HDMI. Максимальное количество коммутаторов в стеке равно 6. Коммутаторы серии DES-3528/3552 поддерживают физическое стекирование через интерфейсы Gigabit Ethernet и позволяют объединить в стек до 8 устройств.

Все устройства стека управляются через один IP-адрес. Передача данных между ними ведется в полнодуплексном режиме.

6.5 Технологии коммутации и модель OSI

Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями модели OSI, на которых они передают, фильтруют и коммутируют кадры. Различают коммутаторы уровня 2 (Layer 2 (L2) Switch) и коммутаторы уровня 3 (Layer 3 (L3) Switch).

Коммутаторы уровня 2 анализируют входящие кадры, принимают решение об их дальнейшей передаче и передают их пунктам назначения на основе MAC-адресов канального уровня модели OSI. Основное преимущество коммутаторов уровня 2 – прозрачность для протоколов верхнего уровня. Т.к. коммутатор функционирует на 2-м уровне, ему нет необходимости анализировать информацию верхних уровней модели OSI.

Коммутация 2-го уровня – аппаратная. Она обладает высокой производительностью. Передача кадра в коммутаторе может осуществляться специализированным контроллером ASIC. В основном коммутаторы 2-го уровня используются для сегментации сети и объединения рабочих групп.

Несмотря на преимущества коммутации 2-го уровня, она все же имеет некоторые ограничения. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров по всем сегментам сети.

Коммутатор уровня 3 осуществляют коммутацию и фильтрацию на основе адресов канального (уровень 2) и сетевого (уровень 3) уровней модели OSI. Коммутаторы 3-го уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

Коммутаторы уровня 3 осуществляют маршрутизацию пакетов аналогично традиционным маршрутизаторам. Они поддерживают протоколы маршрутизации RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), для обеспечения связи с другими коммутаторами уровня 3 или маршрутизаторами и построения таблиц маршрутизации, осуществляют маршрутизацию на основе политик, управление многоадресным трафиком.

Существует две разновидности маршрутизации: аппаратная (коммутация 3 уровня) и программная. При аппаратной реализации пересылка пакетов осуществляется при помощи специализированных контроллеров ASIC. При программной реализации, для пересылки пакетов устройство использует центральный процессор. Обычно в коммутаторах 3 уровня и старших моделях маршрутизаторов маршрутизация пакетов аппаратная, что позволяет выполнять ее на скорости канала связи, а в маршрутизаторах общего назначения функция маршрутизации выполняется программно.

6.6 Программное обеспечение коммутаторов

Программное обеспечение коммутаторов D-Link предоставляет набор сервисов, предназначенных для выполнения различных функций, обеспечивающих безопасность, отказоустойчивость сети, управление многоадресной рассылкой, качество обслуживания

(QoS), а также развитые средства настройки и управления. Помимо этого, программное обеспечение коммутаторов взаимодействует с приложениями D-Link D-View v.6, представляющими собой прикладные программы сетевого управления. Эти управляющие программы поддерживаются всей линейкой управляемых коммутаторов D-Link.

Системное программное обеспечение располагается во Flash-памяти коммутатора, размер которой, в зависимости от модели, может доходить до 32 Мбайт. Компания D-Link предоставляет возможность бесплатного обновления программного обеспечения коммутаторов по мере появления новых версий с обновленным функционалом.

6.7 Общие принципы сетевого дизайна

Грамотный сетевой проект основывается на многих принципах, базовыми из которых являются:

- *Изучение возможных точек отказа сети*. Для того чтобы единичный отказ не мог изолировать какой-либо из сегментов сети, в ней должна быть предусмотрена избыточность. Под избыточностью понимается резервирование жизненно важных компонентов сети и распределение нагрузки. Так, в случае отказа в сети может существовать альтернативный или резервный путь к любому ее сегменту. Распределение нагрузки используется в том случае, если к пункту назначения имеется два или более путей, которые могут использоваться в зависимости от загруженности сети. Требуемый уровень избыточности сети меняется в зависимости от ее конкретной реализации.
- *Определение типа трафика сети*. Например, если в сети используются клиент-серверные приложения, то поток вырабатываемого ими трафика является критичным для эффективного распределения ресурсов, таких как количество клиентов, использующих определенный сервер, или количество клиентских рабочих станций в сегменте.
- *Анализ доступной полосы пропускания*. В сети не должно быть большого различия в доступной полосе пропускания между различными уровнями иерархической модели (описание иерархической модели сети находится в следующем разделе). Важно помнить, что иерархическая модель ссылается на концептуальные уровни, которые обеспечивают функциональность.
- *Создание сети на базе иерархической или модульной модели*. Иерархия позволяет объединить через межсетевые устройства отдельные сегменты, которые будут функционировать как единая сеть. Фактическая граница между уровнями не обязательно должна проходить по физическому каналу связи – ей может быть и внутренняя магистраль определенного устройства.

6.8 Трехуровневая иерархическая модель сети

Иерархическая модель определяет подход к проектированию сетей и включает в себя три логических уровня (Рис. 6.9):

- уровень доступа *(access layer);*
- уровень распределения/агрегации *(distribution layer);*
- уровень ядра *(core layer)*.

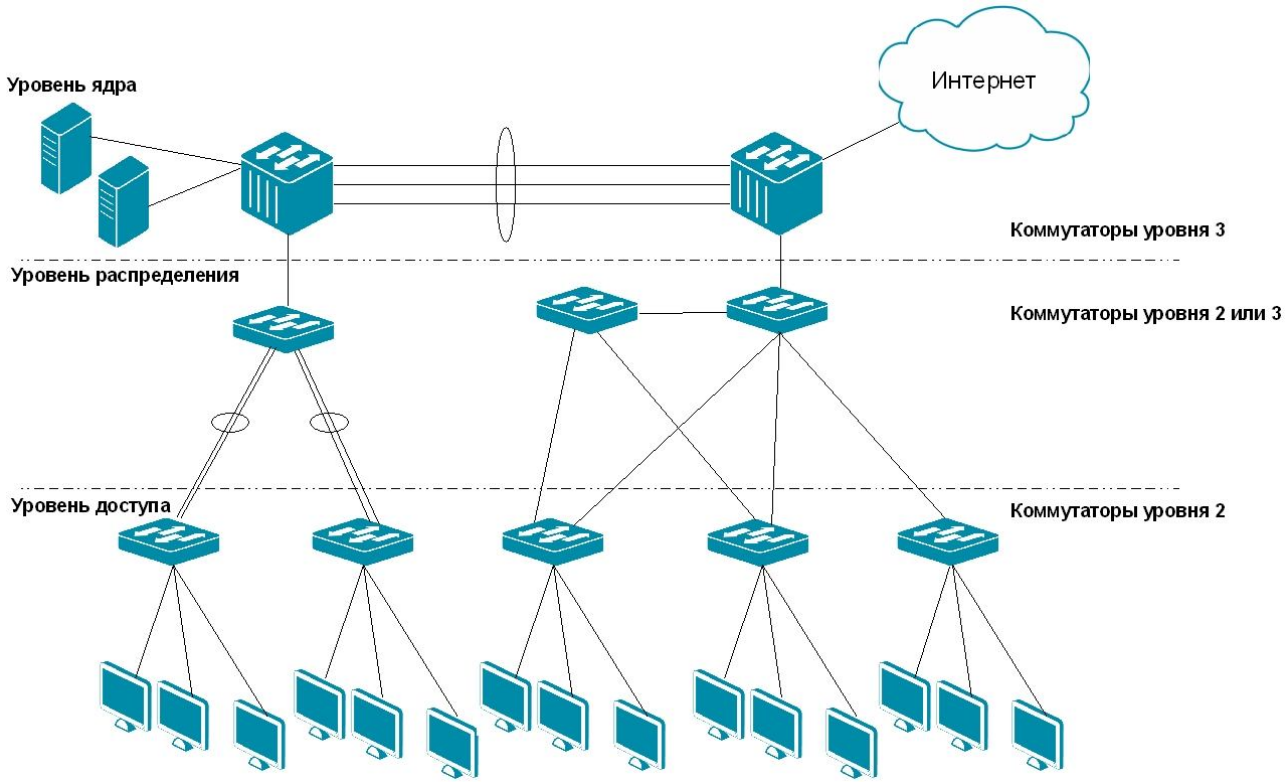


Рис. 6.9 Трехуровневая модель сети

Для каждого уровня определены свои функции. Три уровня не обязательно предполагают наличие трех различных устройств. Если провести аналогию с иерархической моделью OSI, то в ней отдельный протокол не всегда соответствует одному из семи уровней. Иногда протокол соответствует более чем одному уровню модели OSI, а иногда несколько протоколов реализованы в рамках одного уровня. Так и при построении иерархических сетей, на одном уровне может быть как несколько устройств, так и одно устройство, выполняющее все функции, определенные на двух соседних уровнях.

Уровень ядра отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские данные обрабатываются на уровне распределения, который при необходимости пересылает запросы к ядру.

Для уровня ядра большое значение имеет его отказоустойчивость, поскольку сбой на этом уровне может привести к потере связности сети.

Уровень распределения, который иногда называют уровнем рабочих групп, является связующим звеном между уровнями доступа и ядра. В зависимости от способа реализации, уровень распределения может выполнять следующие функции:

- обеспечение маршрутизации, качества обслуживания и безопасности сети;
- агрегирование каналов;
- переход от одной технологии к другой (например, от 100BASE-TX к 1000BASE-T).

Уровень доступа управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть. Уровень выполняет следующие функции:

- управление доступом пользователей, фильтрация трафика, обеспечение качества обслуживания (QoS);
- сегментация;
- подключение рабочих групп к уровню распределения;
- использование технологии коммутируемых локальных сетей.

6.9 Протокол Spanning Tree Protocol (STP)

Сеть с несколькими маршрутами между источником и приемником отличается повышенной отказоустойчивостью. Для обеспечения отказоустойчивости в сетях, построенных на коммутаторах, часто создаются резервные соединения между ними. В случае если какой-то коммутатор или канал вышли из строя, то оставшиеся работоспособные каналы или коммутаторы принимают на себя функции поврежденного. Хотя резервные каналы связи полезны, их создание может привести к появлению *коммуникационных петель*. Также петли могут возникнуть из-за ошибок администратора.

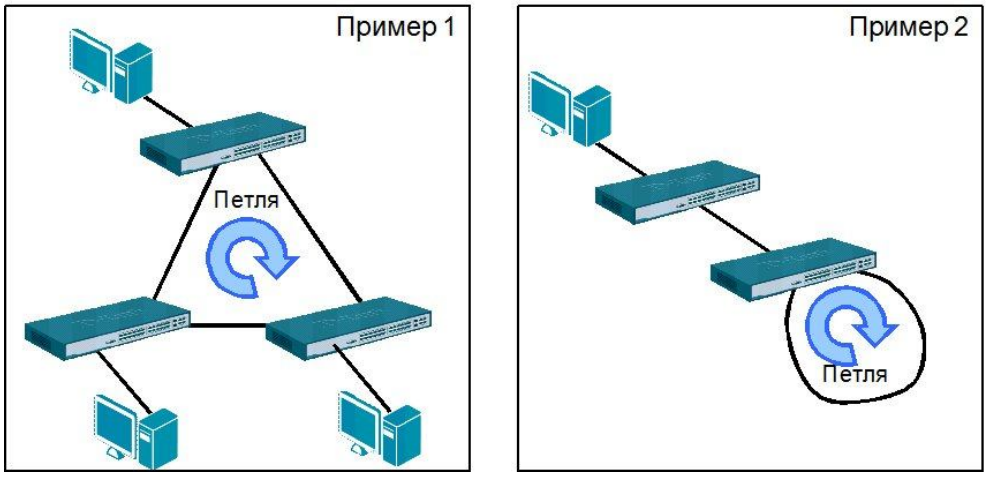


Рис. 6.10 Примеры петель между коммутаторами

Коммутаторы не могут корректно функционировать в среде, в которой существуют петли. Это связано с принципом работы коммутаторов. Алгоритм прозрачного моста позволяет только изучить расположение оборудования, подключенного к коммутатору, но не позволяет определить точную топологию сети и выбрать наилучший путь передачи сообщения. Поэтому наличие петель в коммутируемых сетях приводит к ряду проблем, среди которых бесконечное обновление таблиц коммутации и широковещательные штормы.

Предположим, что кадр, поступивший от одного из узлов на коммутатор, является широковещательным. Коммутатор создаст множество копий этого кадра и передает их через все свои порты, за исключением того, на который он поступил. Если в сети имеется несколько маршрутов между сегментами локальной сети, то коммутаторы будут бесконечно передавать получаемые ими широковещательные кадры (в отличие от пакета сетевого уровня, у кадра нет поля, определяющего время его жизни), используя всю доступную полосу пропускания сети и блокируя передачу других кадров во всех сегментах. Возникнет «широковещательный шторм».

Еще одна проблема заключается в том, что коммутатор нередко получает несколько копий одного кадра, одновременно приходящих из нескольких сегментов сети. В этом случае по таблице коммутации невозможно определить расположение отправителя, поскольку коммутатор получит кадр из нескольких каналов. Может быть так, что коммутатор вообще не сможет переслать кадр, так как будет постоянно выполнять одну задачу – обновлять таблицу коммутации.

Одна из самых сложных проблем – это множественные петли, образующиеся в объединенной сети. Существует возможность появления петли внутри других петель. Если за этим последует широковещательный шторм, то сеть не сможет выполнять коммутацию кадров.

Для решения этих проблем был разработан **протокол связующего** или **остового дерева** (*Spanning Tree Protocol, STP*), который определен в стандарте IEEE 802.1D-1998.

Протокол STP является протоколом 2 уровня модели OSI, который позволяет строить древовидные свободные от петель конфигурации связей между коммутаторами локальной сети. В результате работы протокола STP между двумя рабочими станциями сети всегда существует *только один* активный путь. Помимо этого обеспечивается возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода из строя активных каналов.

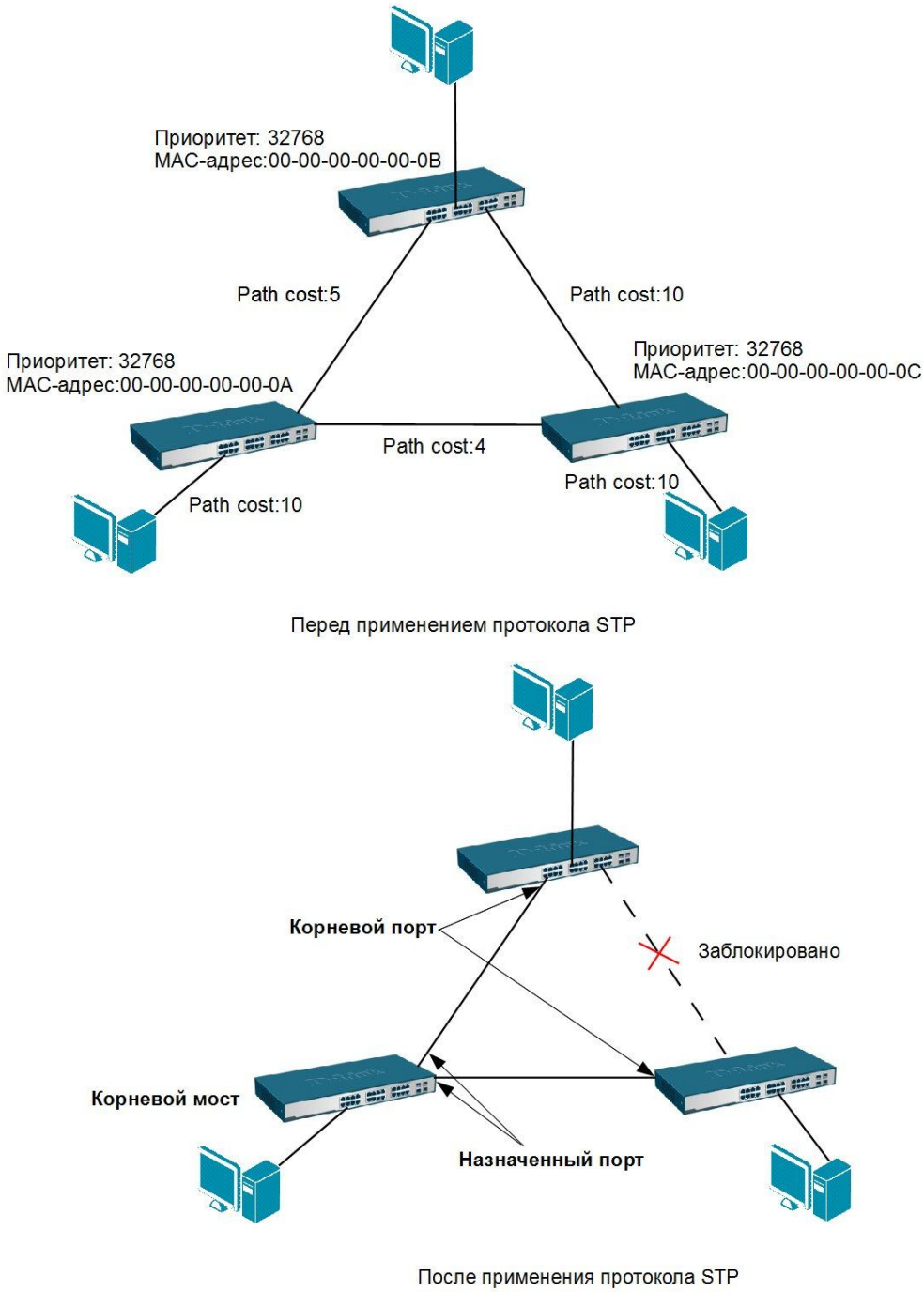


Рис. 6.11 Пример функционирования протокола STP

Коммутаторы, поддерживающие протокол STP, автоматически создают древовидную конфигурацию связей без петель в компьютерной сети. Такая конфигурация называется связующим деревом (Spanning Tree), иногда ее называют остовым или покрывающим деревом. Конфигурация связующего дерева строится коммутаторами автоматически с

использованием обмена служебными кадрами, называемыми Bridge Protocol Data Units (BPDU).

В настоящее время существуют следующие версии протоколов связующего дерева:

- IEEE 802.1D Spanning Tree Protocol (STP);
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP);
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

В данном курсе будет рассматриваться только протокол STP. Изучить принципы работы протоколов RSTP и MSTP можно в курсе «Технологии коммутации и маршрутизации современных сетей Ethernet. Базовый курс D-Link» на портале дистанционного обучения и сертификации D-Link http://learn.dlink.ru.

6.9.1 Построение активной топологии связующего дерева

Для построения устойчивой активной топологии с помощью протокола STP с каждым коммутатором сети ассоциируется уникальный *идентификатор моста (Bridge ID)*, а с каждым портом коммутатора – *стоимость пути (Path Cost)* и *идентификатор порта* (*Port ID*).

Процесс вычисления остового дерева начинается с выбора **корневого моста** *(Root Bridge),* от которого будет строиться дерево. В качестве корня дерева выбирается коммутатор с наименьшим значением идентификатора моста. Идентификатор моста – это 8-байтное поле, которое состоит из 2-х частей: приоритета моста (2 байта), назначаемого администратором (диапазон значений приоритетов: 0 - 61 440, шаг 4096), и MAC-адреса блока управления коммутатора (6 байт).

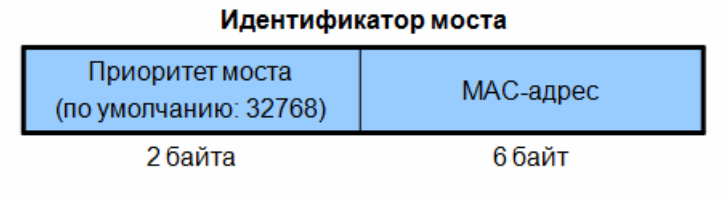


Рис. 6.12 Идентификатор моста

При сравнении идентификаторов двух коммутаторов, сначала рассматривают значения приоритетов. Корневым мостом становится коммутатор с наименьшим значением приоритета. Если приоритеты одинаковы (по умолчанию приоритет равен 32768), то сравниваются MAC-адреса. Устройство с наименьшим MAC-адресом становится корневым мостом.

Рис. 6.13 Выборы корневого моста

В примере, показанном на рисунке Рис. 6.13, корневым мостом становится Коммутатор 1, т.к. при равных приоритетах он имеет наименьший MAC-адрес.

Для того чтобы в качестве корневого моста было выбрано определенное устройство (исходя из структуры сети), администратор может вручную назначить соответствующему коммутатору наименьшее значение приоритета.

Второй этап работы STP – выбор **корневых портов** *(Root Port)*.

После окончания процесса выбора корневого моста, оставшиеся коммутаторы сети определяют стоимость каждого возможного пути от себя до корня дерева (Root Path Cost), которая рассчитывается как *суммарное условное время* на передачу данных от порта данного коммутатора до порта корневого моста. Условное время сегмента рассчитывается, как время передачи одного бита информации через канал с определенной полосой пропускания. Рекомендованные значения стоимости пути по умолчанию с учетом скорости передачи канала определены в стандартах IEEE 802.1D-1998 и IEEE 802.1D-2004. Значения, указанные в стандарте IEEE 802.1D-2004 рекомендуется использовать для совместимости с протоколами RSTP и MSTP.

Таблица 6.1 Стоимость пути STP в соответствии со стандартом IEEE 802.1D-1998

Параметр	**Скорость канала**	**Рекомендованное значение**	**Рекомендованный диапазон**	**Диапазон значений**
Стоимость пути	4 Мбит/с	250	100–1000	1–65 535
Стоимость пути	10 Мбит/с	100	50–600	1–65 535
Стоимость пути	16 Мбит/с	62	40–400	1–65 535
Стоимость пути	100 Мбит/с	19	10–60	1–65 535
Стоимость пути	1 Гбит/с	10	3–10	1–65 535
Стоимость пути	10 Гбит/с	2	1–5	1–65 535

Таблица 6.2 Стоимость пути STP в соответствии со стандартом IEEE 802.1D-2004

Параметр	**Скорость канала**	**Рекомендованное значение**	**Рекомендованный диапазон**	**Диапазон значений**
Стоимость пути	10 Мбит/с	2 000 000	200 000–20 000 000	1–200 000 000
Стоимость пути	100 Мбит/с	200 000	20 000–2 000 000	1–200 000 000
Стоимость пути	1 Гбит/с	20 000	2 000–200 000	1–200 000 000
Стоимость пути	10 Гбит/с	2 000	200–20 000	1–200 000 000

Сравнив стоимости всех возможных маршрутов до корня, каждый коммутатор выбирает среди них один, с наименьшим значением стоимости. Порт, соединяющий коммутатор с этим маршрутом, становится корневым портом. В случае если минимальные стоимости пути нескольких маршрутов окажутся одинаковыми, корневым портом станет порт, имеющий наименьшее значение идентификатора порта.

Рис. 6.14 Выбор корневых портов

Продолжим рассмотрение примера (рисунокРис. 6.14). Между Коммутатором 1 и Коммутатором 2 имеются два канала связи: один канал со скоростью передачи 1 Гбит/с, второй канал со скоростью передачи 100 Мбит/с. Для того чтобы определить, какой из портов Коммутатора 2 (порт 1 или порт 2) станет корневым, необходимо сравнить стоимость каждого из маршрутов до корневого моста. В соответствии с рекомендованными стандартом IEEE 802.1D-2004 значениями стоимость пути через канал со скоростью 1 Гбит/с равна 20 000, стоимость пути через канал 100 Мбит/с равна 200 000. Стоимость маршрута через порт 1 Коммутатора 2 до корневого моста является наименьшей, поэтому порт 1 становится корневым портом Коммутатора 2.

Третий шаг работы STP – определение **назначенных портов** *(Designated Port)*.

Каждый сегмент в коммутируемой сети имеет один назначенный порт. Этот порт функционирует как единственный порт моста, т.е. принимает кадры от сегмента и передает их в направлении корневого моста через корневой порт данного коммутатора. Коммутатор, содержащий назначенный порт для данного сегмента, называется **назначенным мостом** *(Designated Bridge)* этого сегмента. Назначенный порт сегмента определяется путем сравнения значений стоимости пути всех маршрутов от данного сегмента до корневого моста. Им становится порт, имеющий наименьшее значение стоимости среди всех портов, подключенных к данному сегменту. Если минимальные значения стоимости пути окажутся одинаковыми у двух или нескольких портов, то для выбора назначенного порта сегмента STP принимает решение на основе последовательного сравнения идентификаторов мостов и идентификаторов портов.

У корневого моста все порты являются назначенными, а их расстояние до корня полагается равным нулю. Корневого порта у корневого моста нет.

После выбора корневых и назначенных портов все остальные порты коммутаторов сети переводятся в состояние Blocking («Блокировка»), т. е. такое, при котором они принимают и передают только кадры BPDU. При таком выборе активных портов в сети исключаются петли, а оставшиеся связи образуют связующее дерево.

Продолжим рассмотрение примера (Рис. 6.15). В сегменте, соединяющем порт 2 Коммутатора 1 и порт 2 Коммутатора 2 надо заблокировать один из портов. Коммутатор 1 является корневым мостом, поэтому у порта 2 Коммутатора 1 расстояние до корневого моста равно 0, следовательно, порт 2 Коммутатора 2 будет заблокирован. Порт 3 Коммутатора 2 является назначенным портом для данного сегмента, т.к. от него имеется только один маршрут до корневого моста.

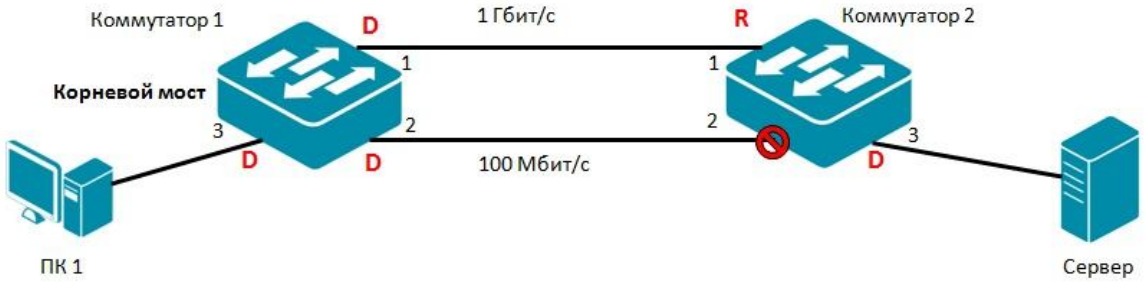


Рис. 6.15 Определение назначенных портов

6.9.2 Bridge Protocol Data Unit (BPDU)

Вычисление структуры связующего дерева происходит при включении коммутатора и при изменении топологии. Эти вычисления требуют периодического обмена информацией между коммутаторами связующего дерева, что достигается при помощи специальных кадров, называемых блоками данных протокола моста – BPDU (Bridge Protocol Data Unit).

Коммутатор отправляет BPDU, используя уникальный MAC-адрес порта в качестве адреса-отправителя и групповой MAC-адрес протокола STP 01-80-C2-00-00-00 в качестве адреса-получателя. Кадры BPDU помещаются в поле данных кадров канального уровня, например кадров Ethernet.

Внимание: иногда, с целью повышения безопасности администраторам необходимо отключать возможность передачи кадров BPDU на граничные коммутаторы сети, чтобы избежать получения случайных кадров BPDU клиентскими портами, которые могут распространить вычисления STP по клиентским сетям. Управляемые коммутаторы D-Link поддерживают возможность включения и отключения передачи кадров BPDU для каждого порта.

Существует три типа кадров BPDU:

- Configuration BPDU (CBPDU) – конфигурационный кадр BPDU, который используется для вычисления связующего дерева (тип сообщения: 0x00).
- Topology Change Notification (TCN) BPDU – уведомление об изменении топологии сети (тип сообщения: 0x80).
- Topology Change Notification Acknowledgement (TCA) – подтверждение о получении уведомления об изменении топологии сети.

Коммутаторы обмениваются BPDU через равные интервалы времени (по умолчанию 2 с), что позволяет им отслеживать состояние топологии сети.

	Байты
Идентификатор протокола (Protocol Identifier)	2
Версия протокола (Protocol Version Identifier)	1
Тип BPDU (BPDU Type)	1
Флаги (Flags)	1
Идентификатор корневого моста (Root Identifier)	8
Расстояние до корневого моста (Root Path Cost)	2
Идентификатор моста (Bridge Identifier)	8
Идентификатор порта (Port Identifier)	2
Время жизни сообщения (Message Age)	2
Максимальное время жизни сообщения (Max Age)	2
Время приветствия (Hello Time)	2
Задержка смены состояний (Forward Delay)	2

Рис. 6.16 Формат кадра BPDU

Кадр BPDU состоит из следующих полей:

- Идентификатор протокола (Protocol Identifier) – занимает 2 байта, значение всегда равно 0.
- Версия протокола STP (Protocol Version Identifier) – 1 байт, значение всегда равно 0.
- Тип BPDU (BPDU Type) – 1 байт, значение «00» – конфигурационный BPDU, «01» – изменение топологии.
- Флаги (Flags) – 1 байт. Бит 1 – флаг изменения топологии, бит 8 – флаг подтверждения изменения топологии.
- Идентификатор корневого моста (Root Identifier) – 8 байт. Идентификатор текущего моста.
- Расстояние до корневого моста (Root Path Cost) – 2 байта. Суммарная стоимость пути до корневого моста.
- Идентификатор моста (Bridge Identifier) – 8 байт. Идентификатор текущего моста.
- Идентификатор порта (Port Identifier) – 2 байта. Уникальный идентификатор порта, который отправил этот BPDU.
- Время жизни сообщения (Message Age) – 2 байта. Нефиксированный временной интервал в секундах, прошедший с момента отправки BPDU корневым мостом. Служит для выявления устаревших сообщений BPDU. Первоначальное значение равно 0. По мере передачи кадра BPDU по сети, каждый коммутатор, добавляет ко времени жизни сообщения время его задержки данным коммутатором. По умолчанию оно равно 1 с. Значение параметра Message Age должно быть меньше значения таймера Max Age.
- Максимальное время жизни сообщения (Max Age) – 2 байта. Временной интервал в секундах, определяющий максимальное время хранения конфигурации STP, прежде чем коммутатор ее отбросит.
- Время приветствия (Hello Time) – 2 байта. Временной интервал в секундах, через который посылаются кадры BPDU.
- Задержка смены состояний (Forward Delay) – 2 байта. Временной интервал в секундах, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение».

6.9.3 Состояния портов

В процессе построения топологии сети каждый порт коммутатора проходит несколько стадий:

- **Blocking** («Блокировка») – при инициализации коммутатора все порты (за исключением отключенных) автоматически переводятся в состояние «Блокировка». В этом случае порт принимает и обрабатывает только кадры BPDU. Все остальные кадры отбрасываются.
- **Listening** («Прослушивание») – в этом состоянии порт продолжает принимать, обрабатывать и ретранслировать только кадры BPDU. Из этого состояния порт может перейти в состояние «Блокировка», если получит BPDU с лучшими параметрами, чем его собственные (стоимость пути, идентификатор моста или порта). В противном случае по истечении периода, установленного таймером задержки смены состояний (Forward Delay), порт перейдет в следующее состояние – «Обучение».
- **Learning** («Обучение») – порт начинает принимать все кадры и на основе MAC-адресов источника строить таблицу коммутации. В этом состоянии порт все еще не передает кадры, но продолжает участвовать в работе алгоритма STP и при поступлении BPDU с лучшими параметрами, переходит в состояние «Заблокирован». В противном случае по истечении периода, установленного таймером смены состояний, порт перейдет в следующее состояние – «Продвижение».
- **Forwarding** («Продвижение») – в этом состоянии порт может обрабатывать кадры данных в соответствии с построенной таблицей коммутации, а также принимать, передавать и обрабатывать кадры BPDU.
- **Disable** («Отключен») – в это состояние порт переводит администратор. Отключенный порт не участвует ни в работе протокола STP, ни в продвижении кадров данных. Порт можно также включить вручную, и он перейдет в состояние «Блокировка».

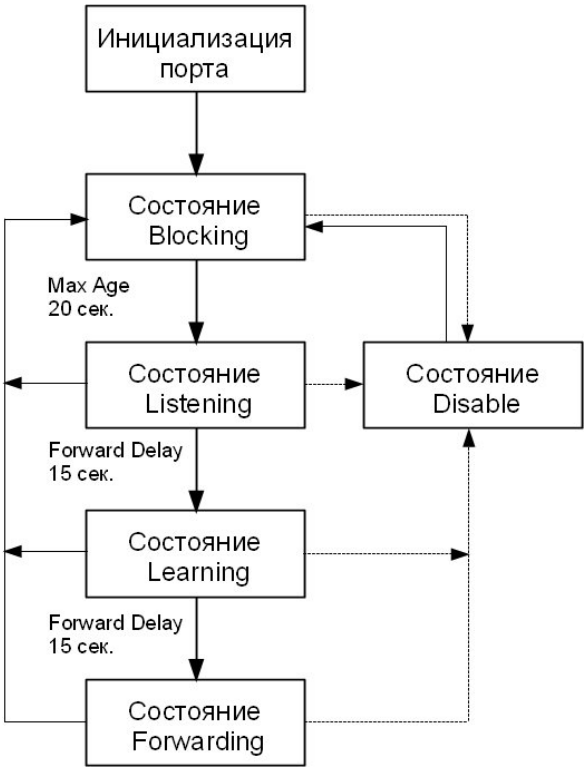


Рис. 6.17 Состояния портов при работе STP

В процессе нормальной работы корневой мост продолжает генерировать служебные кадры BPDU, а остальные коммутаторы продолжают их принимать своими корневыми портами и ретранслировать назначенными. Если по истечении максимального времени жизни сообщения (по умолчанию – 20 с) корневой порт любого коммутатора сети не получит служебный кадр BPDU, то он инициализирует новую процедуру построения связующего дерева.

6.9.4 Таймеры STP

Для того чтобы все коммутаторы сети имели возможность получить точную информацию о конфигурации связующего дерева, в протоколе STP используются следующие таймеры.

- **Hello Time** – интервал времени, через который корневой мост отправляет конфигурационные BPDU. Значение таймера Hello Time, настроенное на корневом мосту, будет определять значения таймеров Hello Time на всех некорневых коммутаторах, так как они просто пересылают конфигурационные BPDU, когда получают их от корневого. Значение таймера Hello Time по умолчанию 2 секунды, диапазон возможных значений от 1 до 10 секунд.
- **Forward Delay** – интервал времени, в течение которого порт коммутатора находится в состояниях «Прослушивание» и «Обучение». Такая задержка смены состояний необходима, чтобы исключить возможность временного возникновения альтернативных маршрутов при неодновременной смене состояний портов во время реконфигурации. Значение таймера Forward Delay по умолчанию 15 секунд, диапазон возможных значений от 4 до 30 секунд.
- **Max Age** – это интервал времени, в течение которого коммутатор хранит параметры текущей конфигурации связующего дерева. Значение таймера Max Age устанавливается корневым мостом и позволяет гарантировать, что все коммутаторы сети обладают одинаковой информацией о времени хранения конфигурации STP. Если период времени, определенный таймером истек, а коммутатор за это время не получил кадр BPDU от корневого моста, то он начинает считать себя корневым мостом и рассылает свои собственные BPDU всем коммутаторам сети, инициируя новую процедуру построения связующего дерева. Значение таймера Max Age по умолчанию 20 секунд, диапазон возможных значений от 6 до 40 секунд.

Значения таймеров Hello Time, Forward Delay и Max Age могут быть вручную настроены администратором на коммутаторе. Обычно эти настройки выполняются только на коммутаторе, являющемся корневым для данной топологии связующего дерева. При настройке важно помнить, что неправильно подобранные значения таймеров могут значительно увеличить время сходимости топологии STP и снизить производительность сети, поэтому рекомендуется использовать значения таймеров по умолчанию.

6.9.5 Изменение топологии

Коммутатор отправляет BPDU с уведомлением об изменении топологии (Topology Change Notification BPDU, TCN BPDU) в случае возникновения одного из следующих событий:

- некорневой мост получает сообщение TCN BPDU на свой назначенный порт;
- после истечения времени, определенного таймером Forward Delay, порт переходит в состояние Forwarding, но коммутатор уже имеет назначенный порт для данного сегмента;
- порт, находившийся в состоянии Forwarding или Listening, переходит в состояние Blocking (в случае проблем с каналом связи);
- коммутатор становится корневым мостом.

TCN BPDU отправляется коммутатором в тот сегмент сети, к которому подключен его корневой порт. Эти BPDU будут передаваться через интервал Hello Time до тех пор, пока коммутатор не получит подтверждение Topology Change Notification Acknowledgement (TCN-ACK) от вышестоящего коммутатора. Соседний коммутатор продолжит трансляцию TCN BPDU через свой корневой порт в направлении корневого моста сети, используя такую же процедуру. Этот процесс будет продолжаться до тех пор, пока TCN BPDU не достигнет корневого моста.

Когда корневой мост получает TCN BPDU или сам изменяет топологию, он устанавливает во всех передаваемых конфигурационных BPDU флаг изменения топологии (Topology Change, TC) на период времени, равный сумме значений таймеров Forward Delay и Max Age. Когда нижележащие коммутаторы получат конфигурационные BPDU с флагом Topology Change, они установят значения таймеров старения записей адресных таблиц (Aging Timer) равными длительности таймера задержки передачи Forward Delay.

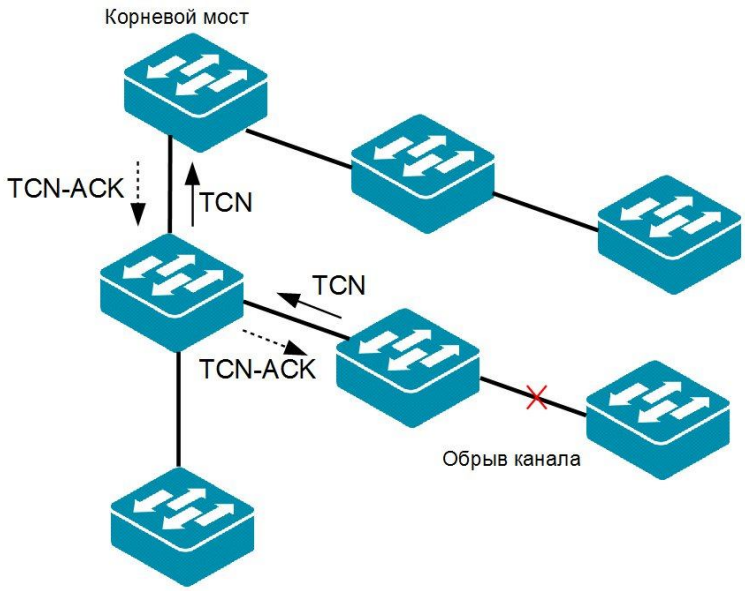


Рис. 6.18 Процесс уведомления об изменении топологии

Управляемые коммутаторы D-Link при настройке функции STP позволяют включать и отключать на каждом порте возможность приема TCN BPDU с помощью параметра *restricted_tcn*. По умолчанию параметр restricted_tcn отключен. Использование данного параметра позволяет избежать сетевых атак, связанных с отправкой ложных кадров TCN BPDU.

6.9.6 Настройка STP

Рассмотрим пример настройки протокола STP на коммутаторах D-Link серии DGS-1210-28/ME в сети, показанной на Рис. 6.19.

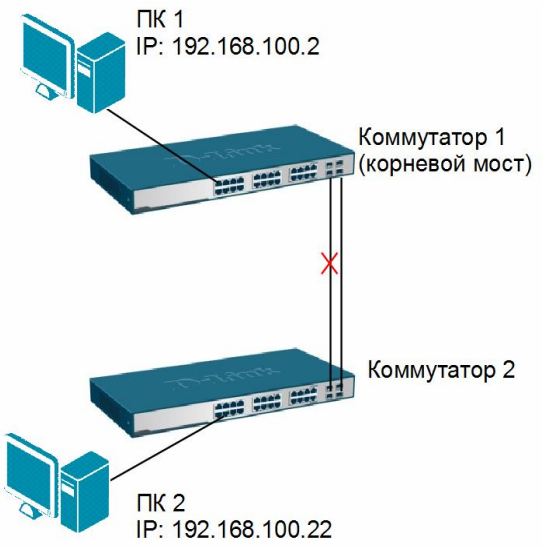


Рис. 6.19 Схема сети

Внимание: по умолчанию протокол STP на коммутаторах D-Link отключен.

Настройка коммутатора 1

Активизировать протокол STP глобально на коммутаторе и установить наименьшее значение приоритета, чтобы он был выбран корневым мостом (приоритет по умолчанию = 32768). Выбрать *Spanning Tree → STP Bridge Global Settings.* В открывшемся окне установить *STP State → Enabled*, в выпадающем меню *STP Version* выбрать *STP*, в открывающемся меню *Bridge Priority* выбрать *4096* и нажать кнопку *Apply* (Рис. 6.20).

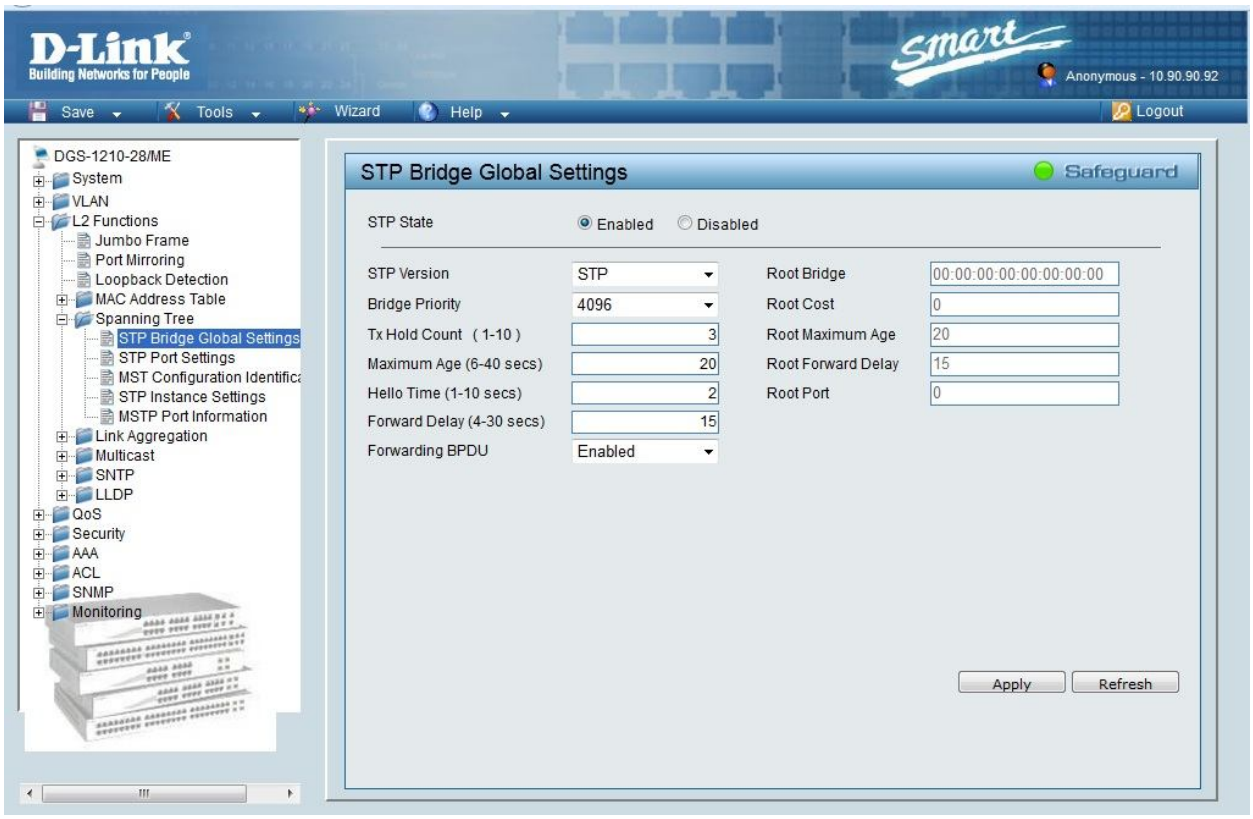


Рис. 6.20 Настройка протокола STP на коммутаторе 1

Настройка коммутатора 2

Активизировать протокол STP глобально на коммутаторе. Выбрать *Spanning Tree* → *STP Bridge Global Settings.* В открывшемся окне установить *STP State* → *Enabled*, в выпадающем меню *STP Version* выбрать *STP* и нажать кнопку *Apply* (Рис. 6.21).

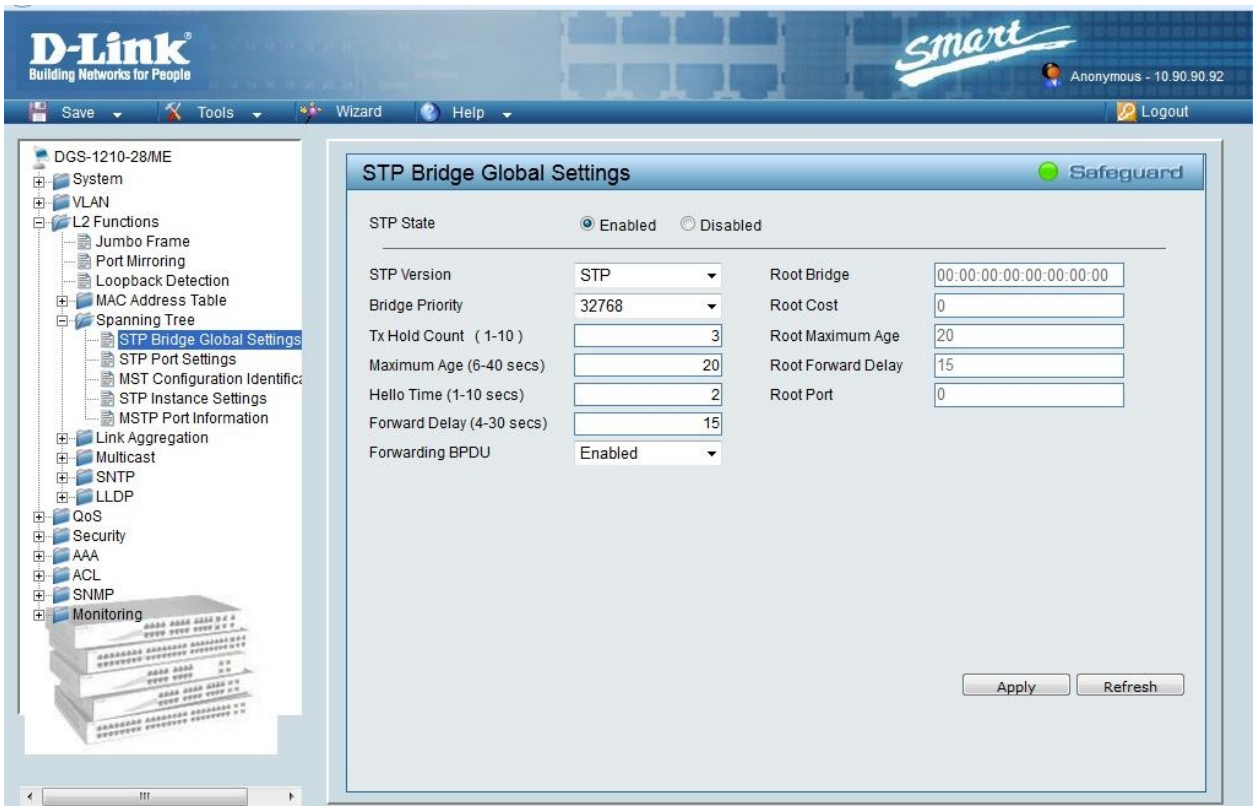


Рис. 6.21 Настройка протокола STP на коммутаторе 2

6.10 Виртуальные локальные сети (VLAN)

В соответствии с логикой работы алгоритма прозрачного моста коммутатор рассылает широковещательные кадры через все порты (за исключением порта-приемника такого кадра). Таким образом, все устройства сети, построенной на коммутаторах, находятся в одном *широковещательном домене*. Широковещательный домен – это область распространения широковещательных кадров. Широковещательные кадры используются при работе многих сетевых протоколов, таких как ARP или DHCP. Большой объем широковещательных кадров в сети, особенно крупной, приводит к нерациональному использованию полосы пропускания. Проблема ограничения распространения широковещательного трафика в сетях, построенных на коммутаторах, решается с помощью технологии *виртуальных локальных сетей* (Virtual LAN, VLAN).

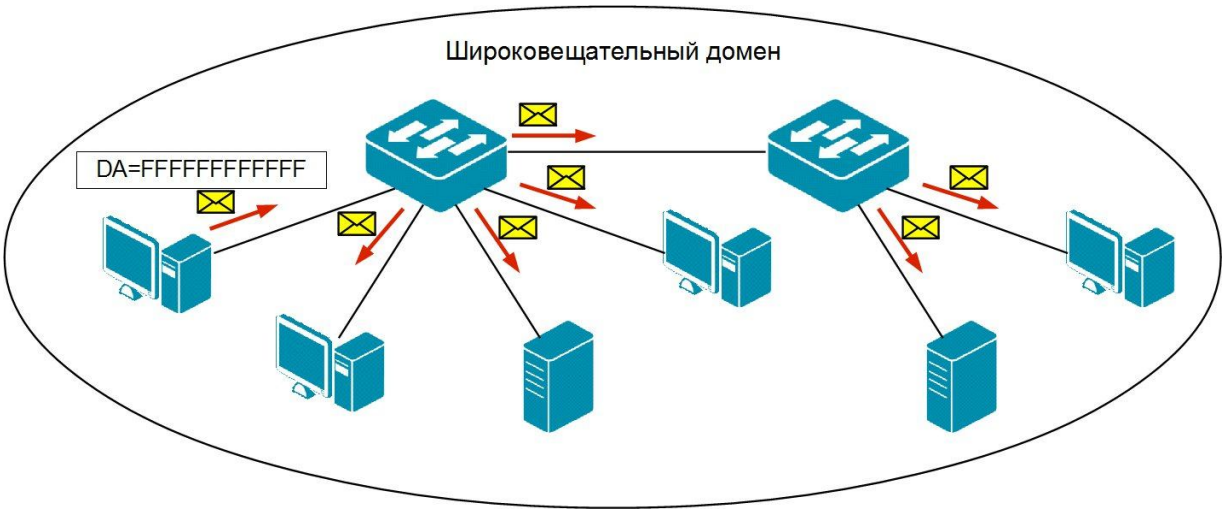


Рис. 6.22 Широковещательный домен

Виртуальной локальной сетью называется логическая группа узлов сети, трафик которой, в том числе и широковещательный, полностью изолирован от других узлов сети на канальном уровне. Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна независимо от типа адреса – индивидуального, группового или широковещательного. В то же время внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с MAC-адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных кадров и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

VLAN обладают следующими преимуществами:

- гибкость внедрения – VLAN являются эффективным способом группировки сетевых пользователей в виртуальные рабочие группы независимо от их физического размещения в сети;
- ограничивают распространение широковещательного трафика, что увеличивает полосу пропускания, доступную для пользователя;
- позволяют повысить безопасность сети, определив с помощью фильтров, настроенных на коммутаторе или маршрутизаторе, политику взаимодействия пользователей из разных виртуальных сетей.

Рассмотрим пример, показывающий эффективность использования логической сегментации сетей с помощью технологии VLAN при решении типовой задачи организации доступа в Интернет сотрудникам офиса, при условии изоляции трафика разных отделов.

Предположим, что в офисе находится несколько кабинетов, в каждом из которых располагается некоторое количество сотрудников. Каждый кабинет представляет собой отдельную рабочую группу.

При стандартном подходе к решению задачи с помощью физической сегментации трафика каждого отдела потребовалось бы в каждый кабинет устанавливать отдельный коммутатор, подключаемый к маршрутизатору, предоставляющему подключение в Интернет. При этом маршрутизатор должен обладать достаточным количеством портов, обеспечивающим возможность подключения всех физических сегментов (кабинетов) сети. Данное решение является плохо масштабируемым и дорогостоящим, так как при увеличении количества отделов, увеличивается количество необходимых коммутаторов, интерфейсов маршрутизатора и магистральных кабелей.

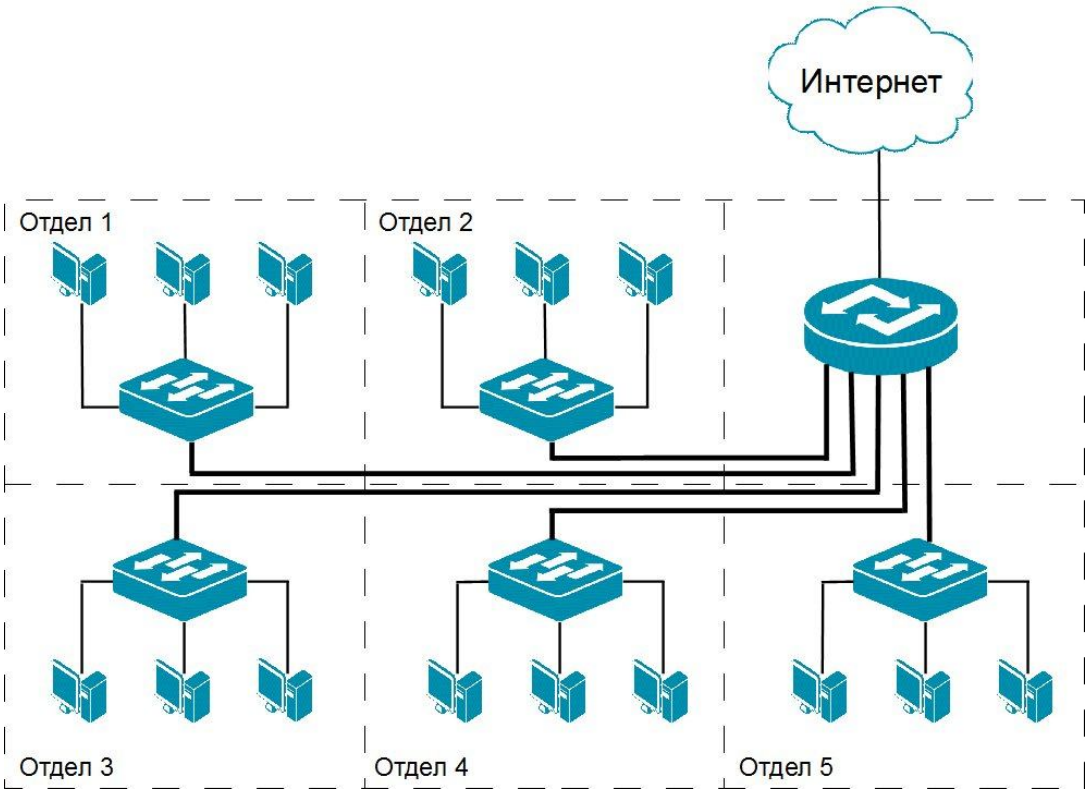


Рис. 6.23 Физическая сегментация сети

При использовании виртуальных локальных сетей не требуется подключать пользователей одного отдела к отдельному коммутатору, что позволяет сократить количество используемых устройств и магистральных кабелей. Коммутатор, программное обеспечение которого поддерживает функцию виртуальных локальных сетей, позволяет выполнять логическую сегментацию сети путем соответствующей программной настройки. Благодаря этому можно подключать компьютеры, находящиеся в разных сегментах сети, к одному коммутатору, а также сократить количество необходимых физических интерфейсов на маршрутизаторе.

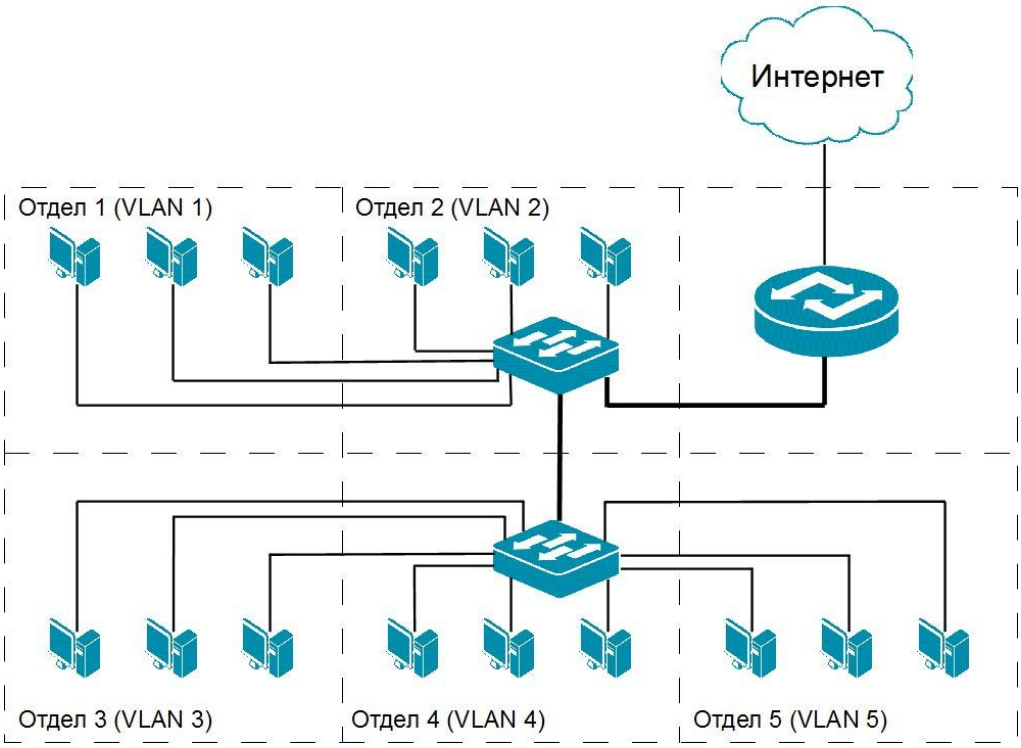


Рис. 6.24 Логическая группировка сетевых пользователей в VLAN

6.10.1 Типы VLAN

В коммутаторах могут быть реализованы следующие типы VLAN:

- на основе портов;
- на основе стандарта IEEE 802.1Q;
- на основе стандарта IEEE 802.1ad (Q-in-Q VLAN);
- на основе портов и протоколов IEEE 802.1v;
- на основе MAC-адресов;
- асимметричные.

Также для сегментации сети на канальном уровне модели OSI в коммутаторах могут использоваться другие функции, например *Traffic Segmentation*. В данном курсе будут рассмотрены VLAN на основе портов и VLAN на основе стандарта IEEE 802.1Q. Изучить принципы работы VLAN на основе стандарта IEEE 802.1ad, портов и протоколов IEEE 802.1v можно в курсе «Технологии коммутации и маршрутизации современных сетей Ethernet. Базовый курс D-Link» на портале дистанционного обучения и сертификации D-Link http://learn.dlink.ru.

6.10.2 VLAN на основе портов

При использовании VLAN на основе портов (Port-based VLAN), каждый порт назначается в определенную VLAN, независимо от того, какой компьютер подключен к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов – статическая и может быть изменена только вручную.

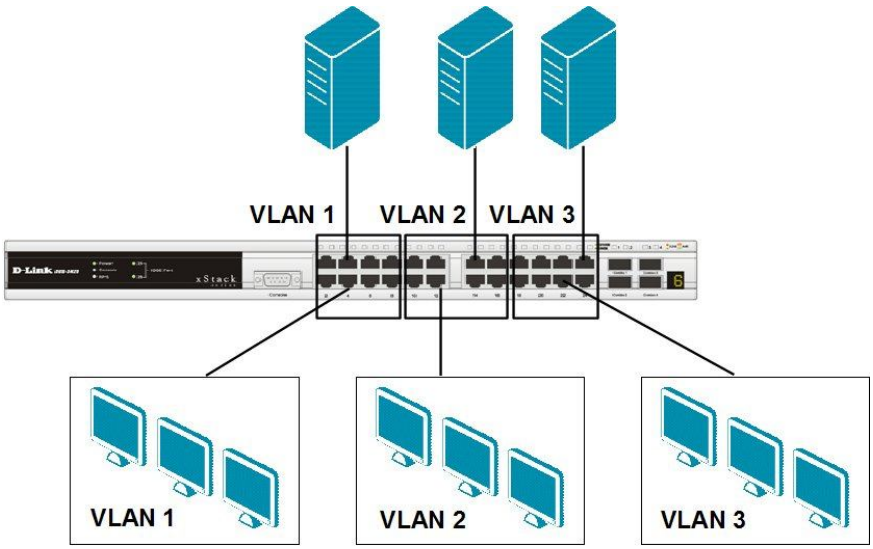


Рис. 6.25 VLAN на основе портов

Перечислим основные характеристики VLAN на основе портов.

1. Применяются в пределах одного коммутатора. Если необходимо организовать несколько рабочих групп небольшой сети на основе одного коммутатора, например, разделить технический отдел и отдел продаж, то VLAN на базе портов оптимально подходит для данной задачи.

2. Простота настройки. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы – достаточно всем портам, помещаемым в одну VLAN, присвоить одинаковый идентификатор VLAN (VLAN ID) .

3. Возможность изменения логической сегментации сети без физического перемещения станций. Достаточно изменить настройки порта, с одной VLAN (например, VLAN технического отдела) на другую (VLAN отдела продаж) и рабочая станция сразу же получает возможность совместно использовать ресурсы с членами новой VLAN. Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети.

4. Каждый порт может входить только в одну VLAN. Для объединения виртуальных подсетей как внутри одного коммутатора, так и между двумя коммутаторами, нужно использовать сетевой уровень модели OSI. Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки кадров из одной подсети (VLAN) в другую (IP-адреса подсетей должны быть разными).

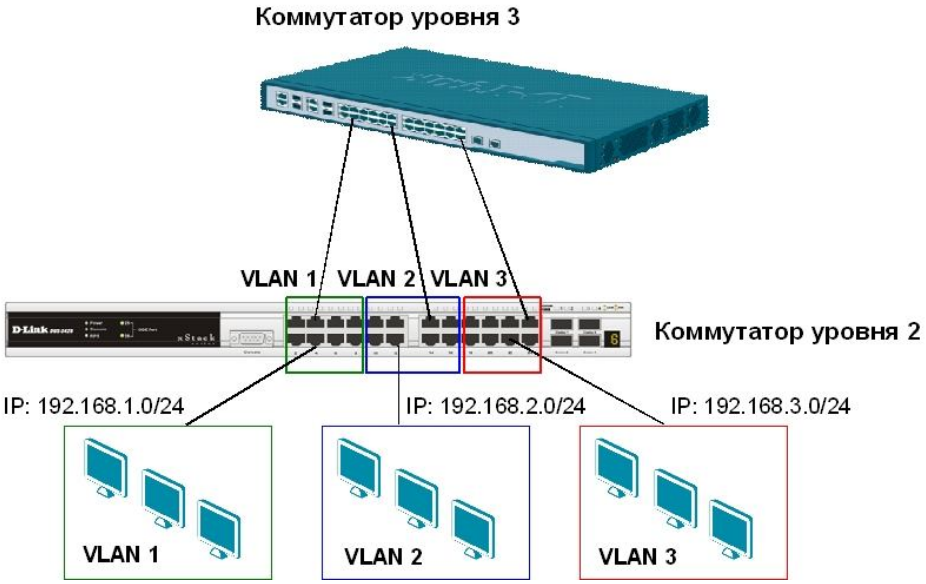


Рис. 6.26 Объединение VLAN с помощью маршрутизирующего устройства

Недостатком такого решения является то, что один порт каждой VLAN необходимо подключать к маршрутизатору, что приводит к дополнительным расходам на покупку кабелей и маршрутизатор, а также снижает количество свободных портов. Решить данную проблему можно двумя способами: использовать коммутаторы, которые позволяют включать порт в несколько VLAN, или использовать коммутаторы 3-го уровня.

6.11 VLAN на основе стандарта IEEE 802.1Q

Построение VLAN на основе портов осуществляется только на добавлении дополнительной информации к адресным таблицам коммутатора и не использует возможности встраивания информации о принадлежности к виртуальной сети в передаваемый кадр. Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра Ethernet для хранения информации о принадлежности к VLAN при его перемещении по сети. С точки зрения удобства и гибкости настроек, VLAN стандарта IEEE 802.1Q является лучшим решением, по сравнению с VLAN на основе портов. Его основные преимущества приведены ниже.

1. Гибкость и удобство в настройке и изменении – можно создавать необходимые комбинации VLAN как в пределах одного коммутатора, так и во всей сети, построенной на коммутаторах с поддержкой стандарта IEEE 802.1Q. Возможность добавления тегов позволяет информации о VLAN распространяться через множество 802.1Q-совместимых коммутаторов по одному физическому соединению (*магистральному каналу, Trunk Link*).
2. Позволяет активизировать алгоритм связующего дерева (Spanning Tree) на всех портах и работать в обычном режиме.
3. Способность VLAN IEEE 802.1Q добавлять и извлекать теги из заголовков кадров Ethernet позволяет использовать в сети коммутаторы и сетевые устройства, которые не поддерживают стандарт IEEE 802.1Q.
4. Устройства разных производителей, поддерживающие стандарт IEEE 802.1Q, могут работать совместно, не используя какие-либо фирменные решения.
5. Чтобы связать подсети на сетевом уровне, необходим маршрутизатор или коммутатор L3. Однако для более простых случаев, например для организации доступа к серверу из различных VLAN, маршрутизатор не требуется. Для этого необходимо включить порт

коммутатора, к которому подключен сервер, во все нужные подсети, а сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.

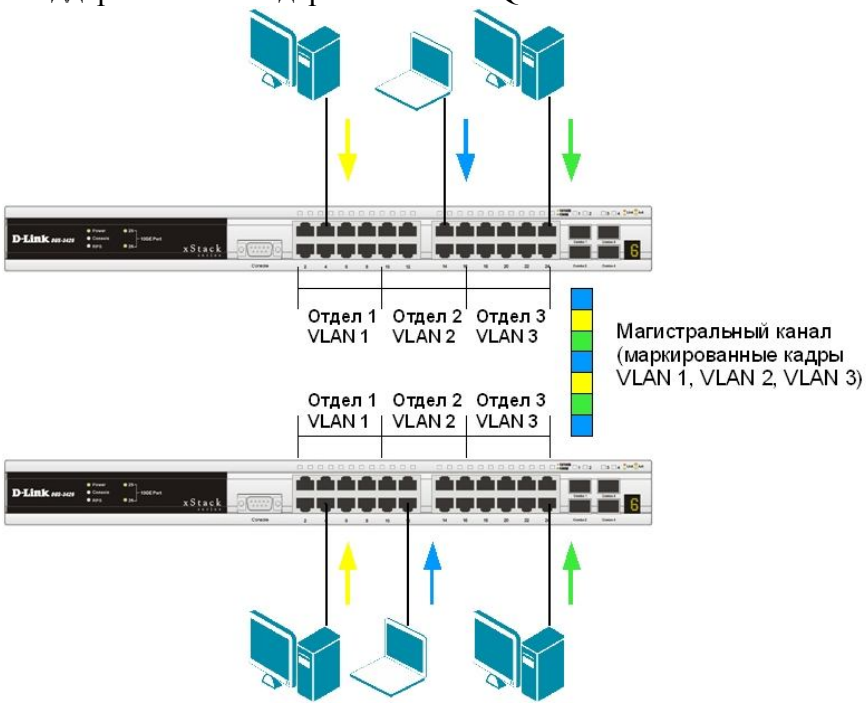


Рис. 6.27 Передача кадров нескольких VLAN по магистральному каналу связи

6.11.1 Некоторые определения IEEE 802.1Q

- **Tagging (Маркировка кадра)** – процесс добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра Ethernet.
- **Untagging (Извлечение тега из кадра)** – процесс извлечения информации о принадлежности к 802.1Q VLAN из заголовка кадра Ethernet.
- **VLAN ID (VID)** – идентификатор VLAN.
- **Port VLAN ID (PVID)** – идентификатор порта VLAN.
- **Ingress port (Входной порт)** – порт коммутатора, на который поступают кадры, и при этом принимается решение о принадлежности к VLAN.
- **Egress port (Выходной порт)** – порт коммутатора, с которого кадры передаются на другие сетевые устройства – коммутаторы или рабочие станции, и при этом приниматься решение о маркировке.

Любой порт коммутатора может быть настроен как *tagged* (маркированный) или как *untagged* (немаркированный). Функция *untagging* позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра Ethernet. Функция *tagging* позволяет настраивать VLAN между несколькими коммутаторами, поддерживающими стандарт IEEE 802.1Q.

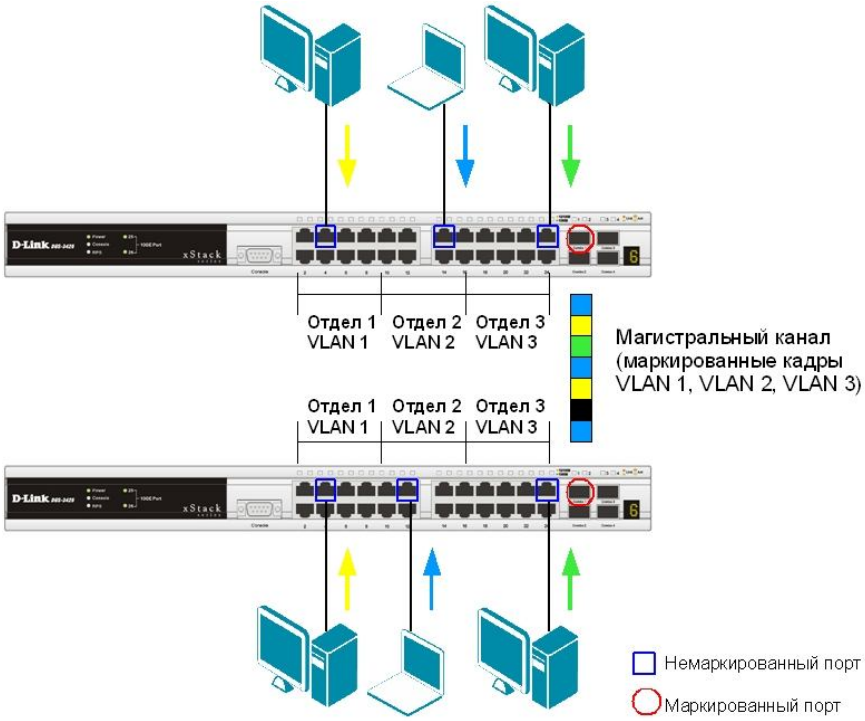


Рис. 6.28 Маркированные и немаркированные порты VLAN

6.11.2 Тег VLAN IEEE 802.1Q

Стандарт IEEE 802.1Q определяет изменения в структуре кадра Ethernet, позволяющие передавать информацию о VLAN по сети. На Рис. 6.29 изображен формат тега 802.1Q VLAN. К кадру Ethernet добавлены 32 бита (4 байта), которые увеличивают его размер до 1522 байт. Первые 2 байта (поле Tag Protocol Identifier, TPID) с фиксированным значение 0x8100 определяют, что кадр содержит тег протокола 802.1Q. Остальные 2 байта содержат следующую информацию:

- *Priority (Приоритет)* – 3 бита поля приоритета передачи кодируют до восьми уровней приоритета (от 0 до 7, где 7 – наивысший приоритет), которые используются в стандарте 802.1p;
- *Canonical Format Indicator (CFI)* – 1 бит индикатора канонического формата зарезервирован для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet;
- *VID (VLAN ID)* – 12-ти битный идентификатор VLAN определяет, какой VLAN принадлежит трафик. Поскольку под поле VID отведено 12 бит, то можно задать 4094 уникальных VLAN (VID 0 и VID 4095 зарезервированы).

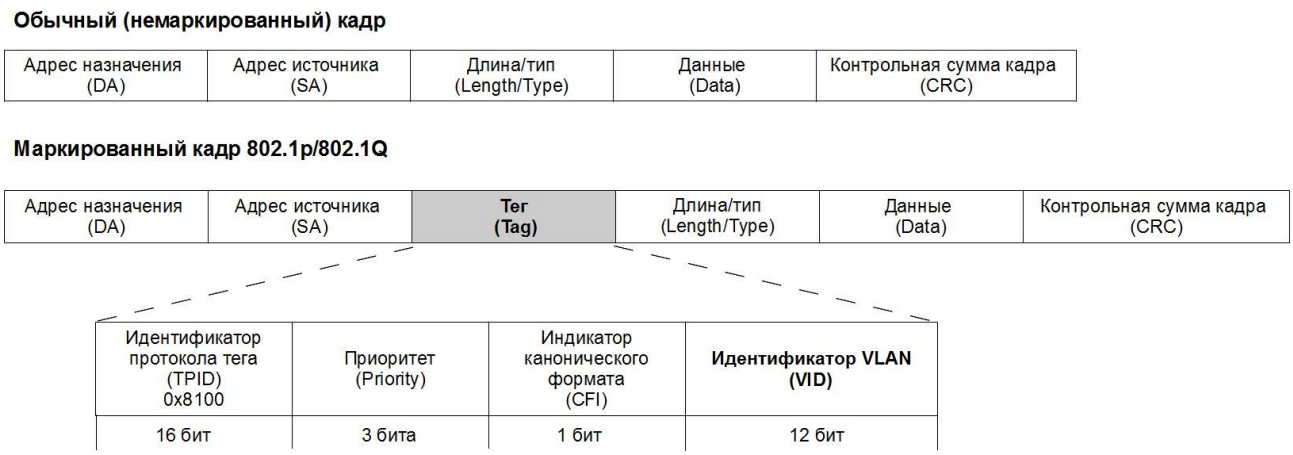


Рис. 6.29 Маркированный кадр Ethernet

6.11.3 Port VLAN ID

Каждый физический порт коммутатора имеет *идентификатор порта VLAN* (*PVID*). Этот параметр используется для того, чтобы определить, в какую VLAN коммутатор направит входящий немаркированный кадр с подключенного к порту сегмента, когда кадр нужно передать на другой порт (внутри коммутатора в заголовки всех *немаркированных кадров* добавляется идентификатор VID равный *PVID* порта, на который они были приняты). Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Коммутаторы, поддерживающие протокол IEEE 802.1Q, должны хранить таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт такого коммутатора может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель коммутатора.

Если на коммутаторе не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

6.11.4 Продвижение кадров VLAN IEEE 802.1Q

Решение о продвижении кадра внутри виртуальной локальной сети принимается на основе трех следующих правил:

- правила входящего трафика (*ingress rules*) – классификация получаемых кадров относительно принадлежности к VLAN;
- правила продвижения между портами (*forwarding rules*) – принятие решения о продвижении или отбрасывании кадра;
- правила исходящего трафика (*egress rules*) – принятие решения о сохранении или удалении в заголовке кадра тега 802.1Q перед его передачей.

Правила входящего трафика выполняют классификацию каждого получаемого кадра относительно принадлежности к определенной VLAN, а также могут служить для принятия решения о приеме кадра для дальнейшей обработки или его отбрасывании на основе классификации и формата принятого кадра.

Классификация кадра по принадлежности VLAN осуществляется следующим образом:

а) Если кадр не содержит информацию о VLAN (*немаркированный кадр*), то в его заголовок коммутатор добавляет тег с идентификатором VID, равным идентификатору PVID порта, через который этот кадр был принят.

б) Если кадр содержит информацию о VLAN (*маркированный кадр*), то его принадлежность к конкретной VLAN определяется по идентификатору VID в заголовке кадра. Значение тега в нем не изменяется.

Активизировав функцию проверки формата кадра на входе, администратор сети может указать, кадры каких форматов будут приниматься коммутатором для дальнейшей обработки. Управляемые коммутаторы D-Link позволяют настраивать прием либо только маркированных кадров (*tagged_only*), либо обоих типов кадров – маркированных и немаркированных (*admit_all*).

Внимание: внутри коммутатора все кадры являются маркированными.

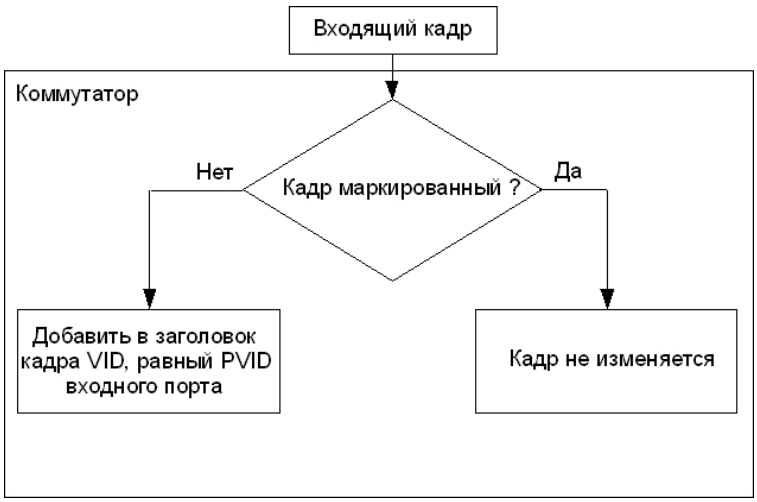


Рис. 6.30 Правила входящего трафика

Правила продвижения между портами осуществляют принятие решения об отбрасывании или передаче кадра на порт назначения на основе его информации о принадлежности конкретной VLAN и MAC-адреса узла-приемника.

Если входящий кадр маркированный, то коммутатор определяет, является ли входной порт членом той же VLAN путем сравнения идентификатора VID в заголовке кадра и набора идентификаторов VID, ассоциированных с портом, включая его PVID. Если нет, то кадр отбрасывается. Этот процесс называется *ingress filtering* (входной фильтрацией) и используется для сохранения пропускной способности внутри коммутатора путем отбрасывания кадров, не принадлежащих той же VLAN, что и входной порт, на стадии их приема.

Если кадр немаркированный, входная фильтрация не выполняется.

Далее определяется, является ли порт назначения членом той же VLAN. Если нет, то кадр отбрасывается. Если же выходной порт входит в данную VLAN, то коммутатор передает кадр в подключенный к нему сегмент сети.

Правила исходящего трафика определяют формат исходящего кадра – маркированный или немаркированный. Если выходной порт является немаркированным (*untagged*), то он будет извлекать тег 802.1Q из заголовков всех выходящих через него маркированных кадров. Если выходной порт настроен как маркированный (*tagged*), то он будет сохранять тег 802.1Q в заголовках всех выходящих через него маркированных кадров.

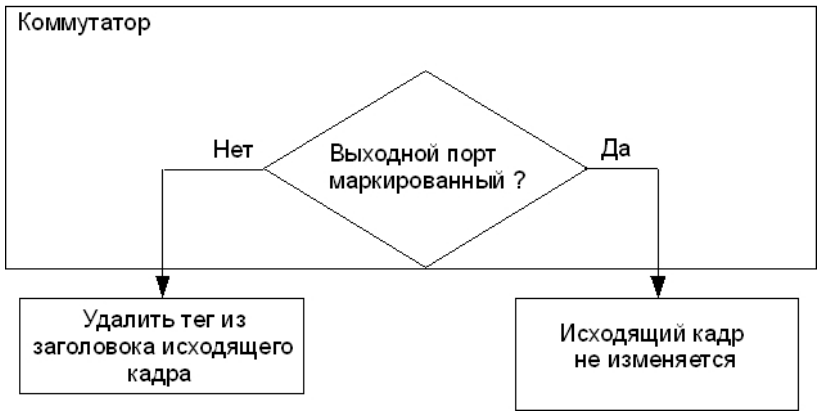


Рис. 6.31 Правила исходящего трафика

На рисунках 6.32–6.35 приведен пример передачи немаркированного и маркированного кадра через маркированный и немаркированный порты коммутатора.

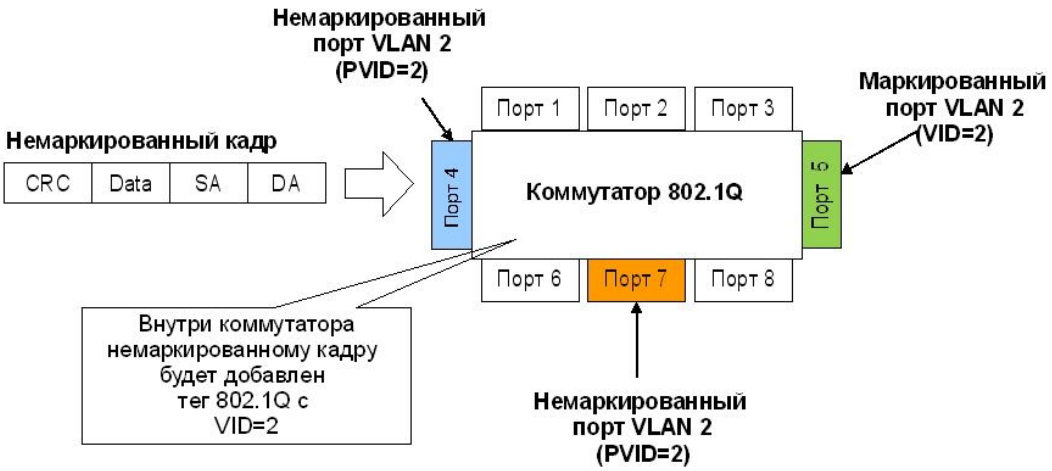


Рис. 6.32 Входящий немаркированный кадр

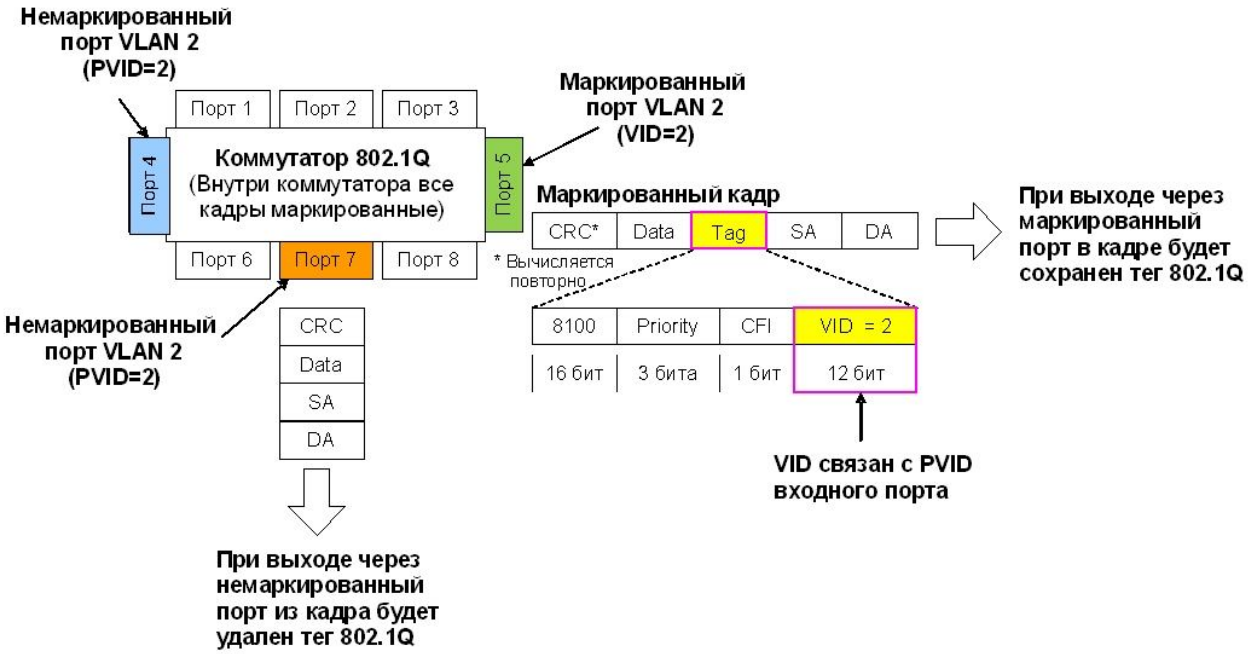


Рис. 6.33 Немаркированный кадр, передаваемый через маркированный и немаркированный порты

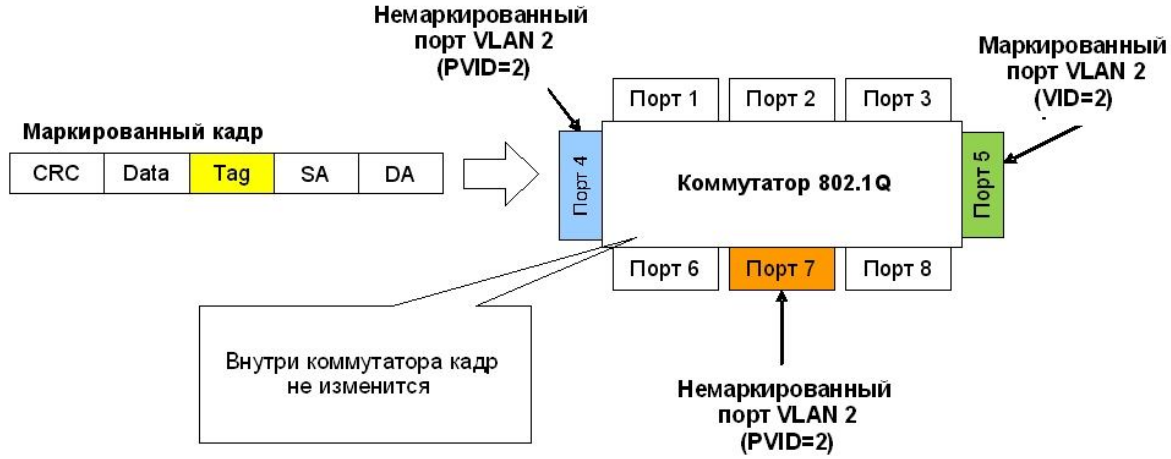


Рис. 6.34 Входящий маркированный кадр

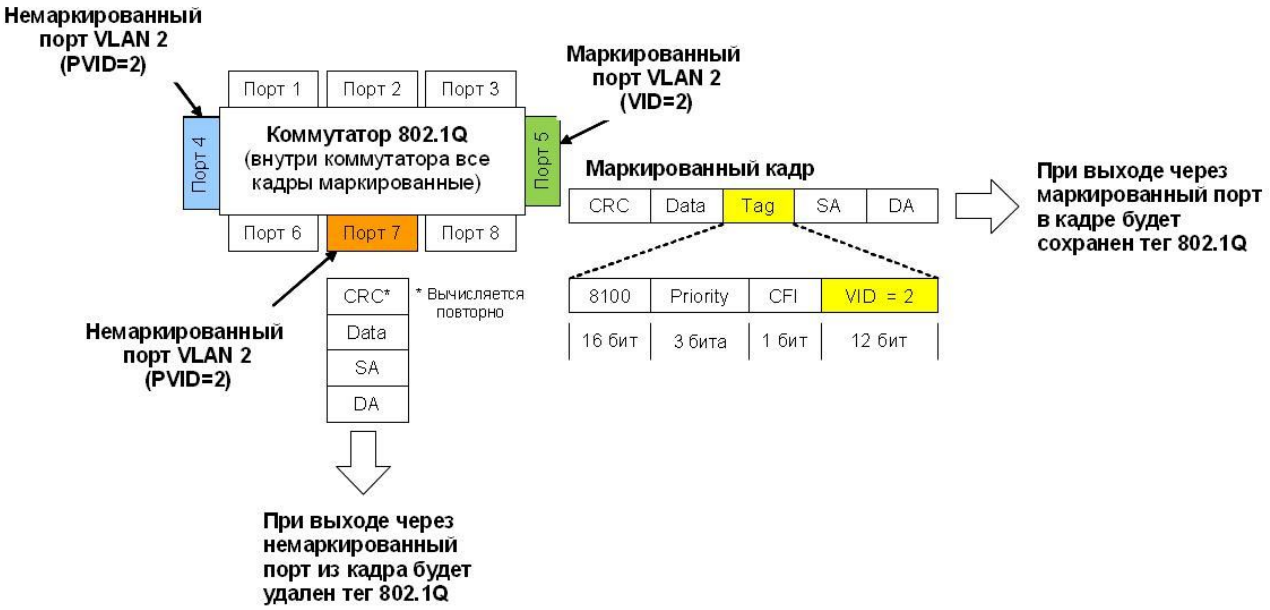


Рис. 6.35 Маркированный кадр, передаваемый через маркированный и немаркированный порты

6.11.5 Пример настройки VLAN IEEE 802.1Q

Предположим, что в небольшом офисе, в котором имеется два отдела, необходимо изолировать трафик сотрудников разных отделов друг от друга, но в то же время обеспечить совместный доступ всех пользователей к серверу. Для этих целей можно использовать коммутатор с поддержкой стандарта IEEE 802.1Q и создать на нем две группы VLAN (VLAN v2 – для первого отдела, VLAN v3 – для второго отдела). Схема сети показана на Рис. 6.36.

В качестве примера передачи данных между VLAN рассмотрим пересылку кадра с порта 1 коммутатора на порт 24, к которому подключен сервер.

Порт 1 является немаркированным портом VLAN v2 (PVID=2). Поэтому, когда любой немаркированный кадр поступает на порт 1, коммутатор снабжает его тегом 802.1Q со значением VID равным 2.

Далее коммутатор проверяет в своей таблице коммутации, через какой порт необходимо передать кадр и принадлежит ли этот порт VLAN v2. Кадр может быть передан через порт 24, так как он является маркированным членом VLAN v2. После передачи кадра через порт 24 тег 802.1Q в нем будет сохранен, поэтому сетевой адаптер сервера должен поддерживать стандарт IEEE 802.1Q.

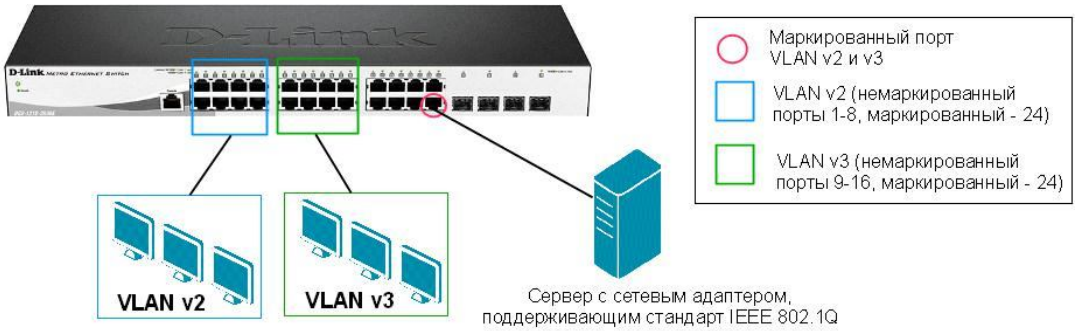


Рис. 6.36 Схема сети с двумя VLAN

Ниже приведен пример настройки коммутатора DGS-1210-28/ME, позволяющий реализовать заданную схему сети с двумя VLAN.

1. Удалить соответствующие порты из VLAN по умолчанию (default VLAN). Выбрать раздел *VLAN → 802.1Q VLAN* и нажать ссылку *VID 1* (Рис. 6.37).

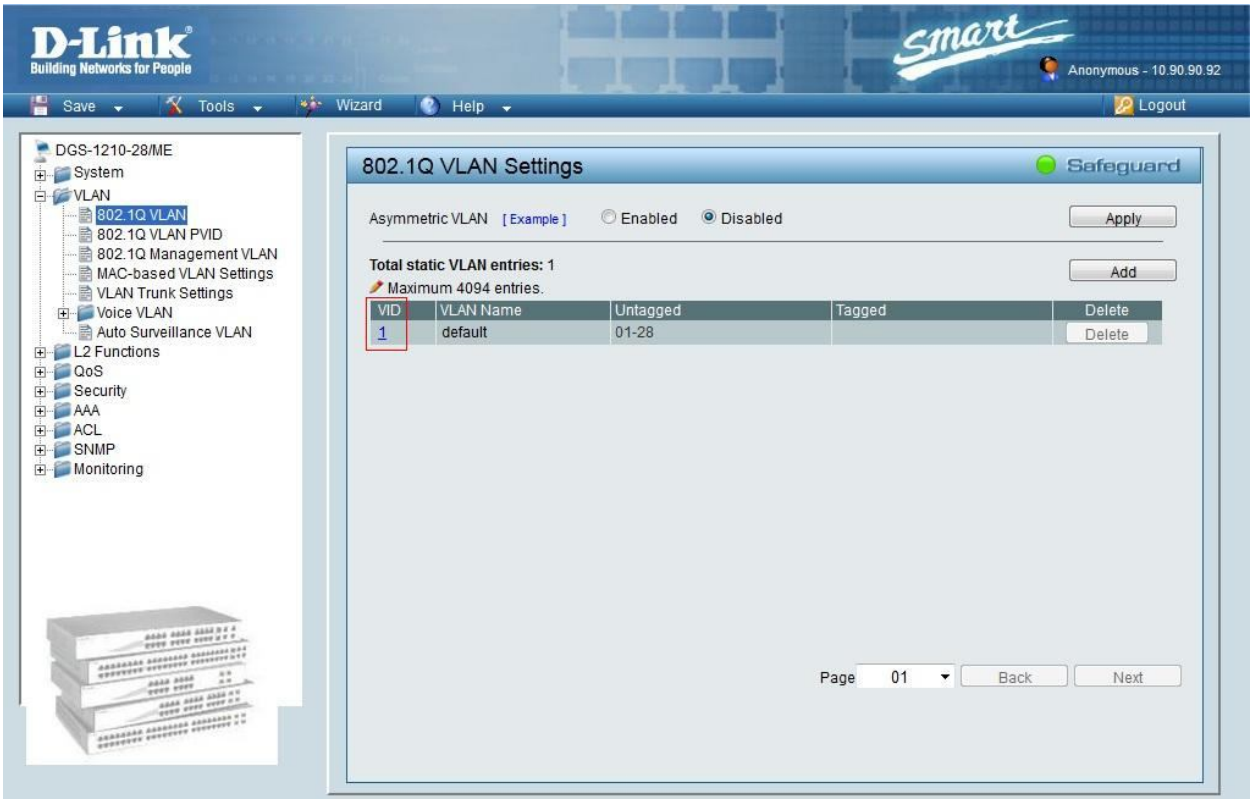


Рис. 6.37 Редактирование VLAN по умолчанию

В открывшемся окне напротив *Not Member* установить галочки для портов 1-16 и нажать кнопку *Apply* (Рис. 6.38).

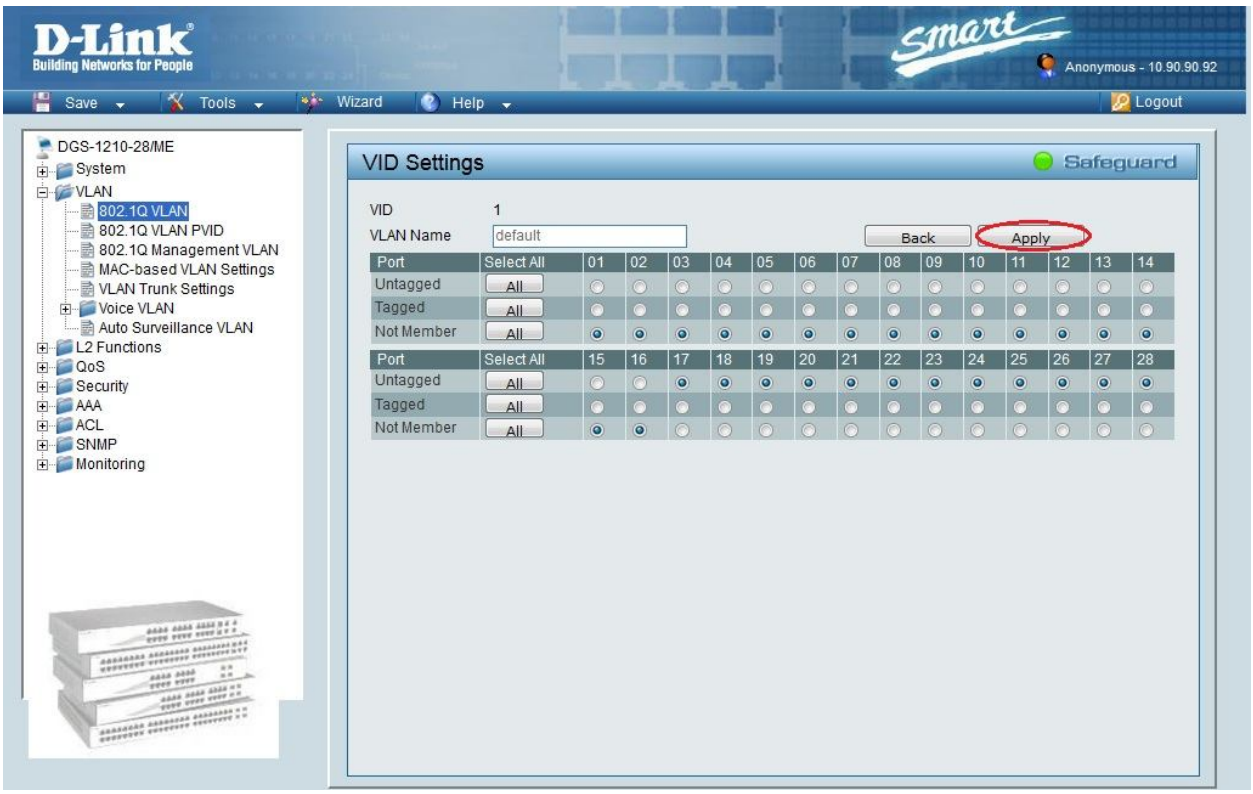


Рис. 6.38 Удаление портов из VLAN по умолчанию

Внимание: заводские установки по умолчанию назначают все порты коммутатора в default VLAN с VID = 1. **Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN.** Немаркированные порты не могут одновременно быть членами нескольких VLAN.

2. Создать VLAN с именем v2 и настроить порты 1-8 как немаркированные, порт 24 – маркированным. Для этого нажать на кнопку *Add* (Рис. 6.39).

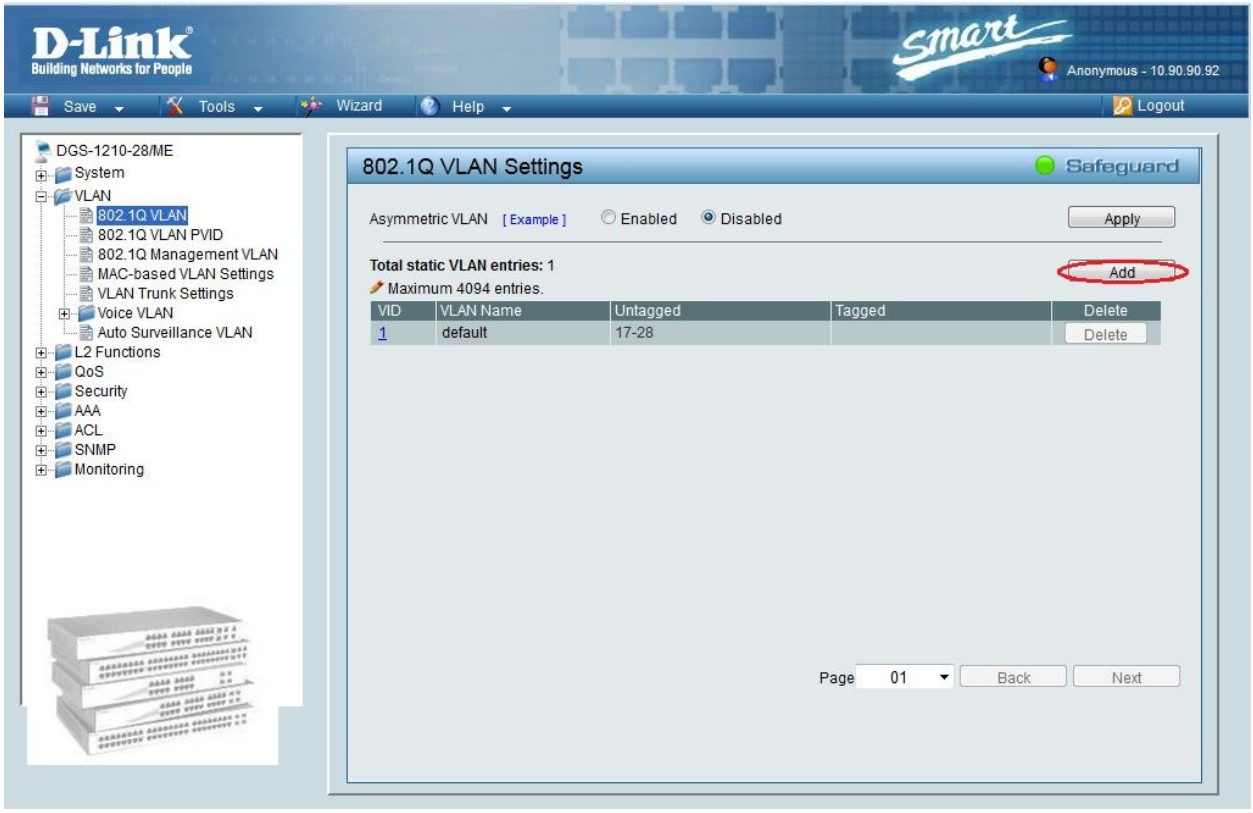


Рис. 6.39 Создание VLAN

В поле *VID* ввести *2*, в поле *VLAN Name* ввести *v2* и установить галочки напротив *Untagged* для портов *1-8*, напротив *Tagged* – для порта *24* и нажать кнопку *Apply* (Рис. 6.40).

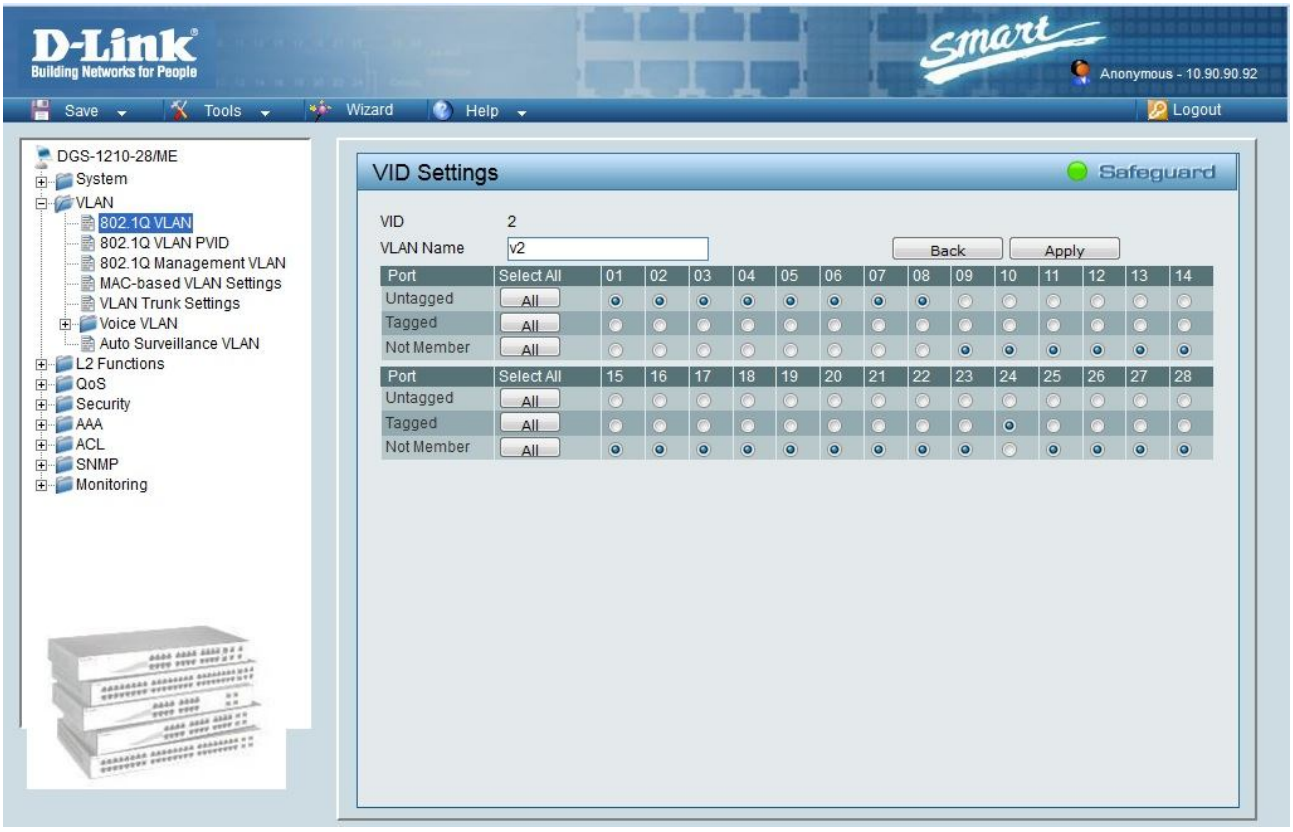


Рис. 6.40 Добавление портов в VLAN v2

3. Создать VLAN с именем v3 и настроить порты 9-16 как немаркированные, порт 24 – маркированным. Для этого нажать на кнопку *Add*. В поле *VID* ввести *3*, в поле *VLAN Name* ввести *v3* и установить галочки напротив *Untagged* для портов *9-16*, напротив *Tagged* – для порта *24* и нажать кнопку *Apply* (Рис. 6.41).

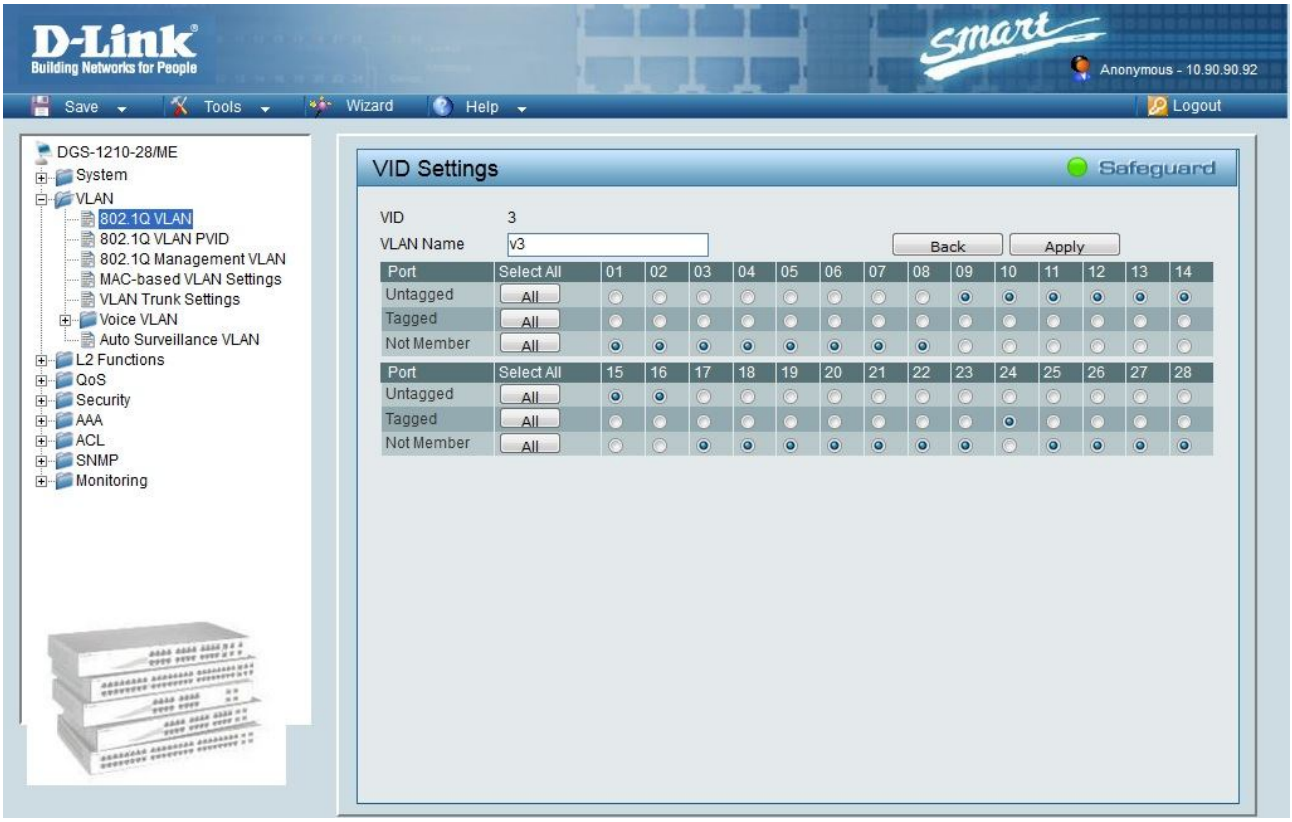


Рис. 6.41 Добавление портов в VLAN v3

4. Созданные VLAN на коммутаторе (Рис. 6.42).

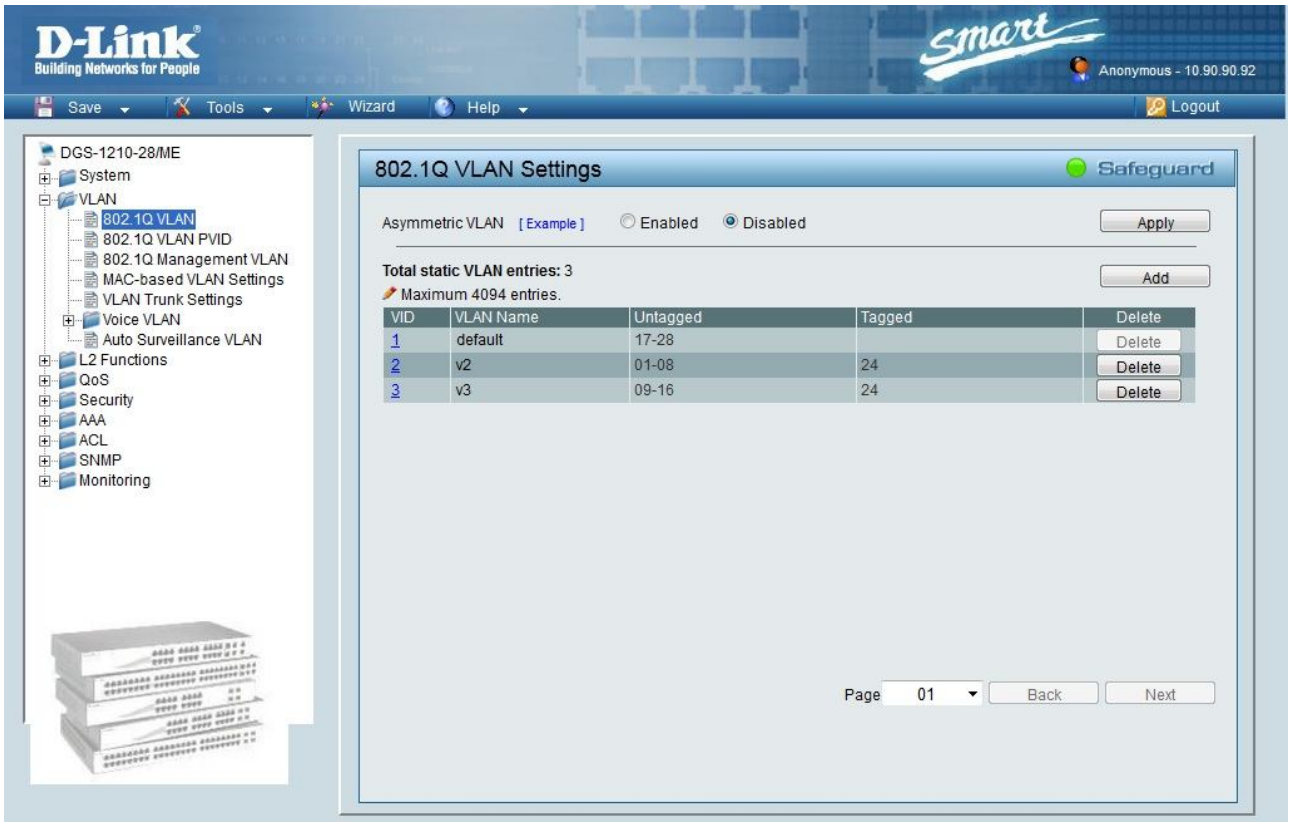


Рис. 6.42 Созданные VLAN

Внимание: при настройке VLAN на основе стандарта IEEE 802.1Q через Web-интерфейс необходимо, чтобы рабочая станция, с которой осуществляется управление коммутатором, была подключена к порту, входящему в VLAN по умолчанию (default VLAN с VID = 1).

6.12 Технология Power over Ethernet

Устанавливая точку доступа Wi-Fi, IP-камеру или IP-телефон, часто приходиться учитывать, где находится ближайшая электрическая розетка, чтобы подключить к ней блок питания устройства. Иногда наилучшее положение устройства может вступать в противоречие с его физическим расположением. Например, для достижения лучшего уровня беспроводного сигнала требуется поместить точку доступа на потолке или крыше, а камеру на заборе или высокой стене. Установка оборудования в труднодоступных местах, где поблизости нет источника питания, а электропроводка отсутствует, представляет собой серьезную проблему. Прокладка силовых кабелей в подобных случаях может оказаться дорогостоящей и непростой задачей.

Установка оборудования сопряжена не только с подводкой кабеля питания к месту его монтажа, но и с подключением сетевых кабелей, по которым передаются данные.

Для решения проблемы электропитания устройств, находящихся в труднодоступных местах была разработана технология **Power over Ethernet (PoE)**. Эта технология позволяет передавать удаленному (оконечному) устройству вместе с данными электрическую энергию через кабель на основе стандартной витой пары в сети Ethernet. Благодаря технологии PoE точку доступа, например, можно устанавливать в месте наилучшего приема сигнала, IP-камеру поместить в любом удобном для обзора месте, а для подключения IP-телефона не монтировать дополнительную розетку.

В качестве основных преимуществ технологии PoE можно выделить следующие:

- электропитание удаленного сетевого устройства и обмен данными с ним осуществляется по одному сетевому кабелю;

- низкие затраты на инсталляцию систем, их модернизацию и сервисное обслуживание;
- повышенная эксплуатационная безопасность: обеспечивается защита от короткого замыкания, падения напряжения, превышения потребляемого тока и т.п.;
- простота развертывания сети, особенно в сложных пространственных условиях (крыши, заборы, внутренние помещения в аэропортах и вокзалах, кафе, кинотеатры и т.п.) и простота перемещения PoE-совместимых оконечных устройств;
- возможность управления параметрами питания удаленных устройств, т.к. оборудование с поддержкой PoE часто является управляемым, что упрощает администрирование сети.

Технология PoE является расширение стандарта IEEE 802.3. Первая версия технологии была описана в стандарте IEEE 802.3af-2003, которая в 2005 году вошла в 33 раздел стандарта IEEE 802.3-2005. В 2009 году появилась новая расширенная версия технологии PoE, описанная в стандарте IEEE 802.3at-2009, также известном как PoE+ или PoE plus. В настоящее время требования к PoE-системам определяются разделом 33 стандарта IEEE 802.3-2012 (в него полностью включен стандарт IEEE 802.3at-2009). Технология PoE предназначена для использования в устройствах с интерфейсами 10BASE-T, 100BASE-TX и 1000BASE-T.

Спецификация PoE описывает работу двух типов устройств: питающих устройств (**Power Sourcing Equipment, PSE**) и питаемых устройств (**Powered Device, PD**).

Питающие устройства (PSE) выполняют функции источников питания и предназначены для подачи электропитания в сеть Ethernet, к которой подключены питаемые устройства (PD). *Питаемые устройства* (PD) получает электропитание через кабель от питающих устройств.

Питающее устройство (PSE) может входить в состав активного оборудования или быть выполнено в виде отдельного устройства, которое включается в сетевой сегмент (в разрыв Ethernet-канала). В первом случае питающее устройство в терминологии PoE обозначается как «Endpoint» и обычно представляет собой коммутатор с поддержкой PoE (коммутаторы D-Link с поддержкой PoE содержат букву «P» в конце названия модели, например, DES-3200-28P). Во втором случае питающее устройство в терминологии PoE обозначается как «Midspan» и представляет собой инжектор PoE.

Инжекторы являются пассивными устройствами. Они не влияют на передачу данных и используются только для передачи электропитания через кабель. На вход инжектор получает данные и электропитание через соответствующие разъемы, а на выходе объединяет их и передает через стандартный разъем RJ-45 к которому подключен кабель. Инжекторы удобно использовать в том случае, когда в существующую сеть Ethernet требуется добавить функционал PoE, например, чтобы подключить камеру или точку доступа. В том случае, если требуется подключить большое количество устройств с поддержкой PoE, например, несколько камер видеонаблюдения, то наилучшим решением будет установка коммутатора PoE. При этом для питания коммутатора PoE рекомендуется использовать источник бесперебойного питания (UPS).

Коммутаторы PoE бывают как управляемые так и не управляемые. Управляемые коммутаторы предпочтительнее, так как позволяют устанавливать максимальные и минимальные значения потребляемого тока, приоритеты по портам, получать информацию об ошибках, а также автоматически проверять подключенные устройства с помощью прерываний и перегружать их путем кратковременного отключения питания в случае необходимости.

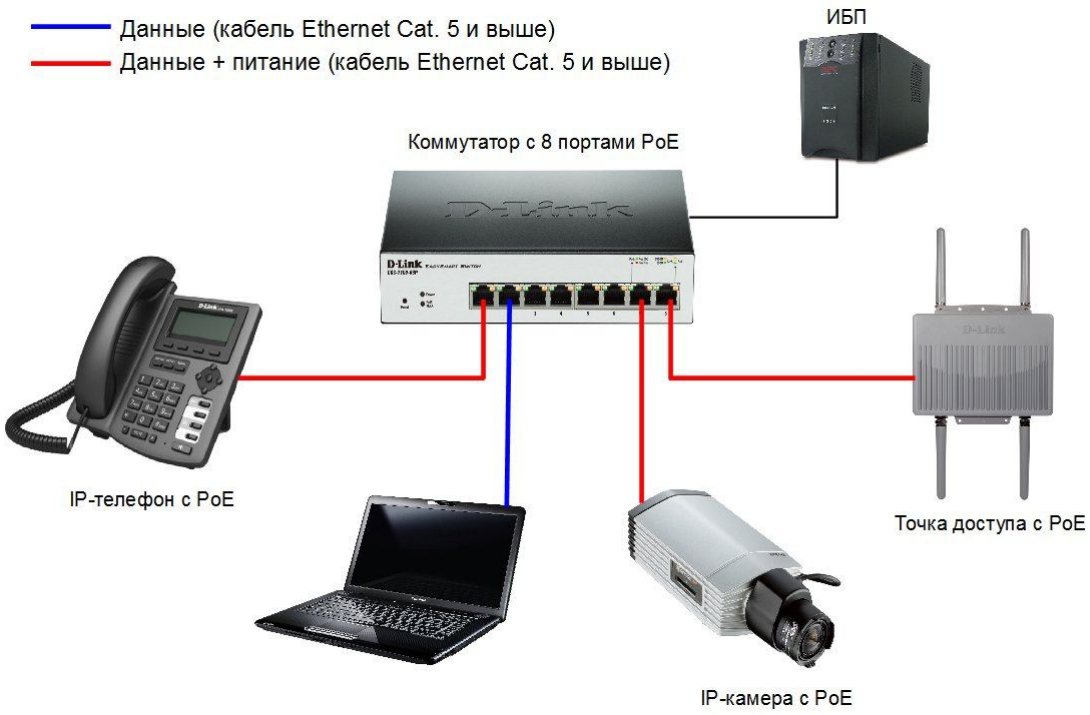


Рис. 6.43 Схема построение сети PoE с использованием коммутатора PoE

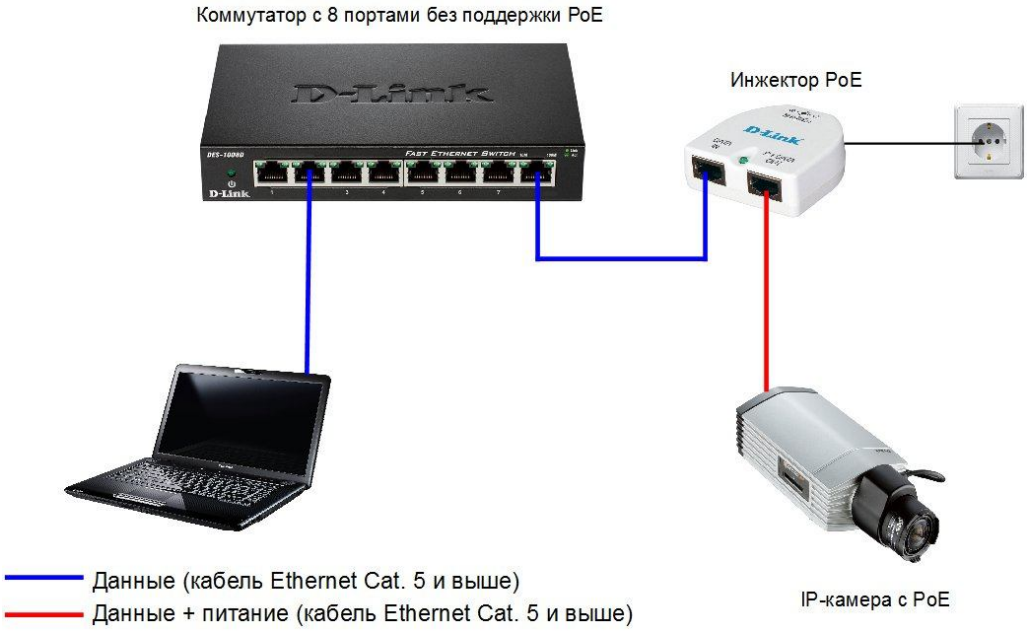


Рис. 6.44 Схема построение сети PoE с использованием инжектора PoE

Питающее устройство получает питание и данные через стандартный разъем 8P8C (RJ-45). При этом у устройства сохраняется возможность получать электроэнергию через традиционный источник питания, т.е. через розетку.

Спецификация PoE определяет два типа систем питания: **Тип 1** (Type 1) и **Тип 2** (Type 2). Система питания состоит из одного PSE и одного PD, связанных каналом связи. Каждый из типов систем питания имеет определенные характеристики.

Устройства PSE и PD Типа 1 предназначены для работы только в сетях 10BASE-T и 100BASE-TX (этот тип устройств описан в стандарте IEEE 802.3af). В системе Типа 1 для передачи питания используются две пары кабеля на основе витой пары категории 3 и выше. Для систем питания Типа 1 определен номинальный постоянный ток 350 мА для каждой витой пары, сопротивление кабеля постоянного току 20 Ом. Выходное напряжение питания

PSE Типа 1 лежит в диапазоне от 44 до 57 В постоянного тока, минимальный уровень выходной мощности равен 15,4 Вт. Входное напряжение PD Типа 1 лежит в диапазоне от 37 до 57 В постоянного тока, максимальная входная мощность в среднем равна 13 Вт с учетом потерь в кабеле.

Устройства PSE и PD Типа 2 предназначены для работы в сетях 10BASE-T, 100BASE-TX и 1000BASE-T (этот тип устройств описан в стандарте IEEE 802.3at). В системе Типа 2 для передачи питания используются две пары кабеля на основе витой пары категории 5/5e и выше. Для систем питания Типа 2 определен номинальный постоянный ток 600 мА для каждой витой пары, сопротивление кабеля постоянного току 12,5 Ом. Выходное напряжение питания PSE Типа 2 лежит в диапазоне от 50 до 57 В постоянного тока, минимальный уровень выходной мощности равен 30 Вт. Входное напряжение PD Типа 2 лежит в диапазоне от 42,5 до 57 В постоянного тока, максимальная входная мощность в среднем равна 25,5 Вт с учетом потерь в кабеле.

Существует четыре базовых схемы подачи питания, каждая из которых имеет два альтернативных (A и B) варианта передачи питания по витым парам:

- Endpoint PSE, поддерживающие работу в сетях 10BASE-T/100BASE-TX (Рис. 6.45): в варианте A питание передается по сигнальным парам 1, 2 и 3, 6; в варианте B питание передается по зарезервированным парам 4, 5 и 7, 8.

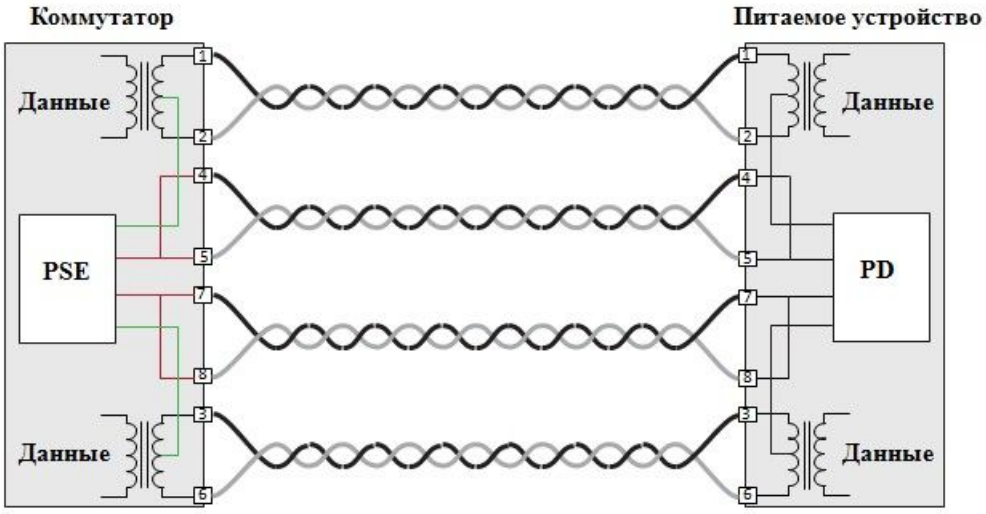


Рис. 6.45 Схема питания Endpoint PSE в сети 10/100BASE-TX (вариант A – зеленый; вариант B - красный)

- Endpoint PSE, поддерживающие 1000BASE-T (Рис. 6.46Рис. 6.45): в варианте A питание передается по сигнальным парам 1, 2 и 3, 6; в варианте B питание передается по сигнальным парам 4, 5 и 7, 8.

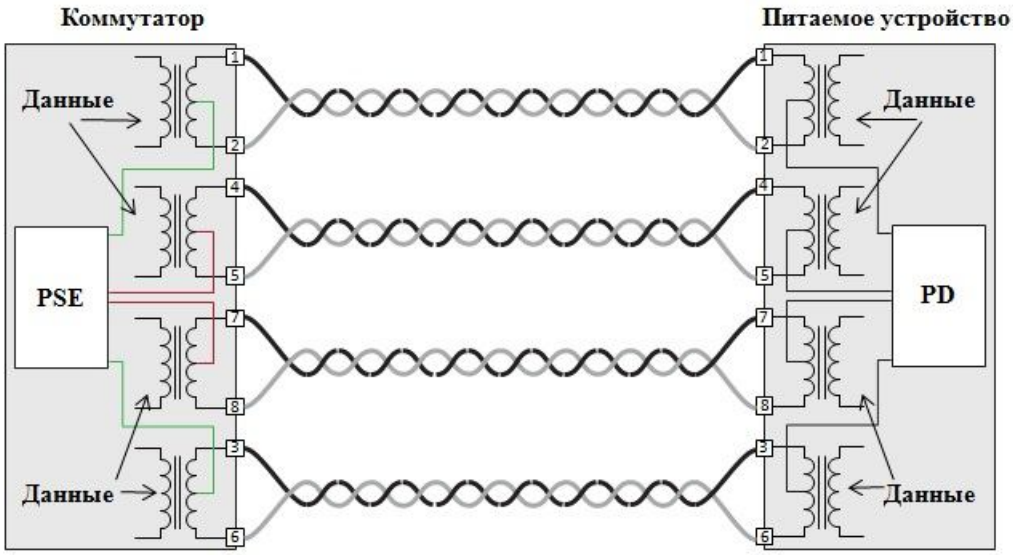


Рис. 6.46 Схема питания Endpoint PSE в сети 1000BASE-T (вариант A – зеленый; вариант B - красный)

- Midspan PSE, поддерживающие 10BASE-T/100BASE-TX (Рис. 6.47): в варианте A питание передается по сигнальным парам 1, 2 и 3, 6; в варианте B питание передается по зарезервированным парам 4, 5 и 7, 8.

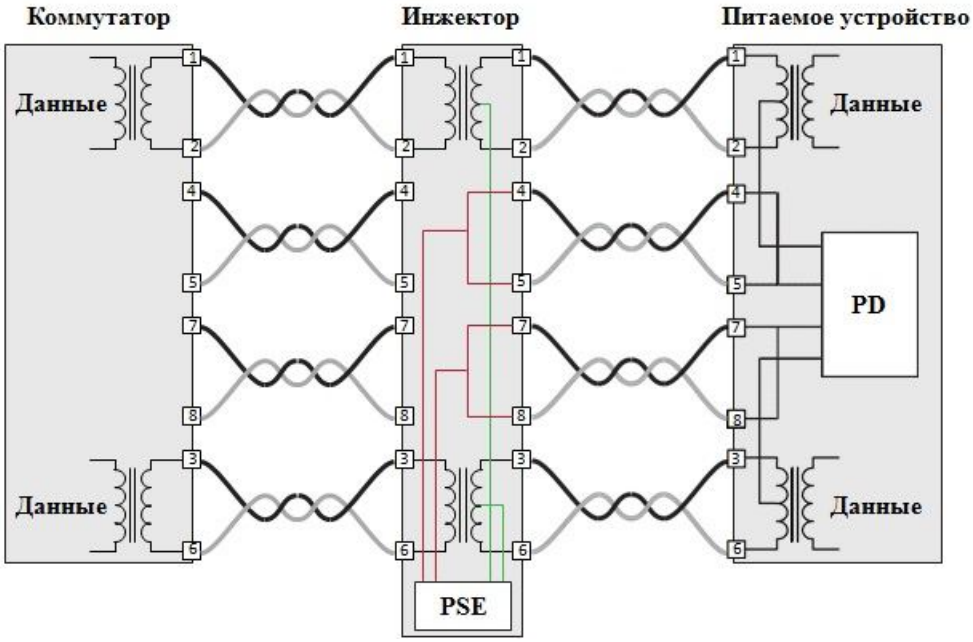


Рис. 6.47 Схема питания Midspan PSE в сети 10/100BASE-TX (вариант A – зеленый; вариант B - красный)

- Midspan PSE, поддерживающие 1000BASE-TX (Рис. 6.48): в варианте A питание передается по сигнальным парам 1, 2 и 3, 6; в варианте B питание передается по сигнальным парам 4, 5 и 7, 8.

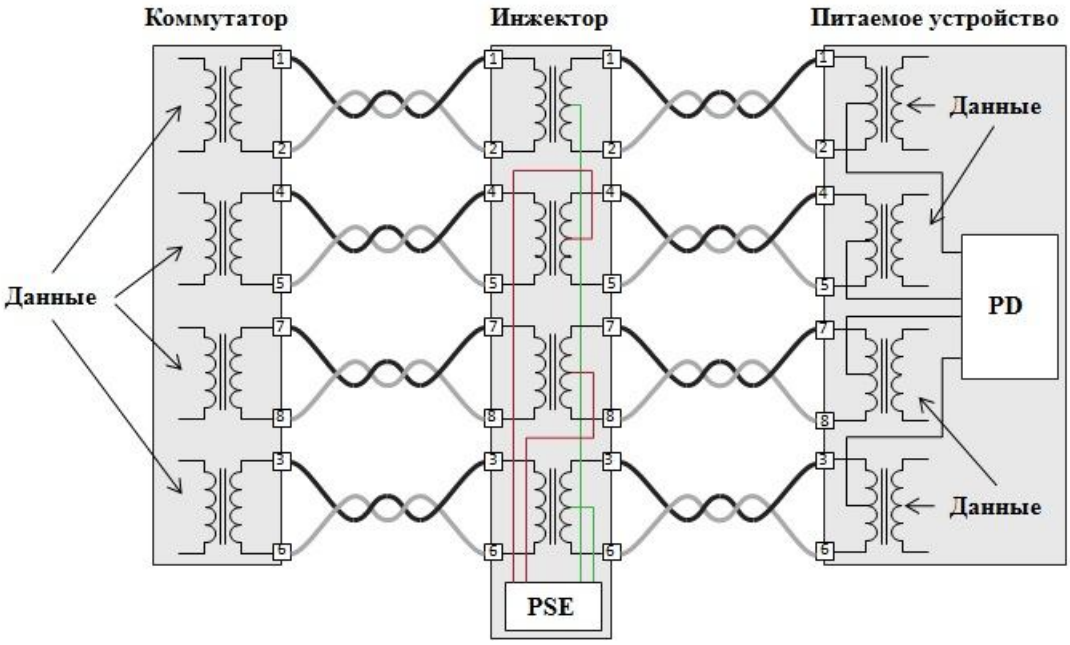


Рис. 6.48 Схема питания Midspan PSE в сети 1000BASE-T (вариант A – зеленый; вариант B - красный)

Устройство PSE может поддерживать передачу питания в соответствии с вариантом A, вариантом B или в соответствии с обоими вариантами. В последнем случае не допускается, чтобы PSE одновременно подавал питание по варианту A и варианту B в подключенный сегмент. Устройство PD обязано уметь принимать из сети и выделять питание при любом варианте его подачи (A или B), в том числе и при изменении полярности подключения (при использовании прямых или перекрестных кабелей).

Устройство PSE подает питание в кабель только в том случае, когда определит, что подключенное к нему устройство является устройством типа PD. Если удаленное устройство не поддерживает PoE, то питание ему подаваться не будет. У всех устройств типа PD величина сопротивления приемника должна лежать в диапазоне от 19 до 26,5 кОм. Специальная процедура инициализации PSE позволяет автоматически определять величину сопротивления подключенного устройства. Для того чтобы удостовериться, что подключенное устройство является устройством типа PD, PSE проводит двойное измерение тока с двумя разными уровнями напряжения (от 2,80 до 10 В) и на основе этих параметров вычисляет значение сопротивления приемника. Если полученное значение сопротивления лежит в диапазоне от 19 до 26,5 кОм, то PSE считает, что подключенное устройство является устройством типа PD и переходит к следующему этапу.

После идентификации удаленного устройства как PoE-совместимого PSE выполняет его классификацию. Классификацией называется способность PSE отправлять запросы PD с целью определения мощности, потребляемой PD.

Процедура классификации по мощности предназначена для взаимной идентификации PSE и PD. Механизм взаимной идентификации позволяет PD Типа 2 отличить PSE Типа 1 от PSE Типа 2, PSE Типа 2 отличить PD Типа 1 от PD Типа 2.

Существует два формы классификации: классификация на физическом уровне и классификация на канальном уровне.

Классификация на физическом уровне использует электрические характеристики PD, на основе которых PSE определяет какой класс присвоить PD на основе потребляемой им мощности и вычисляет свою минимальную мощность на выходе (таблица 6.1). Спецификация PoE делит устройства PD в зависимости от потребляемой мощности на 5 классов: от 0 до 4 (таблица 6.2).

Таблица 6.1 Классификация на физическом уровне

Класс	Минимальная мощность на выходе устройства PSE, Вт
0	15,4
1	4
2	7
3	15,4
4	30

Таблица 6.2 Классификация устройств PD по мощности

Класс	Средняя мощность на входе устройства PD, Вт
0	13
1	3,84
2	6,49
3	13
4	25,5

Классификация на канальном уровне выполняется PSE и PD с помощью протокола Data Link Layer (DLL). Эта классификация обеспечивает более точное определение потребляемой мощности PD и позволяет PSE динамически изменять значение выходной мощности в зависимости от текущих потребностей PD. Устройства PSE могут выполнять классификацию PD на физическом уровне, на канальном уровне или комбинацию обоих методов.

После завершения процесса классификации устройство PSE подает в кабель напряжение 48 В. Спецификация PoE предусматривает автоматическое отключение напряжения питания, если сопротивление приемника или отдаваемый ток резко меняется.

Следует рассказать об еще одном типе устройств PoE, которые не описаны стандартом. Это *PoE-сплиттеры*. Сплиттер является пассивным устройством и используется для подключения к сети PoE устройств без поддержки функции PoE. Функция сплиттера противоположна функции инжектора. Сплиттер подключается к сети PoE, из которой получает данные и питание по кабелю на основе витой пары. На выходе он разделят данные и питание, которые далее передаются соответственно через кабель на основе витой пары и стандартный кабель питания. То есть, на входе у сплиттера стандартный разъем RJ-45, а на выходе – разъем RJ- 45 и разъем питания.

Рассмотрим пример подключения IP-камеры без поддержки технологии PoE через сплиттер PoE, например DWL-P50. Схема подключения устройств показана на Рис. 6.49.

Шаг 1. Соединить между собой PoE-порты коммутатора и сплиттера с помощью Ethernet-кабеля.

Шаг 2. Отдельным кабелем Ethernet подключить порт LAN OUT сплиттера к LAN-порту IP-камеры.

Шаг 3. На сплиттере установить выходное напряжение (5В или 12В), которое требуется для питания IP-камеры, используя встроенный переключатель.

Шаг 4. Подключить кабель питания постоянного тока, входящий в комплект поставки, к сплиттеру и к разъему питания IP-камеры.

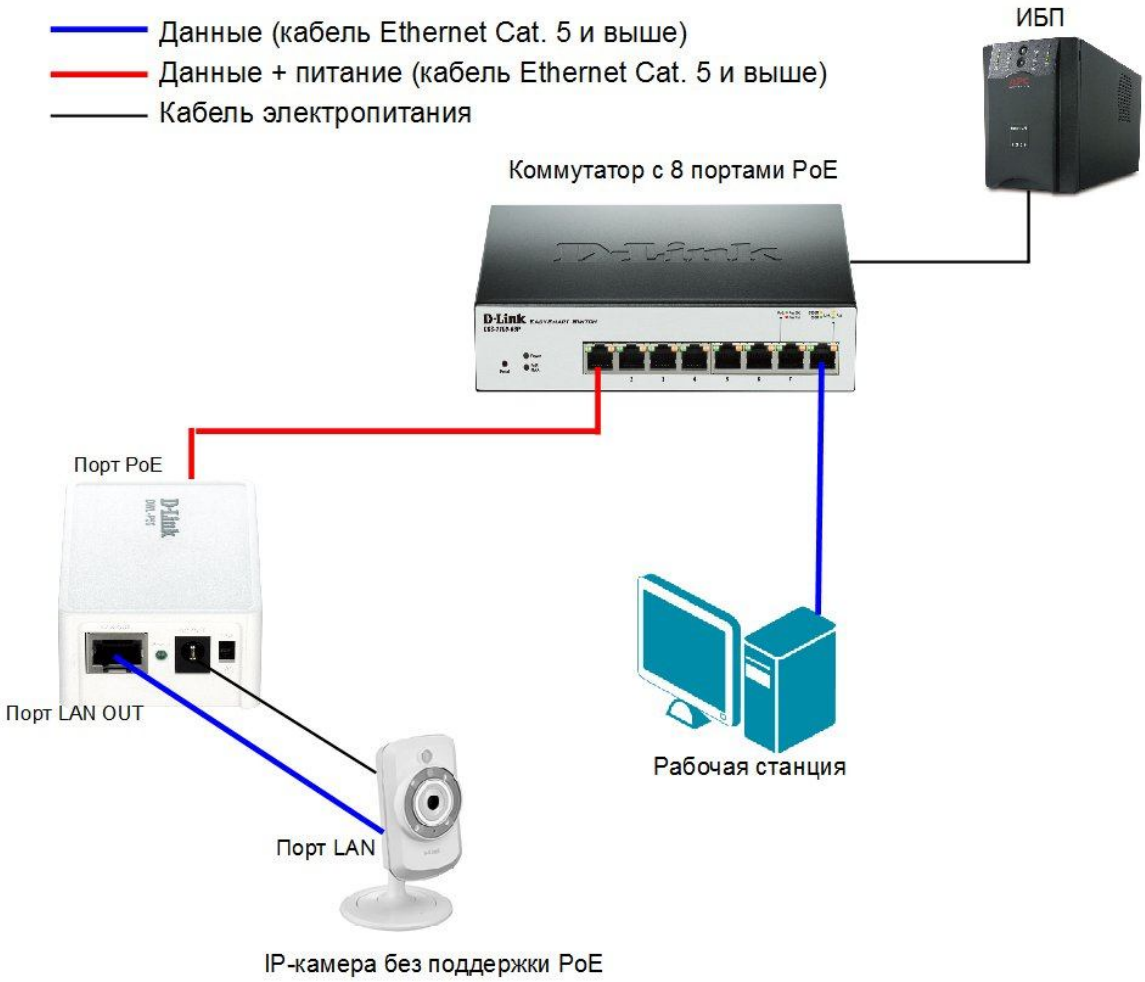


Рис. 6.49 Подключение IP-камеры с помощью сплиттера к сети PoE

Предположим, что организации требуется подключить устройство (точку доступа или камеру), расположенное в труднодоступном месте, но локальная сеть не поддерживает функционал PoE. Решить проблему подведения питания к удаленному устройству с минимальными затратами можно с помощью установки инжектора и сплиттера в разрыв сегмента Ethernet между коммутатором и удаленным устройством. Компания D-Link предлагает наборы, состоящие из инжектора и сплиттера PoE. Рассмотрим пример организации подачи питания для IP-камеры с помощью адаптера PoE DWL-P200 (Рис. 6.50), состоящего из инжектора и сплиттера. Для этого необходимо выполнить следующие шаги по подключению устройств.

Шаг 1. Подключить к основному модулю (инжектору) адаптер питания, который входит в комплект поставки.

Шаг 2. С помощью Ethernet-кабеля соединить порт LAN IN основного модуля и порт коммутатора.

Шаг 3. Соединить отдельным кабелем Ethernet порты PoE основного и терминального (сплиттера) модулей (на рисунке показан красным цветом).

Шаг 4. Подключить один конец Ethernet-кабеля к порту LAN OUT терминального модуля (сплиттера), другой конец – к LAN-порту IP-камеры.

Шаг 5. На терминальном модуле установить выходное напряжение (5В или 12В), которое требуется для питания IP-камеры, используя встроенный переключатель.

Шаг 6. Подключить кабель питания постоянного тока, входящий в комплект поставки, к терминальному модулю и к разъему питания IP-камеры.

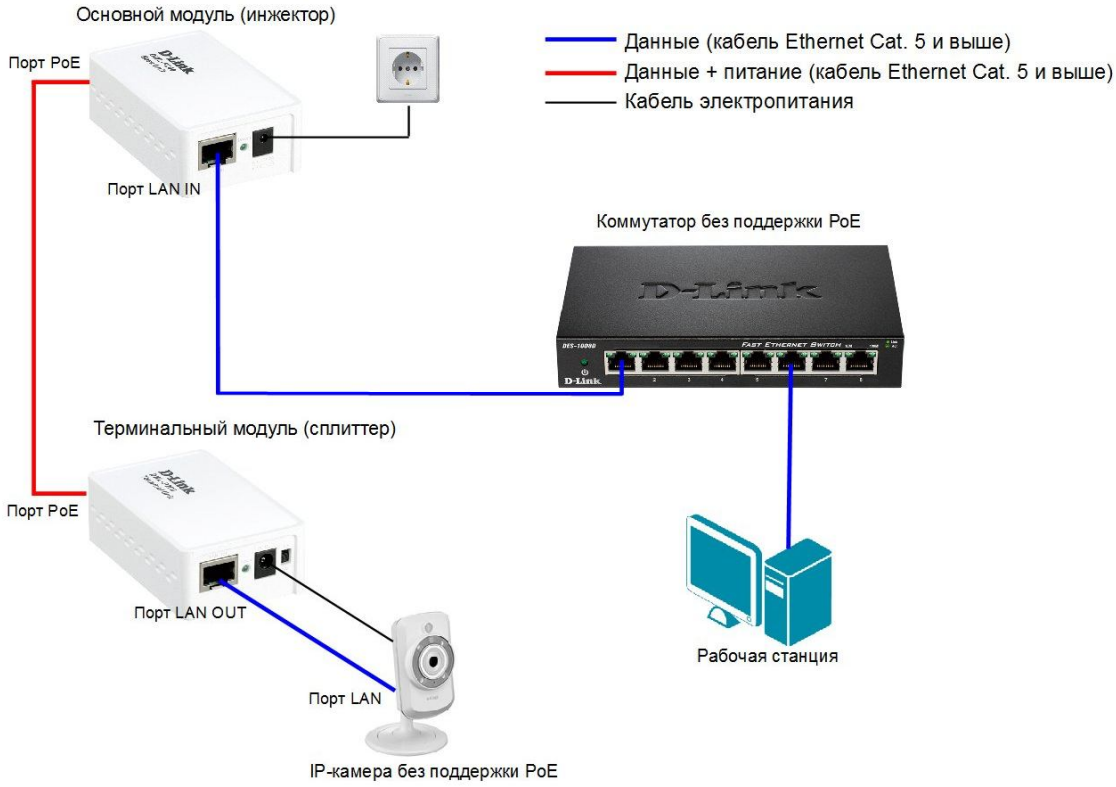


Рис. 6.50 Организация подачи электропитания в сети без поддержки технологии PoE