Министерство образования и науки Российской Федерации
Уральский федеральный университет
им. Первого президента России Б.Н. Ельцина

Руденков Н.А., Долинер Л.И.

ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

учебник

Екатеринбург
2011

Содержание

УДК 681.3(075)

ББК 423

Д64

Руденков Н.А., Долинер Л.И. Основы сетевых технологий: Учебник для вузов. Екатеринбург: Изд-во Уральского. Федерального ун-та, 2011. – 300 с.

Данный материал появился в результате анализа рынка печатных изданий по сходной тематике. Авторы попытались оптимизировать классические объёмы информации, касающейся темы основ сетевых технологий и одновременно систематизировать отдельные сведения о новых технологиях и стандартах.

Данный материал, в первую очередь, предназначен для студентов высших и средних учебных заведений, но будет интересен всем желающим расширить свой кругозор и получить представление об основах современных сетевых технологий. Сетевые технологии стали неотъемлемой частью нашей жизни, и современному человеку поневоле необходимо иметь хотя бы начальное представление обо всех окружающих его компьютерных, интерактивных, мультимедийных и прочих технологиях. Авторы надеются, что этот материал поможет читателю разобраться в многообразии современных технологий и компьютерных терминологий.

Учебник предназначен для студентов технических вузов, которые изучают компьютерные сети. Книга также может быть полезной для учителей информатики и преподавателей профессиональных учебных заведений.

Рецензенты: доктор педагогических наук, профессор Б.Е. Стариченко (Уральский государственный педагогический университет), кандидат физико-математических наук, профессор В.Н. Ларионов (Уральский государственный университет)

1. Базовые понятия сетевых технологий

1.1. Вводная часть

История появления вычислительных сетей напрямую связана с развитием компьютерной техники. Первые мощные компьютеры (*мэйнфреймы*), занимали по объёму комнаты и целые здания. Порядок подготовки и обработки данных был очень сложен и трудоёмок. Пользователи подготавливали перфокарты, содержащие данные и команды программ, и передавали их в вычислительный центр. Операторы вводили эти карты в компьютер, а распечатанные результаты пользователи получали обычно только на следующий день. Такой способ сетевого взаимодействия предполагал полностью централизованную обработку и хранение.

Мэйнфрейм – высокопроизводительный компьютер общего назначения со значительным объемом оперативной и внешней памяти, предназначенный для выполнения интенсивных вычислительных работ. Обычно с мэнфреймом работают множество пользователей, каждый из которых располагает лишь **терминалом**, лишенным собственных вычислительных мощностей.

Компьютерный терминал (от лат. terminalis – относящийся к концу) – устройство ввода/вывода, рабочее место на многопользовательских ЭВМ, монитор с клавиатурой. Примеры терминальных устройств: консоль, терминальный сервер, тонкий клиент, эмулятор терминала, telnet.

Хост (от англ. Host – хозяин, принимающий гостей) – любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. В более частном случае под хостом могут понимать любой компьютер, сервер, подключенный к локальной или глобальной сети.

Компьютерная сеть (вычислительная сеть, сеть передачи данных) – система связи компьютеров и/или компьютерного оборудования (серверы, маршрутизаторы и другое оборудование). Для передачи информации могут быть использованы различные физические явления, как правило— различные виды электрических сигналов или электромагнитного излучения.

Для пользователей удобнее и эффективнее был бы интерактивный режим работы, при котором можно с терминала оперативно руководить процессом обработки своих данных. Но интересами пользователей на первых этапах развития вычислительных систем в значительной степени пренебрегали, поскольку *пакетный режим* – это самый эффективный режим использования вычислительной мощности, так как он позволяет выполнить в единицу времени больше пользовательских задач, чем любые другие режимы. К счастью эволюционные процессы не остановить, и вот в 60-х годах начали развиваться первые интерактивные многотерминальные системы. Каждый пользователь получал в свое

распоряжение терминал, с помощью которого он мог вести диалог с компьютером. И, хотя вычислительная мощность была централизованной, функции ввода и вывода данных стали распределёнными. Часто эту модель взаимодействия называют ***«терминал-хост»*** (**Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.**Рис. 1). Центральный компьютер должен работать под управлением операционной системы, поддерживающей такое взаимодействие, которое называется ***централизованным вычислением.*** Причём терминалы могли располагаться не только на территории вычислительного центра, но и быть рассредоточены по значительной территории предприятия. По сути это явилось прообразом первых ***локальных вычислительных сетей (ЛВС).*** Хотя такая машина полностью обеспечивает хранение данных и вычислительные возможности, подключение к ней удаленных терминалов не является сетевым взаимодействием, так как терминалы, являясь, по сути, периферийными устройствами, обеспечивают только преобразование формы информации, но не ее обработку.

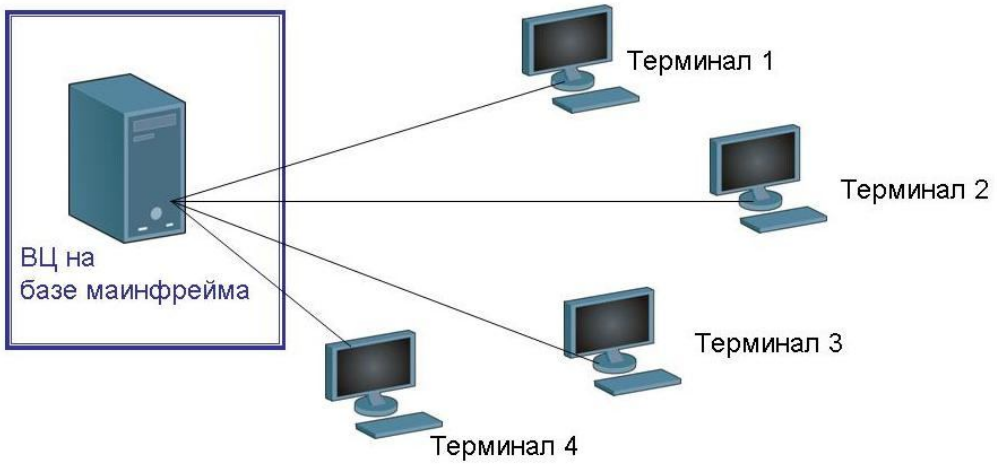


Рис. 1. Многотерминальная система

Локальная вычислительная сеть (ЛВС), (локальная сеть, сленг. локалка; англ. Local Area Network, LAN) – компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

Компьютер *(англ. computer — «вычислитель»),* ***ЭВМ*** *(электронная вычислительная машина)* — вычислительная машина для передачи, хранения и обработки информации.

Термин «компьютер» и аббревиатура «ЭВМ» (электронная вычислительная машина), принятая в СССР, являются синонимами. Однако, после появления **персональных компьютеров,** термин ЭВМ был практически вытеснен из бытового употребления.

Персональный компьютер, ПК *(англ. personal computer,* ***PC****), персональная ЭВМ* – компьютер, предназначенный для личного использования, цена, размеры и возможности которого удовлетворяют запросам большого количества людей. Созданный как вычислительная машина, компьютер, тем не менее, всё чаще используется как инструмент доступа в компьютерные сети.

В 1969 году Министерство обороны США посчитало, что на случай войны Америке нужна надёжная 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, первый из которых находился в Калифорнийском университете, а второй на расстоянии 600 км от него — в Стэндфордском университете.

Компьютерная сеть была названа ARPANET, в рамках проекта сеть объединила четыре указанных научных учреждения, все работы финансировались за счёт Министерства обороны США. Затем сеть ARPANET начала активно расти и развиваться, её начали использовать учёные из разных областей науки.

В начале 70-х годов произошел технологический прорыв в области производства компьютерных компонентов – появились большие интегральные схемы (БИС). Их сравнительно невысокая стоимость и высокие функциональные возможности привели к созданию мини-***ЭВМ*** (**Ошибка! Источник ссылки не найден.**Рис. 2), которые стали реальными конкурентами мэйнфреймов. Мини-ЭВМ выполняли задачи управления технологическим оборудованием, складом и другие задачи уровня подразделения предприятия. Таким образом, появилась концепция распределения компьютерных ресурсов по всему предприятию. Однако при этом все компьютеры одной организации по-прежнему продолжали работать автономно.

Именно в этот период, когда пользователи получили доступ к полноценным компьютерам, назрело решение объединения отдельных компьютеров для обмена данными с другими близко расположенными компьютерами. В каждом отдельном случае эту задачу решали по-своему. В результате появились первые локальные вычислительные сети.

Так как процесс творчества был спонтанным, да и не было единого решения по сопряжению двух и более компьютеров, то ни о каких сетевых стандартах не могло быть и речи.

А между тем к сети ARPANET в 1973 году были подключены первые иностранные организации из Великобритании и Норвегии, сеть стала международной. Параллельно с ARPANET стали появляться и развиваться другие сети университетов и предприятий.

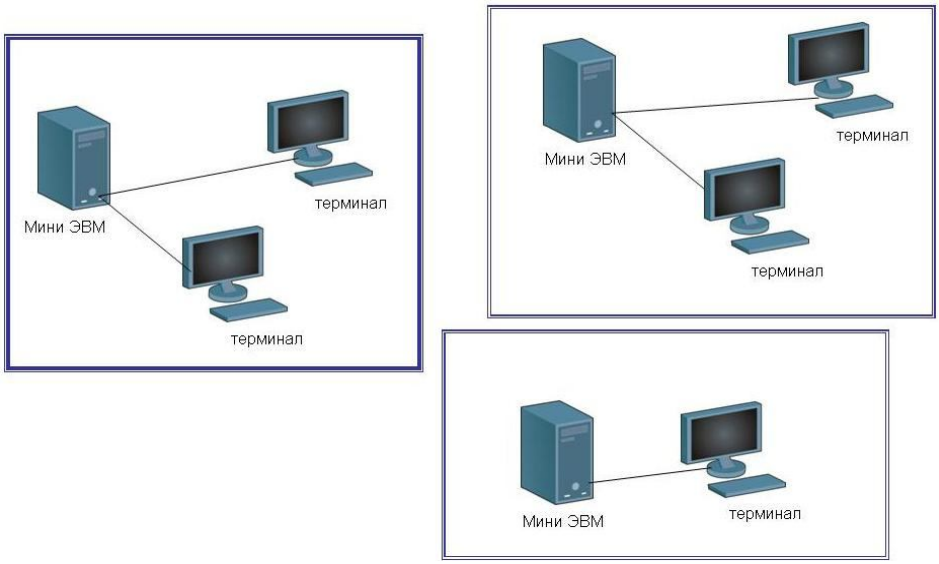


Рис. 2. Автономное использование нескольких мини-компьютеров на одном предприятии

В 1980 году было предложено связать вместе ARPANET и CSnet (Computer Science Research Network) через шлюз с использованием протоколов TCP/IP, и чтобы все подмножества сетей CSnet располагали доступом к шлюзу в ARPANET. Это событие, приведшее к соглашению относительно способа межсетевого общения между содружеством независимых вычислительных сетей, можно считать появлением ***Интернета*** в современном его понимании.

В середине 80-х годов положение дел в локальных сетях стало меняться. Утвердились стандартные технологии объединения компьютеров в сеть — **Ethernet, Arcnet, Token Ring, Token Bus,** несколько позже — **FDDI.** Мощным стимулом для их развития послужили ***персональные компьютеры.*** Эти устройства стали идеальным решением для создания ЛВС (**Ошибка! Источник ссылки не найден.**Рис. 3). С одной стороны они имели достаточную мощность для обработки индивидуальных заданий, и в то же время явно нуждались в объединении своих вычислительных мощностей для решения сложных задач.

Все стандартные технологии локальных сетей опирались на тот же принцип коммутации, который был с успехом опробован и доказал свои преимущества при передаче трафика данных в глобальных компьютерных сетях — ***принцип коммутации пакетов***.

Интернет (произносится как [интэрнэт]; англ. Internet, сокр. от Interconnected Networks – объединённые сети; сленг. инет, нет) – глобальная телекоммуникационная сеть информационных и вычислительных ресурсов. Служит физической основой для **Всемирной паутины (World Wide Web)**. Часто упоминается как **Всемирная сеть, Глобальная сеть,** либо просто **Сеть**.

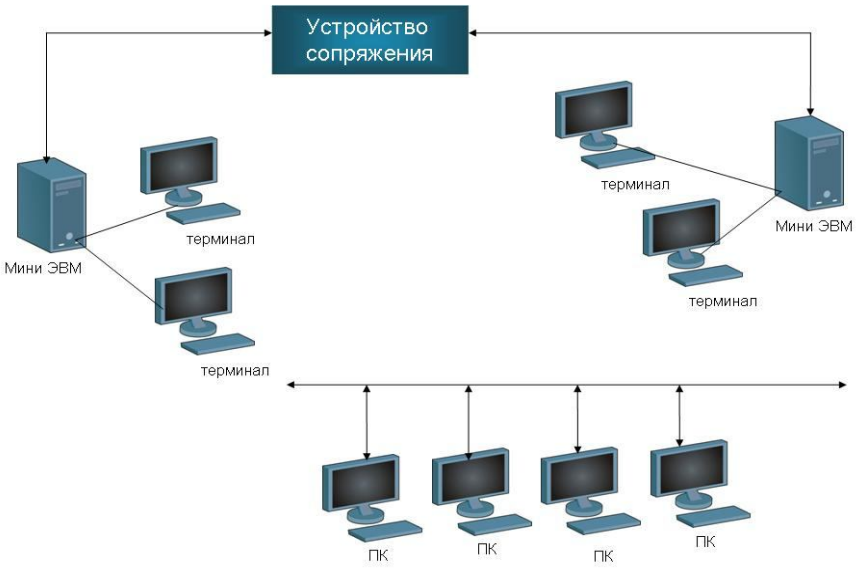


Рис. 3. Варианты подключения ПК в первых ЛВС

Стандартные сетевые технологии сделали задачу построения локальной сети почти тривиальной. Для создания сети достаточно было приобрести сетевые адаптеры соответствующего стандарта, например ***Ethernet***, стандартный кабель, присоединить адаптеры к кабелю стандартными разъемами (Рис. 4) и установить на компьютер одну из популярных сетевых операционных систем, например Novell NetWare. После этого сеть начинала работать, и последующее присоединение каждого нового компьютера не вызывало никаких проблем — естественно, если на нем был установлен сетевой адаптер той же технологии.

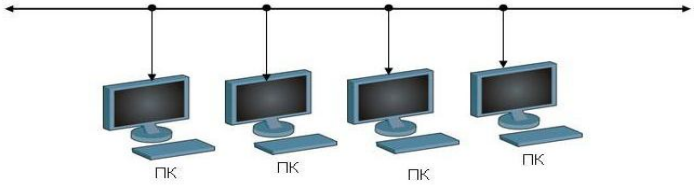


Рис. 4. Подключение нескольких компьютеров по схеме «общая шина».

Сетевая плата**, также известная как **сетевая карта, сетевой адаптер, Ethernet-адаптер, NIC (англ. network interface controller) — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.

Операционная система, ОС (англ. operating system)— базовый комплекс компьютерных программ, обеспечивающий интерфейс с пользователем, управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных программ и утилит.

1.2. Телекоммуникационные и вычислительные сети

1.2.1. Общие понятия, терминология

Компьютерная сеть или телекоммуникационная вычислительная сеть представляет собой сеть обмена и распределенной обработки информации, образуемая множеством взаимосвязанных абонентских систем и средствами связи; средства передачи и обработки информации ориентированы в ней на коллективное использование общесетевых ресурсов – информационных, программных, аппаратных.

Абонентская система – совокупность абонента (объекта, генерирующего и потребляющего информацию) и рабочий станции.

Рабочая станция – система оборудования конечного пользователя сети, включающая персональный компьютер (терминал), вместе с периферийными средствами ввода-вывода и программным обеспечением, средства связи с коммуникационной подсетью компьютерной сети, выполняющие прикладные процессы.

Телекоммуникационная система – это совокупность физической среды передачи информации, аппаратных и программных средств, обеспечивающих взаимодействие абонентской системы.

Прикладной процесс – это различные процедуры ввода, хранения, обработки и выдачи информации, выполняемые в интересах пользователей и описываемые прикладными программами.

Компьютерные сети могут работать в различных режимах: обмена данными между абонентскими системами, запроса и выдачи информации, сбора информации, пакетной обработки данных по запросам пользователей с удаленных терминалов, в диалоговых режимах.

Компьютерные сети решили две очень важные проблемы: обеспечение в принципе неограниченного доступа к ПК пользователей независимо от территориального расположения и возможность оперативного перемещения больших массивов информации на любые расстояния, позволяющая своевременно получать данные для принятия тех или иных решений.

1.2.2. Аппаратные и программные компоненты сети

Что получает пользователь при подключении своего ПК к ЛВС? Прежде всего, он может пользоваться не только файлами, дисками, принтерами и другими ресурсами своего компьютера, но аналогичными ресурсами других компьютеров, подключенных к этой же сети. Правда, для этого недостаточно снабдить компьютеры сетевыми адаптерами и соединить их кабельной системой.

Необходимы еще некоторые добавления к ***операционным системам*** этих компьютеров. На тех компьютерах, ресурсы которых должны быть доступны всем пользователям сети, необходимо добавить *модули*, которые постоянно будут находиться в режиме ожидания запросов, поступающих по сети от других компьютеров. Обычно такие ***модули*** называются ***программными серверами***, так как их главная задача - ***обслуживать*** запросы на доступ к ресурсам своего компьютера. На компьютерах, пользователи которых хотят получать доступ к ресурсам других компьютеров, также нужно добавить к операционной системе некоторые специальные программные модули, которые должны вырабатывать запросы на доступ к удаленным ресурсам и передавать их по сети на нужный компьютер. Такие модули обычно называют программными ***клиентами.*** В современные популярные операционные системы для ПК, все необходимые программные модули для сетевых подключений уже интегрированы.

Собственно же сетевые адаптеры и каналы связи решают в сети достаточно простую задачу – они передают сообщения с запросами и ответами от одного компьютера к другому, а основную работу по организации совместного использования ресурсов выполняют клиентские и серверные части операционных систем.

Таким образом, когда на устройстве, с которым непосредственно взаимодействует пользователь, стала выполняться некоторая предварительная обработка информации, это привело к появлению ***модели взаимодействия «клиент-сервер».***

Сервер *(от англ. server, обслуживающий):*

Сервер (программное обеспечение) **–** программное обеспечение, принимающее запросы от клиентов.

Сервер (аппаратное обеспечение) **–** компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций.

Клиент *(информатика, от лат.cliens, множ. clientes)*– аппаратный или программный компонент вычислительной системы, посылающий запросы серверу.

По способу взаимодействия серверов и клиентов определяют два вида сетей: ***«клиент-сервер» (client-server) и «равный с равным» (peer-to-peer).*** Поскольку клиентом сети является пользователь, выполняющий на компьютере свои задачи, то сам компьютер пользователя, подключенный к сети, называется ***«рабочая станция» (workstation).*** Часто модели «клиент-сервер» и «равный с равным» могут одновременно существовать в одной сети. Сети, построенные по принципу «равный с равным», называют также одноранговыми сетями, в которых все компьютеры имеют одинаковый статус – ***ранг.***

Несмотря на рост вычислительной мощности ПК, многие задачи попрежнему требовали много больших вычислительных ресурсов. Появилась необходимость создания нового типа взаимодействия, новой структуры, обеспечивающей ***распределенную обработку информации***. В этой модели взаимодействия каждая из машин призвана решать свои задачи, что делает возможной специализацию: каждый компьютер работает над конкретной задачей, для ре-

шения которой он оптимизирован (в модели «клиент-сервера» сервер тоже специализирован и выполняет свои специфические задачи, но он при этом «самодостаточен» и никак не связан с другими серверами). При этом для решения задач ему необходимо получать результаты работы других ПК и, в свою очередь, передавать им свои результаты, что стало возможным только с объединением компьютеров в вычислительную сеть. Распределение задач между компьютерами сети позволяет расширить функциональные возможности каждого из них путем организации совместного доступа к ресурсам.

Одной из заметных тенденций развития вычислительной индустрии стала модель ***совместной обработки данных***. В этой модели несколько компьютеров используются для решения одной и той же задачи, а не только для обмена результатами вычислений. При использовании модели совместных вычислений возрастают суммарная вычислительная мощность и доступные ресурсы (оперативная и дисковая память), повышается отказоустойчивость всей системы в целом.

Как отмечалось ранее, модели «клиент-сервер» и «равный с равным» могут одновременно существовать в одной сети. Это стало возможным благодаря различным сетевым компонентам, важнейшими из которых можно назвать ***средства организации канала передачи данных*** между клиентами и серверами сети.

В простейшем случае канал передачи данных строится с использованием двух компонентов:

среды передачи данных (***проводная или беспроводная - wire или wireless***), обеспечивающей доставку информации от одного узла сети к другому;

сетевых интерфейсных карт (**network interface card, NIC**), обеспечивающих взаимодействие компьютера со средой передачи данных.

Однако это не единственные средства, которые используются для соединения компьютеров и формирования самой вычислительной сети. Объединять компьютеры в сеть и обеспечивать их взаимодействие помогают ***сетевые аппаратные и аппаратно-программные средства***. Эти средства можно разделить на следующие группы по их основному функциональному назначению:

- ***пассивное сетевое оборудование*** - соединительные разъёмы, кабеля, патч-корды, патч-панели, информационные розетки, и т.п.;
- ***активное сетевое оборудование*** - преобразователи (adapters), модемы (modems), повторители (repeaters), мосты (bridges), коммутаторы (switches), маршрутизаторы (routers), и т.п.

Некоторые примеры активного сетевого оборудования приведены на Рис. 5.

Проводные среды передачи информации создаются с использованием ***кабельных соединений*** на основе либо металлических проводников электрических сигналов, либо ***волоконно-оптических проводников световых сигналов***. При создании сетей передачи данных чаще всего используют именно проводные среды передачи информации.

Коммутатор DGS-1005D-GE

Сетевой адаптер (проводной) DGE-560T

Маршрутизатор DIR-855

Сетевой адаптер (беспроводной) DWA-556

Сетевой адаптер (беспроводной) DWA-140

Медиаконверторы (преобразователи среды) *DMC-920*

Устройство VoIP DPH-150S

Интернет видео камера DCS-3410

Интернет видео камера DCS-6620G

Рис. 5. Примеры сетевого оборудования

Кабель *(нидерл.* ***kabel)*** **—** один или несколько изолированных друг от друга проводников (жил), заключённых в оболочку.

Беспроводные среды передачи информации предусматривают организацию взаимодействия между компьютерами посредством передачи световых (инфракрасных) и радиочастотных сигналов.

Возможности той или иной компьютерной сети определяются ее информационным, аппаратным и программным обеспечением. Информационное обеспечение сети представляет собой единый информационный фонд, ориентированный на решаемые в сети задачи и содержащий базы данных общего применения, доступные для всех пользователей сети, базы данных индивидуального пользования, предназначенные для отдельных абонентов, базы знаний общего и индивидуального применения, автоматизированные базы данных – локальные и распределенные, общего и индивидуального назначения.

Аппаратное обеспечение составляют компьютеры различных типов (в том числе ноутбуки, нетбуки, карманные ПК, планшетные ПК, а так же сетевые принтеры, плоттеры и пр.), оборудование абонентских систем (в т.ч. локальные периферийные устройства), средства территориальных систем связи (в том числе узлов связи), аппаратура связи и согласования работы сетей одного и того же уровня или различных уровней (коммутаторы и маршрутизаторы).

Для повышения вычислительной мощности сети к ней могут подключаться вычислительные центры или центры обработки информации, к которым пользователи могут обращаться с запросами со своих абонентских систем или других рабочих мест. Такие центры снабжаются компьютерами в широком диапазоне по своим характеристикам: от персональных компьютеров до суперкомпьютеров.

Программное обеспечение (ПО) сетей отличается большим многообразием, как по своему составу, так и по перечню решаемых задач.

В общем виде функции ПО сети заключаются в следующем: планирование, организация и осуществление коллективного доступа пользователей к общесетевым ресурсам – телекоммуникационным, вычислительным, информационным, программным; автоматизация процессов программирования задач обработки информации; динамическое распределение и перераспределение общесетевых ресурсов с целью повышения оперативности и надежности удовлетворения запросов пользователей и т. д.

В составе ПО сетей выделяются такие группы:

- ***общесетевое ПО***, которое в качестве основных элементов включает распределенную операционную систему сети и комплект программ технического обслуживания всей сети и ее отдельных звеньев и подсистем, включая телекоммуникационную сеть;
- ***специальное ПО***, куда входят прикладные программные средства: интегрированные и функциональные пакеты прикладных программ общего назначения, прикладные программы сети, библиотеки стандартных программ, а также прикладные программы специального назначения, отражающие специфику предметной области пользователей при реализации своих задач;

- ***базовое программное обеспечение*** компьютеров абонентских систем, включающее операционные системы ПК, системы автоматизации программирования, контролирующие и диагностические тест-программы.

Важнейшие функции в сети выполняет распределённая операционная система: она управляет работой сети во всех ее режимах, обеспечивает оперативное и надежное удовлетворение запросов пользователей, динамическое распределение общесетевых ресурсов, координацию функционирования звеньев сети. Распределённая операционная система имеет иерархическую структуру, соответствующую стандартной семиуровневой модели взаимодействия открытых систем (ISO/OSI), и представляет собой систему программных средств, реализующих процессы взаимодействия абонентских систем объединенных общей архитектурой и коммуникационными протоколами. Распределённая операционная система обеспечивает взаимодействие асинхронных параллельных процессов в сети, сопровождаемое применением средств передачи сообщений между одновременно реализуемыми процессами и средств синхронизации этих процессов.

В составе распределённой операционной системы сети имеется набор расположенных по функциональным уровням модели ISO/OSI, управляющих и обслуживающих программ, главные функции которых состоят в следующем:

- распределение общесетевых ресурсов с целью удовлетворения запросов пользователей, т. е. обеспечение доступа отдельных прикладных программ к этим ресурсам;
- обеспечение межпрограммных методов доступа, т. е. организация связи между отдельными прикладными программами комплекса пользовательских программ, реализуемыми в различных абонентских системах сети;
- синхронизация работы пользовательских программ при их одновременном обращении к одному и тому же общесетевому ресурсу;
- удаленный ввод заданий с любой абонентской системы сети и их выполнение в любой другой абонентской системе сети в оперативном или пакетном режиме;
- передача текстовых сообщений пользователям в порядке реализации функций службы электронной почты, телеконференций, электронных досок объявлений, дистанционного обучения;
- обмен файлами между абонентскими системами сети, доступ к файлам, хранимым на удаленных компьютерах, и их обработка;
- защита информации и ресурсов сети от несанкционированного доступа, т. е. реализация функций служб безопасности сети;
- выдача справок, характеризующих состояние сети и использование ее ресурсов;
- планирование использования общесетевых ресурсов.

В рамках планирования использования общесетевых ресурсов осуществляется:

- планирование сроков и очередности получения и выдачи информации пользователям,

- распределение решаемых задач по компьютерам сети, распределение информационных ресурсов для этих задач,
- присвоение приоритетов задачам и выходным сообщениям,
- формирование и обработка очередей запросов пользователей с учетом или без учета
- приоритетов этих запросов, изменение конфигурации сети и т. д.

Кроме того, различают статическое планирование, которое осуществляется заранее, и динамическое планирование, выполняемое в процессе функционирования сети непосредственно перед началом решения задачи (группы задач), причем с поступлением каждой новой задачи составленный план корректируется с учетом складывающейся ситуации по свободным и занятым ресурсам сети, наличию очередей задач и т. д. Основным показателем эффективности организации вычислительного процесса в сети, планирования общесетевых ресурсов является время решения комплекса задач.

1.2.3. Классификация информационно-вычислительных сетей

Существует множество способов классификации сетей передачи данных. Основным критерием классификации принято считать способ администрирования. То есть в зависимости от того, как организована сеть и как она управляется, её можно отнести к ***локальной, распределённой, городской или глобальной сети.***

Управляет сетью или её сегментом ***сетевой администратор***.

Системный администратор **–** человек, ответственный за работу локальной сети или её части. В его обязанности входит обеспечение и контроль физической связи, настройка активного оборудования, настройка общего доступа и предопределённого круга программ, обеспечивающих стабильную работу сети. В случае сложных сетей управлением сети занимаются группы администраторов, их права и обязанности строго распределены, ведётся документация и журналирование действий.

Локальная вычислительная сеть (ЛВС, локальная сеть, сленг. локалка; англ. Local Area Network, LAN) — компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).

Отдельная локальная вычислительная сеть может иметь шлюзы с другими локальными сетями, а также быть частью глобальной вычислительной сети (например, Интернет) или иметь подключение к ней. Чаще всего локальные сети построены на технологиях Ethernet или Wi-Fi. Следует отметить, что раньше при построении вычислительных сетей использовались протоколы Frame Relay, Token Ring, на сегодняшний день встречающиеся всё реже и реже. Сегодня их можно встретить лишь в специализированных лабораториях, учебных заведениях и службах.

Для построения простой локальной сети используются сетевые устройства: маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры. В последнее время всё чаще и чаще при построении ЛВС используются преобразователи (конвертеры) среды, усилители сигнала (повторители разного рода) и специальные антенны.

Маршрутизация в локальных сетях обычно простая статическая, либо динамическая (основанная на протоколе RIP).

Иногда в локальной сети организуются рабочие группы (*англ. workgroup*) — формальное объединение нескольких компьютеров в группу с единым названием.

Разновидностью ЛВС можно считать сеть ***кампуса.***

Кампус - университетский городок, включающий, как правило, учебные помещения, научно-исследовательские институты, жилые помещения для студентов, библиотеки, аудитории, столовые и т. д. Иногда ***кампусом*** называют обособленную территорию, принадлежащую государственной или коммерческой крупной компании (организации), включающую внутрифирменную инфраструктуру, например, корпоративный университет. Слово ***Campus*** имеет латинское происхождение (обозначало «поле», «открытое пространство»).

Сеть кампуса (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 ***глобальная сеть.***

Городская вычислительная сеть (Metropolitan area network, MAN, *от англ. «сеть крупного города»)* – объединяет компьютеры в пределах города, представляет собой сеть по размерам меньшую, чем WAN, но большую, чем LAN.

Самым простым примером городской сети является система кабельного телевидения. Когда телевизионный сигнал передавался в дома абонентов через кабельные сети, а сама сеть занимала значительные объёмы по площади «покрытия» абонентов города. Когда Интернет стал привлекать к себе массовую аудиторию, операторы кабельного телевидения поняли, что, внеся небольшие изменения в систему, можно сделать так, чтобы по тем же каналам в неиспользуемой части спектра передавались (причём в обе стороны) цифровые данные. С этого момента кабельное телевидение стало постепенно превращаться в MAN. Но MAN— это не только «продвинутое» кабельное телевидение.

Как правило, MAN не принадлежит какой-либо отдельной организации, в большинстве случаев её соединительные элементы и прочее оборудование принадлежит группе пользователей или же провайдеру, кто берёт плату за обслуживание. MAN часто действует как высокоскоростная сеть, чтобы позволить совместно использовать региональные ресурсы (подобно большой LAN). Это также часто используется, чтобы обеспечить общедоступное подключение к другим сетям, используя связь с WAN.

Недавние разработки, связанные с высокоскоростным беспроводным доступом в Интернет, привели к созданию других MAN, которые описаны в стандарте IEEE 802.16.

Стандарт IEEE 802.16, опубликованный в апреле 2002 года, описывает wireless MAN Air Interface. 802.16 — это беспроводная технология т.н. «последней мили», которая использует диапазон частот от 10 до 66 ГГц. Так как это сантиметровый и миллиметровый диапазон, то необходимо условие «прямой видимости». Стандарт поддерживает топологию point-to-multipoint, технологии frequency-division duplex (FDD) и time-division duplex (TDD), с поддержкой quality of service (QoS). Возможна передача звука и видео. Стандарт определяет пропускную способность 120 Мбит/с на каждый канал в 25 МГц.

Стандарт 802.16a последовал за стандартом 802.16. Он был опубликован в апреле 2003 и использует диапазон частот от 2 до 11 ГГц. Стандарт поддерживает ячеистую топологию (mesh networking). Стандарт не накладывает условие «прямой видимости».

WMAN (Wireless Metropolitan Area Networks) — беспроводные сети масштаба города. Предоставляют широкополосный доступ к сети через радиоканал, где точки связаны скоростными каналами. В диаметре такая сеть может составлять от 5 до 50 километров.

Глобальная вычислительная сеть, ГВС (англ. Wide Area Network, WAN) представляет собой компьютерную сеть, охватывающую большие территории и включающую в себя сети городов, стран, континентов.

ГВС служат для объединения различных сетей так, чтобы пользователи и компьютеры, где бы они ни находились, могли взаимодействовать со всеми остальными участниками глобальной сети. Лучшим примером ГВС является Интернет, но существуют и другие сети, например FidoNet.

Глобальные вычислительные сети совмещают компьютеры, рассредоточенные на расстоянии сотен и тысяч километров. Часто используются уже существующие и не очень качественные линии связи. Более низкие, чем в локальных сетях, скорости передачи данных (десятки килобит в секунду) ограничивают набор задаваемых услуг передачей файлов, преимущественно не в оперативном, а в фоновом режиме, с использованием электронной почты.

Для стойкой передачи дискретных данных применяются более сложные методы и оборудование, чем в локальных сетях.

Некоторые ГВС построены исключительно для частных или государственных организаций, другие являются средством коммуникации корпоративных ЛВС с сетью Интернет или посредством Интернет с удалёнными сетями, входящими в состав корпоративных. Чаще всего ГВС опирается на выделенные линии, на одном конце которых маршрутизатор подключается к ЛВС, а на другом коммутатор связывается с остальными частями ГВС. Основными используемыми протоколами являются TCP/IP, SONET/SDH, MPLS, ATM и Frame relay. Ранее был широко распространён протокол X.25, который может по праву считаться прародителем Frame relay.

Глобальные сети отличаются от локальных тем, что рассчитаны на неограниченное число абонентов и используют различные каналы связи, среды передачи данных, технологии. На магистральных направлениях (между городами, странами) используются существующие каналы общей связи (в том числе министерств и ведомств федерального подчинения).

Большинство локальных сетей имеют выход в глобальную сеть, но характер переданной информации, принципы организации обмена, режимы доступа, к ресурсам внутри локальной сети, как правило, сильно отличаются от тех, что принято в глобальной сети. И хотя все компьютеры локальной сети в данном случае включены также и в глобальную сеть, специфику локальной сети это не меняет. Возможность выхода в глобальную сеть остается всего лишь одним из ресурсов, распределённым между пользователями локальных сетей.

1.3. Топологии локальных вычислительных сетей

При создании компьютерной сети передачи данных, когда соединяются все компьютеры сети и другие сетевые устройства, формируется ***топология компьютерной сети***.

Сетевая топология (от греч. τοπος, - место) - способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

1.3.1. Физическая топология сети передачи данных

Исторически сложились определённые типы физических топологий сети. Рассмотрим некоторые, наиболее часто встречающиеся топологии.

«Общая шина»

Общая шина (**Ошибка! Источник ссылки не найден.**Рис. 6) являлась до недавнего времени самой распространенной топологией для локальных сетей. В этом случае компьютеры подключаются к одному коаксиальному кабелю по схеме «монтажного ИЛИ». Передаваемая информация, в этом случае, распространяется в обе стороны.

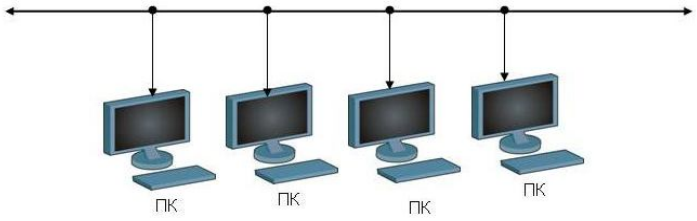


Рис. 6. Схема подключения компьютеров по схеме «общая шина».

Применение топологии «общая шина» снижает стоимость кабельной прокладки, унифицирует подключение различных модулей, обеспечивает возможность почти мгновенного широковещательного обращения ко всем станциям сети. Основными преимуществами такой схемы являются дешевизна и простота разводки кабеля по помещениям. Самый серьезный недостаток общей шины

заключается в ее низкой надежности: любой дефект кабеля или какого-нибудь из многочисленных разъемов полностью парализует всю сеть.

Другим недостатком общей шины является ее невысокая производительность, так как при таком способе подключения в каждый момент времени только один компьютер может передавать данные в сеть. Поэтому пропускная способность канала связи всегда делится здесь между всеми узлами сети.

Топология «звезда»

В этом случае каждый компьютер подключается отдельным кабелем к общему устройству, называемому **коммутатором (концентратором, хабом),** который находится в центре сети (Рис. 7). В функции коммутатора входит направление передаваемой компьютером информации одному или всем остальным компьютерам сети. Главное преимущество этой топологии перед общей шиной - значительно большая надежность. Любые неприятности с кабелем касаются лишь того компьютера, к которому этот кабель присоединен, и только неисправность коммутатора может вывести из строя всю сеть. Кроме того, коммутатор может играть роль интеллектуального фильтра информации, поступающей от узлов в сеть, и при необходимости блокировать запрещенные администратором передачи.

Сетевой концентратор или ***Хаб*** (жарг. от англ. Hub – центр деятельности) – сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент сети. Устройства подключаются при помощи витой пары, коаксиального кабеля или оптоволокна. Термин концентратор (хаб) применим также к другим технологиям передачи данных: USB, FireWire и пр.

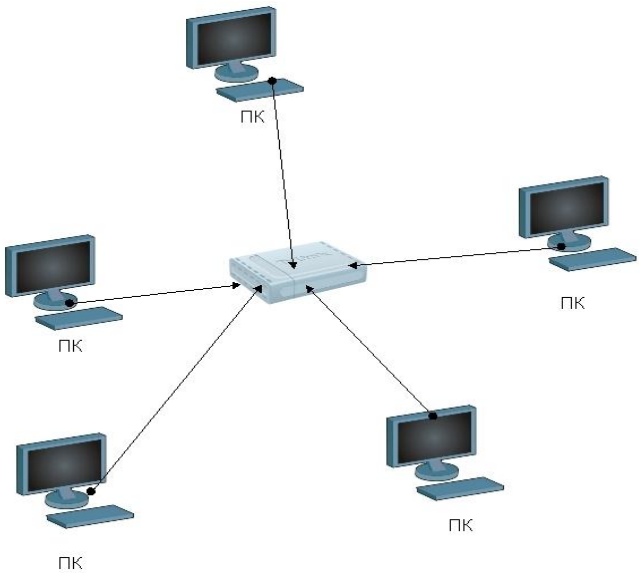


Рис. 7. Схема подключения компьютеров по схеме «звезда»

Топология «кольцо»

В информационно вычислительных сетях с кольцевой **конфигурацией** данные передаются по кольцу от одного компьютера к другому, как правило, в одном направлении (Рис. 8). Если компьютер распознает данные как «свои», то он копирует их себе во внутренний буфер. Кольцо представляет собой очень удобную конфигурацию для организации обратной связи - данные, сделав полный оборот, возвращаются к узлу-источнику. Поэтому этот узел может контролировать процесс доставки данных адресату. Часто это свойство кольца используется для тестирования связности сети и поиска узла, работающего некорректно. Для этого в сеть посылаются специальные тестовые сообщения.

В сети с кольцевой топологией необходимо принимать специальные меры, чтобы в случае выхода из строя или отключения какой-либо станции не прервался канал связи между остальными станциями.

Поскольку такое дублирование повышает надёжность системы, данный стандарт с успехом применяется в магистральных каналах связи.

Данная физическая топология с успехом реализуется в сетях, созданных с использованием технологии FDDI.

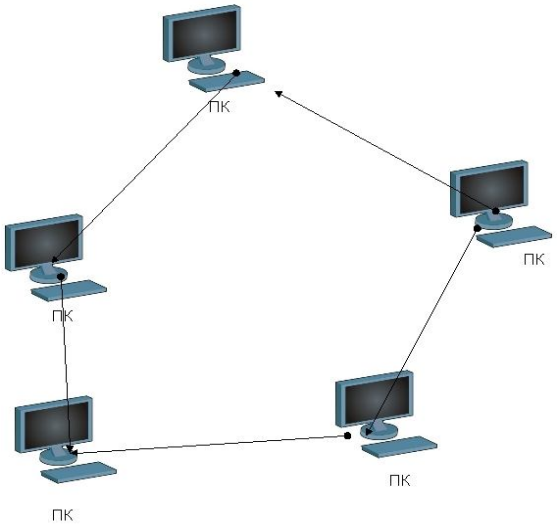


Рис. 8. Схема подключения компьютеров по схеме «кольцо»

FDDI (англ. Fiber Distributed Data Interface — распределённый волоконный интерфейс данных) - стандарт передачи данных в локальной сети, протяжённостью до 200 километров. Стандарт основан на протоколе ***Token Bus***. В качестве среды передачи данных в FDDI рекомендуется использовать волоконно-оптический кабель, однако можно использовать и медный кабель, в таком случае используется сокращение ***CDDI (Copper Distributed Data Interface).*** В качестве топологии используется схема **двойного кольца**, при этом данные в кольцах циркулируют в разных направлениях. Одно кольцо считается основным, по нему передаётся информация в обычном состоянии; второе — вспомогательным, по нему данные передаются в случае обрыва на первом кольце. Для

контроля за состоянием кольца используется сетевой маркер, как и в технологии Token Ring.

Полносвязная топология

Полносвязная топология соответствует сети, в которой каждый компьютер сети связан со всеми остальными (Рис. 9). Несмотря на логическую простоту, этот вариант оказывается громоздким и неэффективным. Действительно, каждый компьютер в сети должен иметь большое количество коммуникационных портов, достаточное для связи с каждым из остальных компьютеров сети. Для каждой пары компьютеров должна быть выделена отдельная электрическая линия связи. Полносвязные топологии применяются редко, так как не удовлетворяют ни одному из приведенных выше требований. Чаще этот вид топологии используется в многомашинных комплексах или глобальных сетях при небольшом количестве компьютеров.

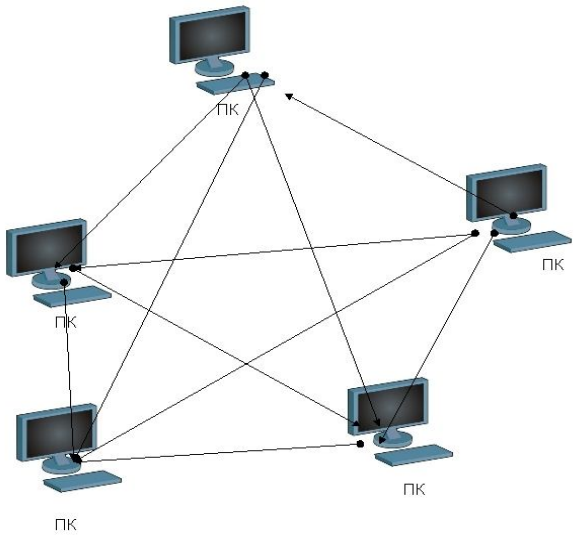


Рис. 9.Схема подключения компьютеров по схеме «полносвязная топология»

Ячеистая топология

Ячеистая топология (англ. mesh-ячейка сети) получается из полносвязной путем удаления некоторых возможных связей (Рис. 10). В сети с ячеистой топологией непосредственно связываются только те компьютеры, между которыми происходит интенсивный обмен данными, а для обмена данными между компьютерами, не соединенными прямыми связями, используются транзитные передачи через промежуточные узлы. Ячеистая топология допускает соединение большого количества компьютеров и характерна, как правило, для глобальных сетей.

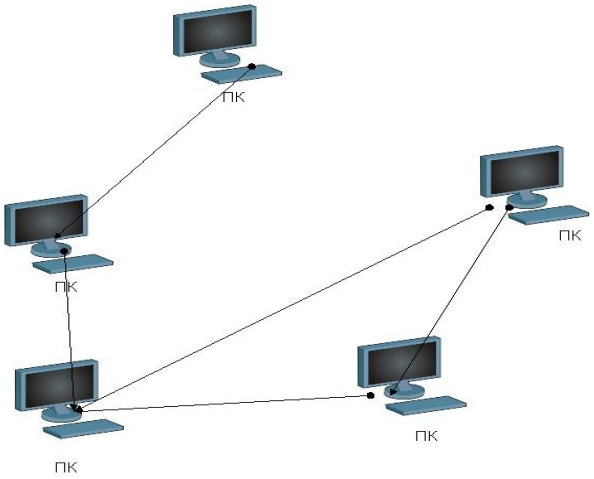


Рис. 10. Схема подключения компьютеров по схеме «ячеистая топология»

В то время как небольшие сети, как правило, имеют типовую топологию - звезда, кольцо или общая шина, для крупных сетей характерен симбиоз различных топологий. В таких сетях можно выделить отдельные произвольно связанные фрагменты (подсети), имеющие типовую топологию, поэтому их называют сетями со смешанной топологией.

Топология «дерево»

Такая топология является смешанной, здесь взаимодействуют системы с различными топологиями. Такой способ смешанной топологии чаще всего применяется при построении ЛВС с небольшим количеством сетевых устройств, а также при создании корпоративных ЛВС (Рис. 11). Данная топология совмещает в себе относительно низкую себестоимость и достаточно высокое быстродействие, особенно при использовании различных сред передачи данных - сочетании медных кабельных систем, ВОЛС, а также применяя управляемые коммутаторы.

В топологиях типа «общая шина» и «кольцо» линии связи, соединяющие элементы сети (компьютеры, сетевые устройства и пр.), являются ***распределёнными (англ. shared)***, т.е. они являются ***линиями связи общего использования*** (Рис.6,8).

Помимо ***распределённых***, существуют ***индивидуальные линии связи***, когда каждый элемент сети имеет свою собственную (не всегда единственную) линию связи. Пример — сеть, построенная по топологии «звезда», когда в центре располагается устройство типа коммутатор, а каждый компьютер подключён отдельной линией связи (Рис. 11).

Общая стоимость сети построенной с применением распределённых линий связи будет гораздо ниже, однако и производительность такой сети будет ниже, потому что сеть с распределённой средой при большом количестве узлов будет работать всегда медленнее, чем аналогичная сеть с индивидуальными линиями связи, так как пропускная способность индивидуальной линии связи достается

одному компьютеру, а при ее совместном использовании - делится на все компьютеры сети.

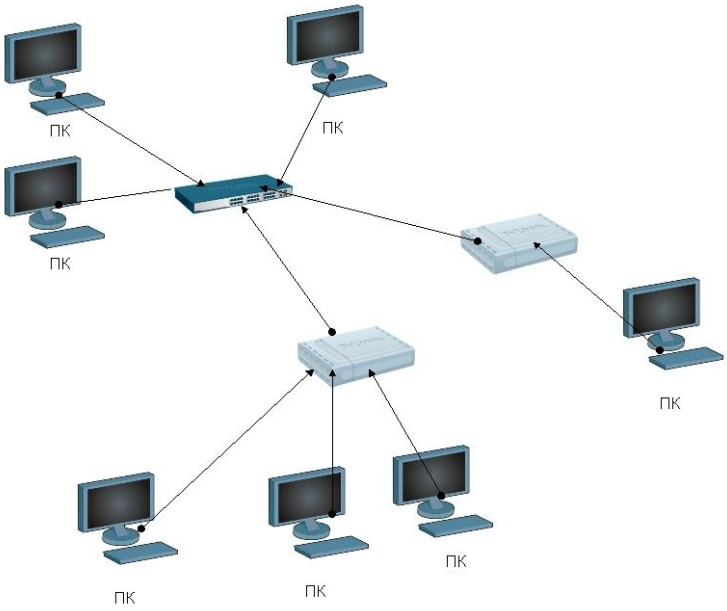


Рис. 11. Схема подключения компьютеров по схеме «дерево»

В современных сетях, в том числе глобальных, индивидуальными являются только линии связи между конечными узлами и коммутаторами сети, а связи между коммутаторами (маршрутизаторами) остаются распределёнными, так как по ним передаются сообщения разных конечных узлов (Рис. 12).

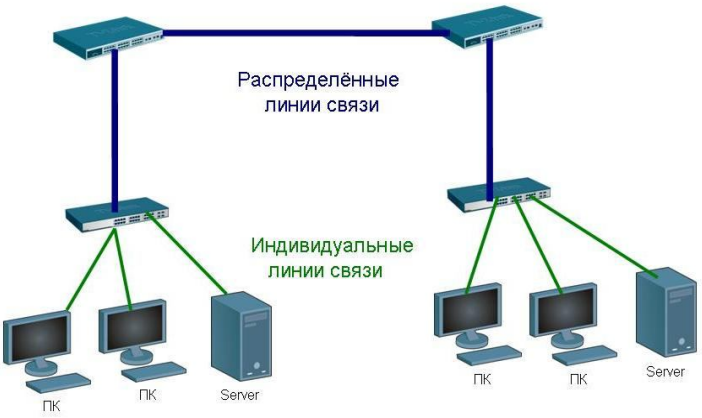


Рис. 12. Индивидуальные и распределённые линии связи в сетях на основе коммутаторов

1.3.2. Логическая топология сети передачи данных

Помимо физической топологии сети передачи данных, предполагается и **логическая топология сети**. Логическая топология определяет маршруты передачи данных в сети. Существуют такие конфигурации, в которых логическая топология отличается от физической. Например, сеть с физической топологией «звезда» может иметь логическую топологию «шина» – все зависит от того, каким образом устроен сетевой коммутатор или интернет-шлюз, маршрутизатор (VLAN, наличие VPN, и т.п.).

Чтобы определить логическую топологию сети, необходимо понять, как в ней принимаются сигналы:

- в логических шинных топологиях каждый сигнал принимается всеми устройствами;
- в логических кольцевых топологиях каждое устройство получает только те сигналы, которые были посланы конкретно ему.

Кроме того, важно знать, каким образом сетевые устройства получают доступ к среде передачи информации.

Разделение сети на логические сегменты

Кабельная система информационно вычислительной сети — самая «консервативная» часть информационной системы предприятия. Любое ее изменение сопряжено с существенными материальными затратами. Однако возможность переконфигурирования инфраструктуры часто может существенно повысить управляемость и надежность всей системы. Например, объединение портов управляемых по сети устройств (коммутаторы, аварийные источники питания и т. п.) в «физически обособленную» сеть существенно повышает уровень безопасности системы, исключая доступ к таким элементам с произвольных рабочих станций. Кроме того, выделение, например, компьютеров бухгалтерии в отдельную сеть исключает доступ к ним по сети всех остальных пользователей.

Подобная возможность изменения конфигурации сетевой конфигурации реализуется путем создания ***виртуальных сетей*** *(англ.* ***Virtual local area network, VLAN)****.*

VLAN представляет собой логически (программно) обособленный сегмент основной сети. Обмен данными происходит только в пределах одной VLAN. Сетевые устройства разных VLAN не видят друг друга. Самое главное, что из одной VLAN в другую не передаются широковещательные сообщения.

VLAN можно создать только на управляемых устройствах. Одна VLAN может объединять порты нескольких коммутаторов (VLAN с одинаковым номером на разных коммутаторах считаются одной и той же VLAN).

Варианты создания VLAN

На практике существует несколько технологий создания VLAN.

- В простейшем случае порт коммутатора приписывается к VLAN определенного номера (port based VLAN или группировка портов). При этом

одно физическое устройство логически разбивается на несколько: для каждой VLAN создается «отдельный» коммутатор. Очевидно, что число портов такого коммутатора можно легко изменить: достаточно добавить или исключить из VLAN соответствующий физический порт.

- Второй, часто используемый способ, заключается в отнесении устройства к той или иной VLAN на основе MAC-адреса. Например, так можно обособить камеры видео наблюдения, IP-телефоны и т.п. При переносе устройства из одной точки подключения в другую, оно останется в прежней VLAN, никакие параметры настройки менять не придется.
- Третий способ заключается в объединении устройств в сеть VLAN по сетевым протоколам. Например, можно «отделить» протокол IPX от IP, «поместить» их в разные VLAN и направить по различным путям.
- Четвертый способ создания VLAN состоит в многоадресной группировке.

VLAN открывают практически безграничные возможности для конфигурирования сетевой инфраструктуры, соответствующей требованиям конкретной организации. Один и тот же порт коммутатора может принадлежать одновременно нескольким виртуальным сетям, порты различных коммутаторов — быть включенными в одну VLAN и т. п. Обычно рекомендуется включать магистральные порты коммутаторов (порты, соединяющие коммутаторы) во все VLAN, существующие в системе. Это значительно облетает администрирование сетевой структуры, поскольку иначе в случае отказа какого-либо сегмента и последующего автоматического изменения маршрута придется анализировать все варианты передачи данных VLAN. Важно помнить, что ошибка в таком анализе, неправильный учет какого-либо фактора приведет к разрыву VLAN.

На Рис. 13 показан пример построения VLAN из компьютеров, подключенных к различным коммутаторам. Обратите внимание, что при использовании агрегированных каналов (на рисунке для связи устройств Switch 2 и Switch 3) в состав VLAN на каждом коммутаторе должны включаться именно агрегированные порты (обычно получают названия AL1, AL2 и т. д.).

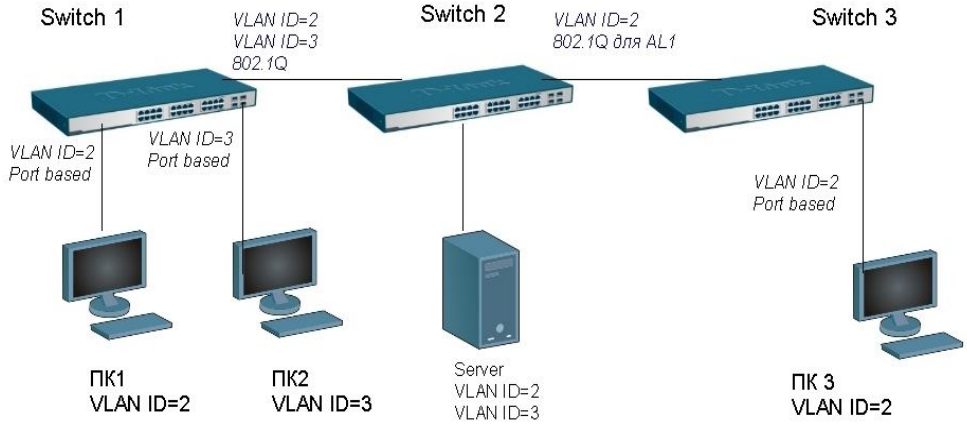


Рис. 13. Пример построения VLAN

Агрегация каналов (англ. Link aggregation, trunking) или IEEE 802.3ad – технология объединения нескольких физических каналов в один логический. Это способствует не только значительному увеличению пропускной способности магистральных каналов коммутатор-коммутатор или коммутатор-сервер, но и повышению их надежности.

Теги 802.1Q

В соответствии со стандартом IEEE 802.1Q номер VLAN передается в специальном поле кадра Ethernet, которое носит название TAG. Поэтому пакеты, содержащие такое поле, стали называть тегированными (*англ. tagged*), а пакеты без этого поля — не тегированными (*англ. untagged*). Поле TAG включает в себя данные QoS (поэтому все пакеты, содержащие информацию о качестве обслуживания, являются тегированными) и номер VLAN, на который отведено 12бит. Таким образом, максимально возможное число VLAN составляет 4096.

Сетевые адаптеры рабочих станций обычно не поддерживают теги, поэтому порты коммутаторов уровня доступа настраиваются в варианте не тегированными (untagged). Для того, чтобы через один порт можно было передать пакеты нескольких VLAN, он включается в соответствующие VLAN в режиме тегирования (обычно это магистральные порты или порты соединения двух коммутаторов). Коммутатор будет анализировать поля TAG принятых пакетов, и пересылать данные только в ту VLAN, номер которой содержится в поле. Таким образом, через один порт можно безопасно передавать информацию сразу для нескольких VLAN.

При соединениях «точка-точка» порты для одинаковых VLAN должны быть либо оба тегированными, либо оба не тегированными.

IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN.

Так как 802.1Q не изменяет заголовки кадра, то сетевые устройства, которые не поддерживают этот стандарт, могут передавать трафик без учёта его принадлежности к VLAN.

Рис. 14. Фрейм Ethernet с тегом 802.1Q

IEEE 802.1Q помещает внутрь фрейма тег, который передает информацию о принадлежности трафика к VLAN. Размер тега – 4 байта. Он состоит из таких полей:

Tag Protocol Identifier (TPID) - Идентификатор протокола тегирования. Размер поля — 16 бит. Указывает, какой протокол используется для тегирования. Для 802.1Q используется значение 0x8100.

Priority - приоритет. Размер поля — 3 бита. Используется стандартом IEEE 802.1p для задания приоритета передаваемого трафика.

Canonical Format Indicator (CFI) - Индикатор канонического формата. Размер поля - 1 бит. Указывает на формат MAC-адреса. 1 - канонический, 0 - не канонический.

VLAN Identifier (VID) - идентификатор VLAN. Размер поля – 12 бит. Указывает, к какому VLAN принадлежит фрейм. Диапазон возможных значений VID от 0 до 4095.

При использовании стандарта Ethernet II, 802.1Q вставляет тег перед полем «Тип протокола». Так как фрейм изменился, пересчитывается контрольная сумма.

VLAN 1

При создании VLAN следует учитывать тот факт, что служебная сетевая информация пересылается не тегированными пакетами. Для правильной работы сети администратору необходимо обеспечить передачу таких пакетов по всем направлениям. Самый простой способ настройки заключается в использовании VLAN по умолчанию (VLAN 1). Соответственно, все порты компьютеров необходимо включать в VLAN с другими номерами.

В VLAN 1 по умолчанию находятся интерфейсы управления коммутаторами, причем ранее выпускавшиеся модели коммутаторов не позволяют сменить номер для VLAN управления. Поэтому администратору следует тщательно продумать систему разбиения на VLAN, чтобы не допустить случайного доступа к управлению коммутаторами посторонних лиц, например, можно переместить все порты доступа коммутатора в другую VLAN, оставив для VLAN 1 только магистральный порт. Таким образом, пользователи не смогут подключиться к управлению коммутатором.

GVRP

Протокол GVRP предназначен для автоматического создания VLAN 802.1Q. С его помощью можно автоматически назначать порты во все вновь создаваемые VLAN. Несмотря на определенные удобства, такое решение является существенной брешью в системе обеспечения сетевой безопасности. Администратор должен представлять структуру VLAN и производить назначения портов ручными операциями.

1.3.3. Сетевые устройства локальных сетей в топологии

При построении любой информационно вычислительной сети нельзя обойтись без специальных сетевых устройств, разнообразных по своему предназначению и функциональным возможностям. Рассмотрим некоторые из них.

Одной из главных задач, которая стоит перед любой технологией транспортировки данных, является возможность их передачи на максимально большое расстояние. Физическая среда накладывает на этот процесс свои ограничения – рано или поздно мощность сигнала падает, и приём становится невозможным. Но ещё большее значение имеет то, что искажается «форма сигнала» – закономерность, в соответствии с которой мгновенное значение уровня сигнала изменяется во времени. Это происходит в результате того, что физическая среда, например металлические провода, по которым передаётся сигнал, имеют собственную ёмкость и индуктивность. Электрические и магнитные поля одного проводника наводят ЭДС в других проводниках (длинная линия).

В случае передачи данных решение было найдено в ограничении сегмента сети передачи данных и применением повторителей. При этом повторитель на входе должен принимать сигнал, далее распознавать его первоначальный вид, и генерировать на выходе его точную копию. Такая схема в теории может передавать данные на сколь угодно большие расстояния (если не учитывать особенности разделения физической среды в Ethernet).

Сегмент сети – логически или физически обособленная часть сети (подсеть).

Повторитель – предназначен для увеличения расстояния сетевого соединения путём повторения электрического сигнала «один в один». Бывают одно и много портовые повторители.

Первоначально в Ethernet использовался коаксиальный кабель с топологией «шина», и нужно было соединять между собой всего несколько сегментов. Для этого обычно использовались повторители (*англ. repeater*), имевшие два порта. Несколько позже появились многопортовые устройства, называемые **концентраторами** (*англ. concentrator*). Их физический смысл точно такой же, но восстановленный сигнал транслируется на все активные порты, кроме того, с которого пришёл сигнал.

С появлением протокола 10baseT во избежание терминологической путаницы **многопортовые повторители** для витой пары стали называться ***сетевыми концентраторами (хабами),*** а коаксиальные – ***повторителями (репитерами)***, по крайней мере, в русскоязычной литературе. Эти названия хорошо прижились и используются в настоящее время очень широко.

Термин концентратор (хаб) применим также к другим технологиям передачи данных: USB, FireWire и пр.

Мост, сетевой мост, бридж (жарг., калька с англ. bridge) — сетевое устройство, предназначенное для объединения сегментов (подсети) компьютерной сети разных топологий и архитектур.

Мосты «изучают» характер расположения сегментов сети путем построения адресных таблиц, в которых содержатся адреса всех сетевых устройств и сегментов, необходимых для получения доступа к данному устройству. Мост рассматривается как устройство с функциями хранения и дальнейшей отправки, поскольку он должен проанализировать поле адреса пункта назначения пакета данных и вычислить контрольную сумму CRC в поле контрольной последова-

тельности пакета данных перед отправкой его на все порты. Если порт пункта назначения в данный момент занят, то мост может временно сохранить фрейм до освобождения порта. Для выполнения этих операций требуется некоторое время, что замедляет процесс передачи и увеличивает латентность.

В настоящее время мосты практически не используются, за исключением ситуаций, когда связываются сегменты сети с разной организацией физического уровня, например, между xDSL соединениями, оптикой, Ethernet.

Сетевой коммутатор или свитч (жарг. от англ. switch - переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента сети (Рис. 15). В отличие от концентратора, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик всем узлам сети. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутаторы иногда рассматриваются как многопортовые мосты, поскольку были разработаны с использованием мостовых технологий. В случае SOHO-оборудования, режим прозрачной коммутации часто называют «мостовым режимом» (bridging).

Традиционно разделяют две категории коммутаторов: неуправляемые и управляемые. Однако компания D-Link предлагает еще одну, промежуточную категорию – **настраиваемые коммутаторы** (*smart switches*). Эти коммутаторы предназначены для использования на уровне доступа сетей малых и средних предприятий (*Small-to-Medium Business*, *SMB*).

Рис. 15 Коммутатор DES-1210-28.

Сетевой шлюз (англ. gateway) – аппаратный маршрутизатор или программное обеспечение для сопряжения компьютерных сетей, использующих разные протоколы (например, локальной и глобальной).

Сетевой шлюз конвертирует протоколы одного типа физической среды в протоколы другой физической среды (сети). Например, при соединении локального компьютера с сетью Интернет используется сетевой шлюз.

Сетевой шлюз – это точка сети, которая служит выходом в другую сеть. В сети Интернет узлом или конечной точкой может быть или сетевой шлюз, или хост. Интернет-пользователи и компьютеры, которые доставляют веб-страницы пользователям - это хосты, а узлы между различными сетями - это сетевые шлюзы.

Сетевой шлюз часто объединен с маршрутизатором, который управляет распределением и конвертацией пакетов в сети.

Маршрутизатор или роутер (от англ. router) - сетевое устройство, на основании информации о топологии сети и определённых правил принимающее решения о пересылке пакетов сетевого уровня между различными сегментами сети .

Роутеры (маршрутизаторы) являются одним из примеров аппаратных сетевых шлюзов (Рис. 16). Основная задача сетевого шлюза — конвертировать протокол между сетями. Роутер сам по себе принимает, проводит и отправляет пакеты только среди сетей, использующих одинаковые протоколы.

Рис. 16 Беспроводной маршрутизатор 802.11g DIR-320

Современные тенденции развития и построения информационно вычислительных сетей таковы, что применение беспроводных технологий стало повсеместным явлением. Беспроводные устройства создают сегменты (подсети) компьютерных сетей и имеют в своём составе различное по назначению оборудование. Особенно это характерно для сетевого оборудования класса SOHO.

Сетевые устройства этого класса часто совмещают в себе функции сетевого шлюза, маршрутизатора, беспроводной точки доступа, коммутатора, принт-сервера и др. В частности, беспроводной 802.11g интернет маршрутизатор DIR-320 позволяет создать проводную/беспроводную сеть в доме и (или) малом офисе.

В качестве примера применения вышеупомянутого сетевого оборудования, рассмотрим схему построения информационной вычислительной сети класса SOHO.

SOHO (от англ. **Small Office** / **Home Office** – малый/домашний офис) – название сегмента рынка электроники, предназначенного для домашнего использования. Как правило, характеризует устройства, не предназначенные для производственных нагрузок и довольно хорошо переживающие длительные периоды бездействия.

1.3.4. Пример построения простой информационно вычислительной сети

Простые информационно вычислительные сети класса SOHO, как правило, имеют топологию типа «звезда». Центральным устройством такой сети является интернет-шлюз, совмещающий в себе функции нескольких устройств.

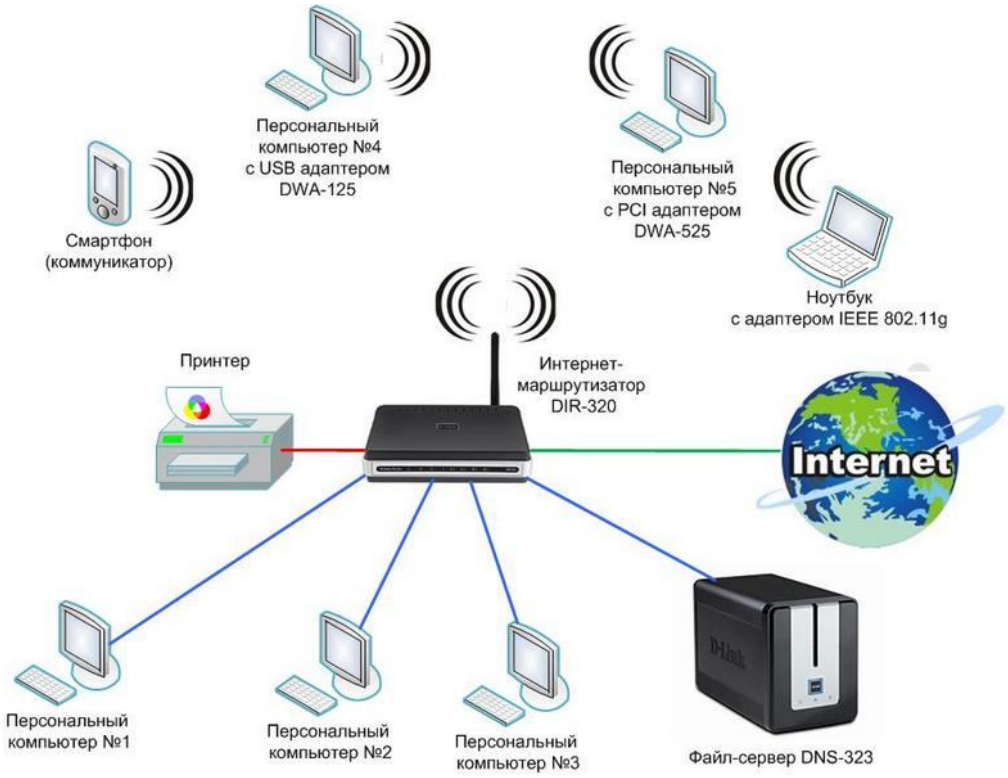


Рис. 17. Схема информационно вычислительной сети SOHO

В приведённой схеме (Рис. 17) центральным устройством является интернет-маршрутизатор **DIR-320**. Основное предназначение этого устройства – распределение услуги «доступ в Интернет» между пользователями информационно вычислительной сети класса SOHO.

Подключив DIR-320 к выделенной линии или широкополосному модему, пользователи могут совместно использовать высокоскоростное соединение с Интернет, подключившись к встроенному в устройство коммутатору или посредством беспроводной технологии 802.11g. Функция «Guest Zone» предоставляет второй «канал» беспроводного соединения и второй домен маршрутизации, что отделяет гостевую зону от главной сети для наилучшей защиты и управления.

Интернет маршрутизатор D-Link DIR-320 содержит порт USB для подключения USB-принтера, что позволяет пользователям совместно использовать принтер. Кроме того, встроенный 4-х портовый Ethernet-коммутатор позволяет подключать компьютеры, оснащенные Ethernet-адаптерами, игровые консоли и другие устройства к сети

DIR-320 оснащен встроенным межсетевым экраном, что защищает пользовательскую сеть от вредоносных атак. Это минимизирует угрозы от действий хакеров и предотвращает нежелательные вторжения в сеть. Дополнительные функции безопасности такие, как например, фильтр MAC-адресов, предотвращают неавторизованный доступ к сети. Функция «родительского контроля» позволяет запретить пользователям просмотр нежелательного контента. Также

беспроводной маршрутизатор 802.11g поддерживает стандарты шифрования WEP и WPS. Благодаря поддерживаемому функционалу маршрутизации и безопасности, беспроводной маршрутизатор D-Link DIR-320 позволяет создать беспроводную сеть для дома или офиса.

Кроме выше перечисленных возможностей, к USB порту DIR-320 возможно подключить EVDO/3G/WiMax модуль, тем самым получить резервный канал подключения к Интернет.

Сетевой дисковый массив **DNS-323** с 2 отсеками для жестких дисков SATA предоставляет пользователям возможность совместного использования документов, файлов, и цифровых медиафайлов в домашней или офисной сети. Благодаря встроенному FTP-серверу возможен удаленный доступ к файлам через Интернет. DNS-323 обеспечивает защиту данных, предоставляя доступ к файлам по локальной сети или через Интернет только определенным пользователям или группам пользователей с правом чтения или чтения/записи каталогов.

В DNS-323 доступны 4 различных режима работы с жесткими дисками (Standart, JBOD, RAID 0, RAID 1), позволяющих пользователям выбрать необходимую конфигурацию. В режиме Standart для использования доступны два отдельных жестких диска. Режим JBOD объединяет оба диска в один. Режим RAID 0 обеспечивает высокую производительность за счет разделения записи и чтения между двумя жесткими дисками. При использовании режима RAID 1 содержимое одного жесткого диска дублируется на другой, что обеспечивает максимальную надежность. Если один из жестких дисков выходит из строя, второй продолжает функционировать в полном объеме.

Функциональные возможности приведённой на рис.16 схемы информационно вычислительной сети можно расширить, включив в её состав устройства IPTV, IP-телефонии, видео наблюдения и т.п. Принципиально структура данной сети, от включения в её состав дополнительных сервисов, не изменится.

1.4. Вопросы для самопроверки

1. Каково соотношение между понятиями «сообщение» и «информация»?
2.

1.5. Упражнения

1. Переведите следующие числа из десятичной системы в двоичную: 3, 7, 15
2.

1.6. Исследовательские задания

1. Существует другой, так называемый энтропийный, подход к измерению количества информации. Выясните, какова технология измерения информации при этом подходе.

1.7. Список рекомендуемой литературы

1. *Олифер В.Г.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов / В.Г. Олифер, Н.А. Олифер. – Изд. 4-е.– СПб: Питер, 2007. – 960 с.
2. *Киселев С.В.* Основы сетевых технологий (1-е изд.) учеб. пособие / С.В. Киселев И.Л. Киселев. – Изд.: ИЦ Академия, 2008. – 208 с.
3. *Таненбаум Э.* Компьютерные сети. – СПб: Питер, 2007. – 992 с.
4. Базовые понятия сети (Перевод документации – Red Line Software) [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.redline-software.com/rus/support/docs/winproxy/user manual/ Net–work-basics.php
5. Основы сетевых технологий [Электронный ресурс]. – Электрон. дан. – http://znetwork.narod.ru/
6. Основы сетевых компьютерных технологий [Электронный ресурс]. – Электрон. дан. – http://academy.odoportal.ru/documents/akadem/bibl/ techno-logy/ base/6.1.html
7. Эволюция вычислительных систем [электронный ресурс]: sesia5.ru/lokseti/ s_11.htm
8. *Храмцов П. Б.* Администрирование сети и сервисов internet: Учебное пособие. – [Электронный ресурс]. – Электрон. дан. : http://citforum.ru/nets/ services/ index.shtml
9. Эволюция вычислительных систем [электронный ресурс]: http://sesia5.ru/lokseti/s_11.htm

2. Основы передачи данных

1.8. Основные определения

Информация – сведения о каких-либо процессах, событиях, фактах или предметах.

Известно, что 80-90% информации человек получает через органы зрения и 10-20% - через органы слуха. Другие органы чувств дают в сумме 1-2% информации. Физиологические возможности человека не позволяют обеспечить передачу больших объемов информации на значительные расстояния.

Связь - техническая база, обеспечивающая передачу и прием информации между удаленными друг от друга людьми или устройствами. Аналогия между связью и информацией такая же, как у транспорта и перевозимого груза. Средства связи не нужны, если нет информации, как не нужны транспортные средства при отсутствии груза.

Сообщение – форма выражения (представления) информации, удобная для передачи на расстояние. Различают оптические (телеграмма, письмо, фотография, видео и т.п.) и звуковые (речь, музыка) сообщения. Документальные сообщения наносятся и хранятся на определенных носителях, чаще всего на бумаге. Сообщения, предназначенные для обработки на компьютерах (ЭВМ), принято называть ***данными.***

Информационный параметр сообщения – параметр, в изменении которого «заложена» информация. Для звуковых сообщений информационным параметром является мгновенное значение звукового давления, для неподвижных изображений - коэффициент отражения, для подвижных - яркость свечения участков экрана. По характеру изменения информационных параметров различают ***непрерывные и дискретные сообщения***.

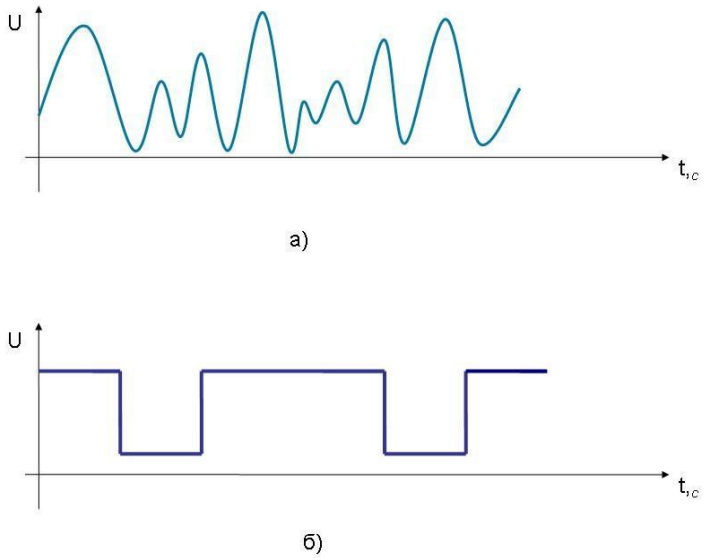


Рис. 18. Виды сигналов: а - аналогового, б – дискретного

Сигнал - физический процесс, отображающий передаваемое сообщение. Отображение сообщения обеспечивается изменением какой-либо физической величины, характеризующей процесс. Эта величина является ***информационным параметром сигнала***. Сигналы, как и сообщения, могут быть ***непрерывными и дискретными***. Информационный параметр непрерывного сигнала с течением времени может принимать любые мгновенные значения в определенных пределах. Непрерывный сигнал часто называют ***аналоговым***. Дискретный сигнал характеризуется конечным числом значений информационного параметра. Часто этот параметр принимает всего два значения. На Рис. 17 показаны виды аналогового и дискретного сигналов.

В дальнейшем будем рассматривать принципы и средства связи, основанные на использовании электрической энергии в качестве переносчиков сообщений, т.е. электрических сигналов. Выбор электрических сигналов для переноса сообщений на расстояние обусловлен их высокой скоростью распространения (около 300 000 км/с).

1.9. Параметры первичных сигналов

Описание сигналов электросвязи некоторым образом необходимо для их адекватной обработки в процессе передачи. Описанием сигнала может служить некоторая функция времени. Определив так или иначе данную функцию, определяем и сигнал. Однако такое полное определение сигнала не всегда требуется. Достаточно описание в виде нескольких параметров, характеризующих основные свойства сигнала с точки зрения его передачи.

Если провести аналогию с транспортированием грузов, то для транспортной сети определяющими параметрами груза являются его масса и габариты. Сигнал также является объектом транспортирования, а техника связи - техникой транспортирования (передачи) сигналов по каналам связи.

Основными ***первичными сигналами электросвязи*** являются: телефонный, звукового вещания, факсимильный, телевизионный, телеграфный, передачи данных.

Телефонный (речевой) сигнал. Звуки речи образуются в результате прохождения воздушного потока из легких через голосовые связки и полости рта и носа. Частота импульсов основного тона (f0 *Рис*.18) лежит в пределах от 50..80 Гц (бас) до 200..250 Гц (женский и детский голоса). Импульсы основного тона содержат большое число гармоник (до 40) (2f0,..,nf0 на *Рис*. 18), причем их амплитуды убывают с увеличением частоты со скоростью приблизительно 12 дБ на октаву (кривая 1 на *Рис*. 18). (Напомним, что октавой называется диапазон частот, верхняя частота которого в два раза выше нижней. Т.о. амплитуда гармоники 2f0 на 12 дБ больше, чем гармоники 4f0 и т.д.). При разговоре частота основного тона f0 меняется в значительных пределах.

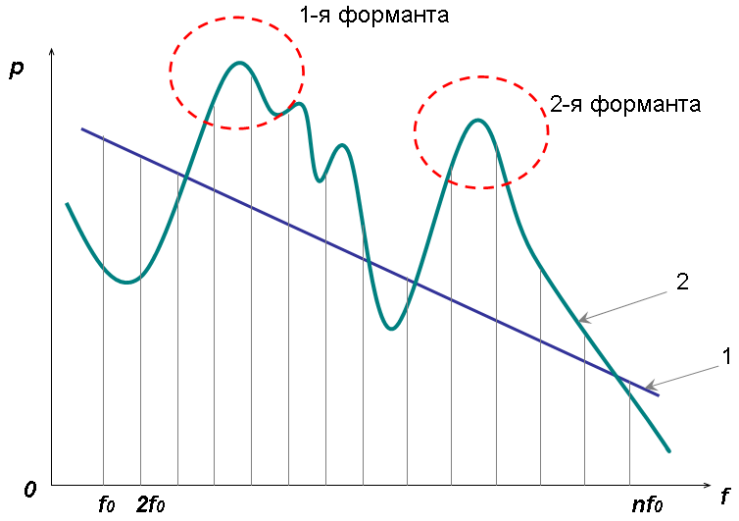


Рис. 19. Спектральный состав речевого сигнала

В процессе прохождения воздушного потока из легких через голосовые связки и полости рта и носа образуются звуки речи, причем мощность гармоник частоты основного тона меняется (кривая 2 на Рис.18). Области повышенной мощности гармоник частоты основного тона называются формантами. Различные звуки речи содержат от двух до четырех формант. Высокое качество передачи телефонного сигнала характеризуется уровнем громкости, разборчивостью, естественным звучанием голоса, низким уровнем помех. Эти факторы определяют требования к телефонным каналам.

Основными параметрами телефонного сигнала являются:

- мощность телефонного сигнала
- коэффициент активности телефонного сообщения, т.е. отношение времени, в течение которого мощность сигнала на выходе канала превышает заданное пороговое значение, к общему времени занятия канала для разговора.
- динамический диапазон определяется выраженным в децибелах отношением максимальной и минимальной мощности сигнала
- пик-фактор сигнала

Сигналы звукового вещания. Источником звука при передаче программ вещания обычно являются музыкальные инструменты или голос человека. Динамический диапазон вещательной передачи следующий: речь диктора 25..35 дБ, художественное чтение 40..50 дБ, вокальные и инструментальные ансамбли 45..55 дБ, симфонический оркестр до 65 дБ. При определении динамического диапазона максимальным считается уровень, вероятность превышения которого равна 2%, а минимальным - 98%. Средняя мощность сигнала вещания существенно зависит от интервала усреднения. В точке с нулевым измерительным уровнем средняя мощность составляет 923 мкВт при усреднении за час, 2230 мкВт - за минуту и 4500 мкВт - за секунду. Максимальная мощность сигнала вещания в точке с нулевым измерительным уровнем составляет 8000 мкВт.

Частотный спектр сигнала вещания расположен в полосе частот 15..20000 Гц. При передаче, как телефонного сигнала, так и сигналов вещания полоса, частот ограничивается. Для достаточно высокого качества (каналы вещания первого класса) эффективная полоса частот должна составлять 0,05..10 кГц, для безукоризненного воспроизведения программ (каналы высшего класса) 0,03...15 кГц.

Факсимильный сигнал формируется методом построчной развертки. Частотный спектр первичного факсимильного сигнала определяется характером передаваемого изображения, скоростью развертки и размерами сканирующего пятна. Для параметров факсимильных аппаратов, рекомендованных МСЭ-Т, верхняя частота сигнала может составлять 732, 1100 и 1465 Гц. Динамический диапазон сигнала составляет около 25 дБ, пик-фактор равен 4,5 дБ при 16 градациях яркости.

Телевизионный сигнал также формируется методом развертки. Анализ показывает, что энергетический спектр телевизионного сигнала сосредоточен в полосе частот 0..6 МГц. Динамический диапазон DC 40 дБ, пик-фактор 4,8 дБ.

Основным параметром ***дискретного сигнала*** с точки зрения его передачи является требуемая скорость передачи (бит/с).

Аналогичные параметры определяются и для каналов связи. Параметры каналов связи должны быть не меньше соответствующих параметров сигналов.

Свести параметры аналоговых сигналов к единому параметру (скорости передачи) позволяет преобразование этих сигналов в цифровые.

Система электросвязи - совокупность технических средств и среды распространения, обеспечивающая передачу сообщений. Обобщенная структурная схема систем электросвязи показана на Рис. 19

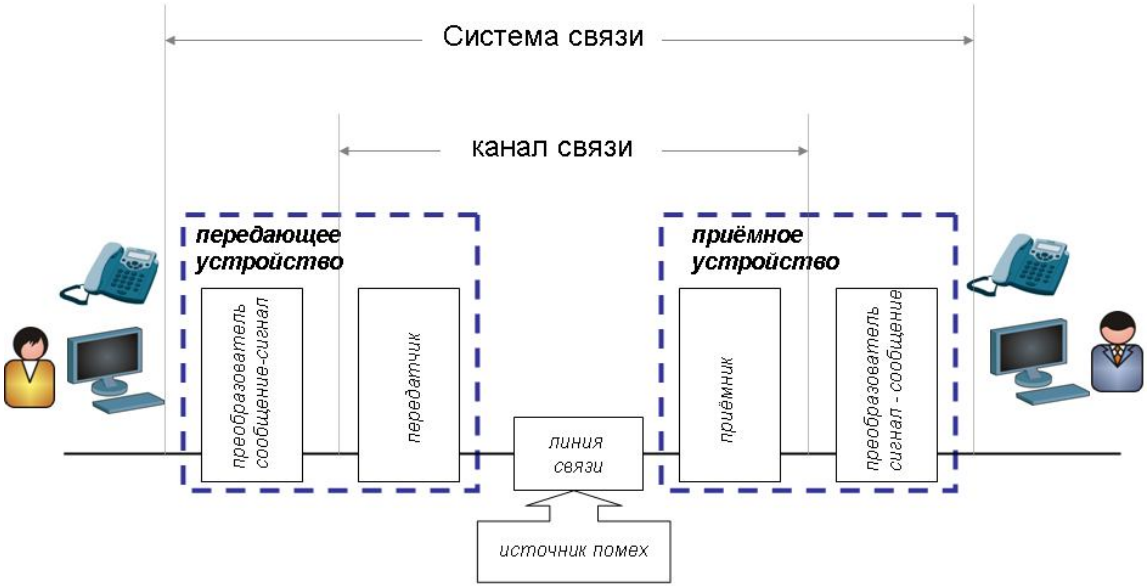


Рис. 20 Обобщенная структурная схема систем электросвязи

Сообщение при помощи преобразователя сообщение-сигнал преобразуется в первичный электрический сигнал. Первичные сигналы не всегда удобно (а иногда невозможно) непосредственно передавать по линии связи. Поэтому ***первичные сигналы*** при помощи передатчика преобразуются в так называемые ***вторичные сигналы***, характеристики которых хорошо согласуются с характеристиками линии связи.

Канал связи - совокупность технических устройств и среды распространения, обеспечивающих передачу сигналов на расстояние.

Каналы и системы связи, использующие искусственную среду распространения (металлические провода, оптическое волокно), называются ***проводными,*** а каналы и системы связи, в которых сигналы передаются через открытое пространство - ***радиоканалами и радиосистемами.***

Сеть связи - совокупность технических средств, обеспечивающих передачу и распределение сообщений. Принципы построения сетей связи зависят от вида передаваемых и распределяемых сообщений.

Уровнем передачи сигнала в некоторой точке канала или тракта называют логарифмическое преобразование отношения энергетического параметра S (мощности, напряжения или тока) к отсчетному значению этого же параметра. Уровни передачи измеряются в децибелах, если справедливы соотношения:

- для уровней по мощности Pm=10lgP\Po, дБм;
- для уровней по напряжению Pu=20lgP\Po, дБн;

Уровень передачи называется **абсолютным**, если P0=1 мВт.

Для обеспечения передачи индивидуальных сообщений необходимо связать (соединить) оконечные аппараты абонентов. Электрическая цепь (канал), состоящая из нескольких участков и обеспечивающая передачу сигналов между абонентами, называется ***соединительным трактом.***

Процесс поиска и соединения электрических цепей называется ***коммутацией каналов***. Сеть, обеспечивающая коммутацию каналов, называется **сетью с коммутацией каналов**. Узловые станции в такой сети называются ***станциями коммутации***.

При передаче документальных сообщений (передачи данных) кроме организации связи с коммутацией каналов, возможно, осуществлять *поэтапную передачу* сообщения от узла к узлу. Такой способ передачи получил название ***коммутации сообщений***. Соответственно сеть, обеспечивающая коммутацию сообщений, называется ***сетью с коммутацией сообщений.***

Разновидностью такой сети является ***сеть с коммутацией пакетов.*** В этом случае полученное от передающего абонента сообщение разбивается на блоки (пакеты) фиксированной длины. Пакеты передаются по сети (необязательно по одному и тому же маршруту) и объединяются в сообщение перед выдачей принимающему абоненту. Узловые станции таких сетей называются ***центрами коммутации сообщений*** и ***пакетов*** соответственно.

В историческом плане все виды электросвязи длительный период развивались независимо друг от друга, в результате чего сформировались несколько независимых сетей. Вместе с тем, сети общего пользования (Министерства связи) не справлялись с требуемыми объемами передачи сообщений, требуемых для нормального экономического развития страны, и поэтому ряд министерств и ведомств стали создавать свои сети для удовлетворения собственных нужд. Такая техническая политика привела к еще большему разобщению технических средств, а эффективность совокупности сетей в масштабах страны оставалась низкой. Уже в начале 60-х годов стало ясно, что перспективным направлением развития связи должно стать объединение сетей.

Предпосылки для объединения сетей: унификация методов преобразования, необходимость передачи сигналов в совпадающих направлениях, сходство функций систем передачи и коммутации. В 70-х годах было принято решение о создании ***Единой автоматизированной сети связи*** Союза ССР. Работа по созданию единой сети не была завершена и прекратилась в связи с развалом СССР. В настоящее время этот проект, отражая изменение геополитической ситуации и новые революционные достижения в области связи, носит название ***Взаимоувязанная сеть связи России.***

Взаимоувязанная сеть связи (ВСС) - это совокупность технически сопряженных сетей электросвязи общего пользования, ведомственных и других сетей электросвязи на территории России независимо от ведомственной принадлежности и форм собственности, обеспеченная общим централизованным управлением.

Основными требованиями к взаимоувязанной сети связи являются надежность и экономичность. Определенные технические средства ВСС участвуют в процессе передачи *не зависимо от вида* передаваемых сообщений. Совокупность этих элементов образует ***первичную сеть (ПС) ВСС***. В состав первичной сети входят сетевые узлы, сетевые станции и линии передачи.

Структура первичной сети учитывает административное деление страны. Территория страны поделена на *зоны*. Признак зоны - единая 7-значная нумерация. Как правило, зоны совпадают с территориями областей. В соответствии с этим делением ПС состоит из отдельных частей:

- местные первичной сети - ограничены территорией города или сельского района;
- внутризоновые первичной сети - охватывают территорию зоны и обеспечивают соединение местных сетей внутри зоны;
- магистральные первичной сети - соединяют зоновые сети.

Каждая сеть связи, входящая в ВСС, помимо технических средств первичной сети использует устройства, присущие этой сети.

Вторичная сеть (ВС) взаимоувязанной сети связи - совокупность технических средств, обеспечивающих передачу сообщений определенного вида. В состав ВС входят: оконечные абонентские устройства, абонентские линии, коммутационные устройства и каналы, выделенные из первичной сети для организации данной вторичной сети.

1.10. Линии и каналы связи

Существующие типы линий связи в зависимости от используемой среды распространения сигналов принято делить на проводные и линии в атмосфере (радиолинии).

К линиям связи предъявляются следующие основные требования:

- осуществление связи на практически требуемые расстояния;
- широкополосность и пригодность для передачи различных видов сообщений;

- защищенность цепей от взаимных влияний и внешних помех, а также от физических воздействий (атмосферных явлений, коррозии и пр.);
- стабильность параметров линии, устойчивость и надежность связи;
- экономичность системы связи в целом.

Проводные линии связи на основе металлических проводников

В простейшем случае проводная линия связи - физическая цепь, образуемая парой металлических проводников.

К основным характеристикам линий связи относятся:

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

В первую очередь разработчиков вычислительной сети интересуют ***пропускная способность и достоверность передачи данных*****,** поскольку эти характеристики прямо влияют на производительность и надежность создаваемой сети. Пропускная способность и достоверность - это характеристики, как линии связи, так и способа передачи данных. Поэтому если способ передачи (протокол) уже определен, то известны и эти характеристики. Например, пропускная способность цифровой линии всегда известна, так как на ней определен протокол физического уровня, который задает битовую скорость передачи данных - 64 Кбит/с, 2 Мбит/с и т. п.

Однако нельзя говорить о пропускной способности линии связи, до того как для нее определен ***протокол физического уровня***. Именно в таких случаях, когда только предстоит определить, какой из множества существующих протоколов можно использовать на данной линии, очень важными являются остальные характеристики линии, такие как полоса пропускания, перекрестные наводки, помехоустойчивость и другие характеристики.

Кабельные линии связи (кабели связи) образованы проводами с изоляционными покрытиями, помещенными в защитные оболочки. По конструкции и взаимному расположению проводников различают симметричные и коаксиальные кабели связи.

Симметричная цепь состоит из двух совершенно одинаковых в электрическом и конструктивном отношениях изолированных проводников. В зарубежных источниках симметричные кабели часто называют **«витая пара»** (TP - twisted pair). Различают **экранированные (shielded) и неэкранированные (unshielded)** симметричные кабели**.**

Коаксиальная цепь представляет собой два цилиндра с совмещенной осью, причем один цилиндр - сплошной внутренний проводник, концентри-

Рассмотрим основные параметры кабелей с металлическими проводниками.

Коэффициент затухания α, дБ/км. Зависит от свойств материалов проводников и изоляционного материала. Наилучшими свойствами (малым сопротивлением) обладают медь и серебро. Коэффициент затухания зависит также от геометрических размеров проводников. Симметричный кабель с большими диаметрами проводников обладают меньшим коэффициентом затухания.

Очень важной характеристикой, фактически определяющей широкополосность системы связи, является *зависимость коэффициента затухания от частоты*. Если определен граничный коэффициент затухания $\alpha_{ГР}$ (обычно он определяется возможностями усилителей или регенераторов), то данному коэффициенту соответствует граничная частота пропускания системы $f_{ГР}$. Полоса пропускания системы не превышает граничной частоты пропускания.

Скорость распространения v, км/мс. С ростом частоты скорость распространения увеличивается, приближаясь к скорости света в вакууме $v_C \approx 300$ км/мс. Данный параметр зависит также от свойств диэлектрика, применяемого в кабеле.

Волновое сопротивление (импеданс) $Z_В$ (Ом) - сопротивление, которое встречает электромагнитная волна при распространении вдоль однородной линии без отражения, т.е. при условии, что на процесс передачи не влияют несогласованности на концах линии. Волновое сопротивление симметричного кабеля зависит от удельных значений емкости и индуктивности кабеля. Для коаксиа-

ального кабеля волновое сопротивление определяется как $Z_B = \frac{1}{2\pi} Z_Д \ln \frac{D}{d}$, где Zд - волновое сопротивление диэлектрика, D и d - соответственно диаметры внешнего и внутреннего проводников.

Основные требования к симметричному кабелю определены в рекомендации МСЭ-Т G.613. Диаметр жилы СК обычно составляет 0.4...1.2 мм. СК обычно используются в диапазоне частот до 10 МГц.

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.

Емкость - это свойство металлических проводников накапливать энергию. Два электрических проводника в кабеле, разделенные диэлектриком, представляют собой конденсатор, способный накапливать заряд. Емкость является нежелательной величиной, поэтому следует стремиться к тому, чтобы она была как можно меньше (иногда применяют термин «паразитная емкость»). Высокое значение емкости в кабеле приводит к искажению сигнала и ограничивает полосу пропускания линии.

Уровень внешнего электромагнитного излучения или *электрический шум*. Электрический шум - это нежелательное переменное напряжение в проводнике. Электрический шум бывает двух типов: фоновый и импульсный. Электрический шум можно также разделить на низко-, средне- и высокочастотный. Источниками фонового электрического шума в диапазоне до 150 кГц являются линии электропередачи, телефоны и лампы дневного света; в диапазоне от 150 кГц до 20 МГц - компьютеры, принтеры, ксероксы; в диапазоне от 20 МГц до 1 ГГц - телевизионные и радиопередатчики, микроволновые печи. Основными источниками импульсного электрического шума являются моторы, переключатели и сварочные агрегаты. Электрический шум измеряется в милливольтах.

Помимо универсальных характеристик, таких, например, как затухание, которые применимы для всех типов кабелей, существуют характеристики, которые применимы только к определенному типу кабеля. Например, параметр шаг скрутки проводов используется только для характеристики витой пары, а параметр NEXT применим только к многопарным кабелям на основе витой пары.

Воздушные линии связи

Воздушные линии связи не имеют изолирующего покрытия между проводниками, роль изолятора играет слой воздуха. Проводники выполняются, в основном, из биметаллической сталемедной (сталеалюминевой) проволоки. Внутренний диаметр стальной проволоки обычно составляет 1.2...4 мм, толщи-

на внешнего слоя меди (алюминия) - 0.04...0.2 мм. Проволока подвешивается на деревянных или железобетонных опорах с помощью фарфоровых изоляторов. Используемый частотный диапазон ВЛС не превышает 150 кГц.

Цепи линий связи постоянно находятся под воздействием сторонних электромагнитных полей различного происхождения. Различают две основные группы источников сторонних полей ***(помех):***

- *внутренние* - соседние физические и искусственные цепи данной линии связи;
- *внешние* - энергетически и конструктивно не связанные с линией связи.

Внешние источники помех в свою очередь по своему происхождению делятся на:

- *естественные* - грозовые разряды, солнечная радиация и пр.;
- *созданные человеком* - высоковольтные линии передачи, радиостанции, линии электрифицированных железных дорог, электрические сети промышленных предприятий и отдельные энергоемкие устройства.

Сторонние электромагнитные поля индуцируют в цепях линий связи помехи, которые не только снижают качество передачи, но иногда возбуждают большие напряжения и токи, приводящие к разрушению линий связи и аппаратуры. Указанные воздействия называют ***электромагнитными влияниями на цепи*** линий связи.

Данная проблема является общей для всех систем и устройств телекоммуникаций и называется ***проблемой электромагнитной совместимости.*** Сущность ее состоит в том, что в процессе проектирования, строительства и эксплуатации телекоммуникационных устройств и систем необходимо учитывать два противоречивых требования:

- необходимо обеспечить достаточную для нормальной работы телекоммуникационных систем защиту от воздействия на них сторонних электромагнитных полей;
- необходимо ограничить допустимыми значениями уровни влияния электромагнитных полей проектируемых устройств и систем на другие устройства.

В настоящее время проводные линии связи широко используются при построении локальных вычислительных сетей (более подробно рассмотрим далее). Данные линии связи стандартизированы и обычно называются структури-

рованной кабельной системой. Известны кабельные системы категорий 3, 4, 5 стандартов EIA/TIA-568, TSB-36, TSB-40 специального подкомитета TR41.8.1.

Базовыми стандартами структурированных кабельных систем являются: ANSI/TIA/EIA-568-A. Стандарт телекоммуникационных кабельных систем коммерческих зданий. Октябрь 1995 года; ISO/IEC 11801. Информационные технологии. Структурированная кабельная система для помещений заказчиков. Июль 1995 года; EN 50173:1995. Информационные технологии. Структурированные кабельные системы. Июль 1995 года.

Волоконно-оптические линии связи

Волоконно-оптические линии связи (ВОЛС) имеют ряд существенных преимуществ по сравнению с линиями связи на основе металлических кабелей. К ним относятся: большая пропускная способность, малое затухание, малые масса и габариты, высокая помехозащищенность, надежная техника безопасности, практически отсутствующие взаимные влияния, малая стоимость из-за отсутствия в конструкции цветных металлов.

В ВОЛС применяют электромагнитные волны оптического диапазона. Напомним, что видимое оптическое излучение лежит в диапазоне длин волн 380...760 нм. Практическое применение в ВОЛС получил *инфракрасный* диапазон, т.е. излучение с длиной волны более 760 нм.

В оптическом волноводе может одновременно существовать несколько типов волн (***мод***). В зависимости от модовых характеристик оптическое волокно со ступенчатым профилем преломления делятся на два вида: ***многомодовые и одномодовые.***

Радиолинии связи

В радиолиниях связи средой распространения электромагнитных волн в подавляющем большинстве случаев (за исключением случая связи между космическими аппаратами) является атмосфера Земли. Строение атмосферы сложно и условно разделяется на тропосферу, стратосферу и ионосферу. Высота слоев приблизительна и различна для разных географических точек Земли. В тропосфере сосредоточено около 80% массы атмосферы и около 20% - в стратосфере. Плотность атмосферы в ионосфере крайне мала, граница между ионосферой и космическим пространством является условным понятием, так как следы атмосферы встречаются даже на высотах более 400 км. Считается, что плотные слои атмосферы заканчиваются на высоте около 120 км.

Линия радиосвязи может состоять из двух оконечных станций. Типичным примером таких радиолиний являются линии сетей передачи сообщений массового характера (сети телевизионного и радиовещания). Радиолиния может содержать несколько промежуточных переприёмных станций. Так строятся линии ***радиорелейных систем*** передачи.

Радиоволны, излучаемые передающей антенной, прежде чем попасть в приемную антенну, проходят в общем случае сложный путь. На величину напряженности поля в точке приема оказывает влияние множество факторов. Основные из них:

- отражение электромагнитных волн от поверхности Земли;
- преломление (отражение) в ионизированных слоях атмосферы (ионосфере);
- рассеяние на диэлектрических неоднородностях нижних слоев атмосферы (тропосфере);
- дифракция на сферической выпуклости Земли;

Напряжённость электрического поля— векторная физическая величина, характеризующая электрическое поле в данной точке и численно равная отношению силы F действующей на пробный заряд, помещенный в данную точку поля, к величине этого заряда q: **E=F\q**

Модуль напряжённости электрического поля в СИ измеряется в В/м (Вольт на метр).

Также напряженность поля в точке приема зависит от типа применяемых антенн, неоднородностей в атмосфере, от длины волны, освещенности земной атмосферы Солнцем и ряда других факторов.

1.11. Основные характеристики линий и каналов связи

Линия связи искажает передаваемые сигналы из-за того, что ее физические параметры отличаются от идеальных. Так, например, медные провода всегда представляют собой некоторую распределенную по длине комбинацию активного сопротивления, емкостной и индуктивной нагрузки. В результате для синусоид различных частот линия связи будет обладать различным полным сопротивлением, а значит, и передаваться они будут по-разному. Волоконно-оптический кабель также имеет отклонения, мешающие идеальному распро-

странению света. Если линия связи включает промежуточную аппаратуру, то она также может вносить дополнительные искажения, так как невозможно создать устройства, которые бы одинаково хорошо передавали весь спектр синусоид, от нуля до бесконечности.

Степень искажения синусоидальных (аналоговых) сигналов линиями связи оценивается с помощью таких характеристик, как ***амплитудно-частотная характеристика***, ***полоса пропускания и затухание на определенной частоте.***

Амплитудно-частотная характеристика (АЧХ)— функция, показывающая зависимость модуля некоторой комплекснозначной функции от частоты. Чаще всего означает модуль комплексного коэффициента передачи линейного четырёхполюсника. Также может рассматриваться АЧХ других комплекснозначных функций частоты, например, спектральной плотности мощности сигнала АЧХ в теории линейных стационарных систем означает зависимость модуля передаточной функции системы от частоты. АЧХ показывает, во сколько раз амплитуда сигнала на выходе системы отличается от амплитуды входного сигнала на всём диапазоне частот.

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

Несмотря на полноту информации, предоставляемой амплитудно-частотной характеристикой о линии связи, ее использование осложняется тем обстоятельством, что получить ее весьма трудно. Ведь для этого нужно провести тестирование линии эталонными синусоидами по всему диапазону частот от нуля до некоторого максимального значения, которое может встретиться во входных сигналах. Причем менять частоту входных синусоид нужно с небольшим шагом, а значит, количество экспериментов должно быть очень большим. Поэтому на практике вместо амплитудно-частотной характеристики применяются другие, упрощенные характеристики — ***затухание и полоса пропускания.***

Затухание линий связи

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

тудно-частотной характеристики линии. Часто при эксплуатации линии заранее известна основная частота передаваемого сигнала, то есть та частота, гармоника которой имеет наибольшую амплитуду и мощность. Поэтому достаточно знать затухание на этой частоте, чтобы приблизительно оценить искажения передаваемых по линии сигналов. Более точные оценки возможны при знании затухания на нескольких частотах, соответствующих нескольким основным гармоникам передаваемого сигнала.

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

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

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

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

Например, кабель на витой паре категории 5 характеризуется затуханием не ниже -23,6 дБ для частоты 100 МГц при длине кабеля 100 м. Частота 100 МГц выбрана потому, что кабель этой категории предназначен для высокоскоростной передачи данных, сигналы которых имеют значимые гармоники с частотой примерно 100 МГц. Кабель категории 3 предназначен для низкоскоростной передачи данных, поэтому для него определяется затухание на частоте 10 МГц (не ниже -11,5 дБ). Часто оперируют с абсолютными значениями затухания, без указания знака.

Абсолютный уровень мощности, например, уровень мощности передатчика, также измеряется в децибелах. При этом в качестве базового значения мощности сигнала, относительно которого измеряется текущая мощность, принимается значение в 1 мВт. Таким образом, уровень мощности р вычисляется по следующей формуле:

$$p = 10 \log_{10} P/1мВт \ [дБм],$$

где Р - мощность сигнала в милливаттах, а дБм (dBm) - это единица измерения уровня мощности (децибел на 1 мВт).

Полоса пропускания

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

ределяет диапазон частот синусоидального сигнала, при которых этот сигнал передается по линии связи без значительных искажений. Знание полосы пропускания позволяет получить с некоторой степенью приближения тот же результат, что и знание амплитудно-частотной характеристики. Пропускная способность линии связи зависит не только от ее характеристик, таких как амплитудно-частотная характеристика, но и от спектра передаваемых сигналов.

Таким образом, амплитудно-частотная характеристика, полоса пропускания и затухание являются универсальными характеристиками, и их знание позволяет сделать вывод о том, как через линию связи будут передаваться сигналы любой формы. Полоса пропускания зависит от типа линии и ее протяженности.

Пропускная способность

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

Пропускная способность линий связи и коммуникационного сетевого оборудования традиционно измеряется в битах в секунду, а не в байтах в секунду. Это связано с тем, что данные в сетях передаются последовательно, то есть **побитно**, а не параллельно, **байтами**, как это происходит между устройствами внутри компьютера. Такие единицы измерения, как килобит, мегабит или гигабит, в сетевых технологиях строго соответствуют степеням (то есть килобит - это 1000 бит, а мегабит - это 1 000 000 бит), а не близким к этим числам степеням 2, как это принято в программировании, где приставка «кило» равна 2^{10} =1024, а «мега» - 2^{20} = 1 048576.

Сигналы передачи данных обычно имеют вид последовательностей двуполярных или однополярных прямоугольных импульсов. Сигналы такой формы называются ***двоичными***. Длительность импульсов τ_u определяется скоростью передачи В, измеряемой в бит/сек (число символов в секунду) Вводится понятие ***тактовая частота*** $Fm= 1/\tau_u$, которая численно равна скорости передачи.

Выбор способа представления дискретной информации в виде сигналов, подаваемых на линию связи, называется ***физическим*** или ***линейным кодированием***. От выбранного способа кодирования зависит спектр сигналов и, соответственно, пропускная способность линии. Таким образом, для одного способа

кодирования линия может обладать одной пропускной способностью, а для другого - другой. Например, витая пара категории 3 может передавать данные с пропускной способностью 10 Мбит/с при способе кодирования стандарта физического уровня l0Base-T и 33 Мбит/с при способе кодирования стандарта 100Base-T4.

Большинство способов кодирования используют изменение какого-либо параметра периодического сигнала - частоты, амплитуды и фазы синусоиды или же знак потенциала последовательности импульсов. Периодический сигнал, параметры которого изменяются, называют ***несущим сигналом*** **или** ***несущей частотой***, если в качестве такого сигнала используется синусоида.

Если сигнал изменяется так, что можно различить только два его состояния, то любое его изменение будет соответствовать наименьшей единице информации - ***биту.*** Если же сигнал может иметь более двух различимых состояний, то любое его изменение будет нести несколько бит информации.

Количество изменений информационного параметра несущего периодического сигнала в секунду измеряется в ***бодах (baud)***. Период времени между соседними изменениями информационного сигнала называется ***тактом работы передатчика***.

Пропускная способность линии в битах в секунду в общем случае не совпадает с числом бод. Она может быть как выше, так и ниже числа бод, и это соотношение зависит от способа кодирования. Если сигнал имеет более двух различимых состояний, то пропускная способность в битах в секунду будет выше, чем число бод. Например, если информационными параметрами являются фаза и амплитуда синусоиды, причем различаются 4 состояния фазы в 0,90,180 и 270 градусов и два значения амплитуды сигнала, то информационный сигнал может иметь 8 различимых состояний. В этом случае модем, работающий со скоростью 2400 бод (с тактовой частотой 2400 Гц) передает информацию со скоростью 7200 бит/с, так как при одном изменении сигнала передается 3 бита информации.

При использовании сигналов с двумя различимыми состояниями может наблюдаться обратная картина. Это часто происходит потому, что для надежного распознавания приемником пользовательской информации каждый бит в последовательности кодируется с помощью нескольких изменений информационного параметра несущего сигнала. Например, при кодировании единичного значения бита импульсом положительной полярности, а нулевого значения бита - импульсом отрицательной полярности физический сигнал дважды изменяет свое состояние при передаче каждого бита. При таком кодировании пропускная способность линии в два раза ниже, чем число бод, передаваемое по линии.

На пропускную способность линии оказывает влияние не только физическое, но и *логическое кодирование.* ***Логическое кодирование*** выполняется до физического кодирования и подразумевает замену бит исходной информации новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных. Сопровождение ка-

ждого *байта* исходной информации одним ***битом четности*** - это пример очень часто применяемого способа логического кодирования при передаче данных с помощью модемов.

Другим примером логического кодирования может служить шифрация данных, обеспечивающая их конфиденциальность при передаче через общественные каналы связи. При логическом кодировании чаще всего исходная последовательность бит заменяется более длинной последовательностью, поэтому пропускная способность канала по отношению к полезной информации при этом уменьшается.

Байт (англ. byte)— единица хранения и обработки цифровой информации. Чаще всего байт считается равным восьми битам, в этом случае он может принимать одно из 256 различных значений. Для того чтобы подчеркнуть, что имеется в виду восьмибитный байт, в описании сетевых протоколов используется термин **«октет»** (лат.octet).

Чем выше частота несущего периодического сигнала, тем больше информации в единицу времени передается по линии и тем выше пропускная способность линии при фиксированном способе физического кодирования. Однако, с другой стороны, с увеличением частоты периодического несущего сигнала увеличивается и ширина спектра этого сигнала, то есть разность между максимальной и минимальной частотами того набора синусоид, которые в сумме дадут выбранную для физического кодирования последовательность сигналов. Линия передает этот спектр синусоид с теми искажениями, которые определяются ее полосой пропускания. Чем больше несоответствие между полосой пропускания линии и шириной спектра передаваемых информационных сигналов, тем больше сигналы искажаются и тем вероятнее ошибки в распознавании информации принимающей стороной, а значит, скорость передачи информации на самом деле оказывается меньше, чем можно было предположить.

Связь между полосой пропускания линии и ее максимально возможной пропускной способностью, вне зависимости от принятого способа физического кодирования, установил Клод Шеннон:

$$C = F \log_2 (1 + P_c/P_ш),$$

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

Из этого соотношения видно, что хотя теоретического предела пропускной способности линии с фиксированной полосой пропускания не существует, на практике такой предел имеется. Действительно, повысить пропускную способность линии можно за счет увеличения мощности передатчика или же уменьшения мощности шума (помех) на линии связи. Обе эти составляющие поддаются изменению с большим трудом. Повышение мощности передатчика ведет к

значительному увеличению его габаритов и стоимости. Снижение уровня шума требует применения специальных кабелей с хорошими защитными экранами, что весьма дорого, а также снижения шума в передатчике и промежуточной аппаратуре, чего достичь весьма не просто. К тому же влияние мощностей полезного сигнала и шума на пропускную способность ограничено логарифмической зависимостью, которая растет далеко не так быстро, как прямопропорциональная. Так, при достаточно типичном исходном отношении мощности сигнала к мощности шума в 100 раз повышение мощности передатчика в 2 раза даст только 15 % увеличения пропускной способности линии.

Помехоустойчивость линии связи

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

Перекрестные наводки на ближнем конце (Near End Cross Talk - NEXT) определяют помехоустойчивость кабеля к внутренним источникам помех, когда электромагнитное поле сигнала, передаваемого выходом передатчика по одной паре проводников, наводит на другую пару проводников сигнал помехи. Если ко второй паре будет подключен приемник, то он может принять наведенную внутреннюю помеху за полезный сигнал. Показатель NEXT, выраженный в децибелах, равен 10 log $P_{вых}/P_{нав}$, где $P_{вых}$ - мощность выходного сигнала, $P_{нав}$ - мощность наведенного сигнала.

Чем меньше значение NEXT, тем лучше кабель. Так, для витой пары категории 5 показатель NEXT должен быть меньше -27 дБ на частоте 100 МГц.

Показатель NEXT обычно используется применительно к кабелю, состоящему из нескольких витых пар, так как в этом случае взаимные наводки одной пары на другую могут достигать значительных величин. Для одинарного коаксиального кабеля (то есть состоящего из одной экранированной жилы) этот показатель не имеет смысла, а для двойного коаксиального кабеля он также не применяется вследствие высокой степени защищенности каждой жилы. Оптические волокна также не создают, сколько-нибудь заметных помех друг для друга.

В связи с тем, что в некоторых новых технологиях используется передача данных одновременно по нескольким витым парам, в последнее время стал

применяться показатель *PowerSUM*, являющийся модификацией показателя NEXT. Этот показатель отражает суммарную мощность перекрестных наводок от всех передающих пар в кабеле.

Достоверность передачи данных

Достоверность передачи данных характеризует вероятность искажения для каждого передаваемого бита данных. Иногда этот же показатель называют ***интенсивностью битовых ошибок (Bit Error Rate, BER).*** Величина BER для каналов связи без дополнительных средств защиты от ошибок (например, самокорректирующихся кодов или протоколов с повторной передачей искаженных кадров) составляет, как правило,10^{-4} - 10^{-6}, в оптоволоконных линиях связи - 10^{-9}. Значение достоверности передачи данных, например, в 10^{-4} говорит о том, что в среднем из 10000 бит искажается значение одного бита.

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

1.12. Особенности построения цифровых систем передачи

Магистральные линии связи (основные понятия)

Высокая стоимость линий связи обуславливает разработку систем и методов, позволяющих одновременно передавать по одной линии связи большое число независимых сообщений, т.е. использовать линию многократно. Такие системы связи называют ***многоканальными.*** Связь, осуществляемую с помощью этих систем, принято называть ***многоканальной связью.*** Практически все современные системы связи за редким исключением являются многоканальными.

В современных сетях связи используются ***аналоговые и цифровые системы передачи*** с тенденцией постепенного перехода к применению только цифровых систем.

Многоканальные системы передачи с частотным и временным разделением каналов - это сложный комплекс технических средств, включающий в себя оконечную аппаратуру, устанавливаемую на *оконечных* пунктах (ОП), промежуточную аппаратуру, размещаемую в ***обслуживаемых (ОУП) или необслуживаемых (НУП) усилительных пунктах***, а также линий связи (*Рис. 21*).

В отличие от аналоговых систем в цифровых системах на обслуживаемых и необслуживаемых пунктах устанавливается аппаратура для восстановления (***регенерации***) импульсных сигналов линейного тракта. Отсюда обслуживаемые и необслуживаемые пункты в этих системах принято называть ***регенерационными (ОРП, НРП).***

Поясним, для чего нужны усилительные и регенерационные пункты. Дальность передачи сигналов по физическим цепям (средам) определяется, прежде всего, ***затуханием*** (ослаблением) сигнала из-за того, что в цепи теряется часть энергии передаваемого сигнала. Конкретные электрические параметры цепи и чувствительность приемного устройства определяют допустимую дальность связи. Например, при передаче речи мощность сигнала на выходе микрофона телефонного аппарата $P_{ПЕР}$ = 1 мВт, а чувствительность телефона приемного аппарата $P_{ПР}$ = 0,001 мВт. Таким образом, максимально допустимое затухание цепи не должно быть больше $a_{max}=10lg(P_{ПЕР}/P_{ПР})=10lg(1/0.001)=30$ дБ. Зная затухание a_{max} и километрический коэффициент затухания α, можно определить дальности передачи $l=a_{max}/\alpha$.

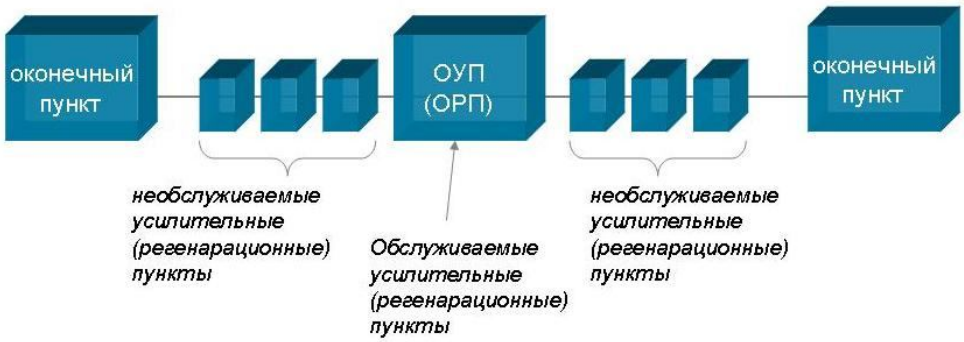


Рис. 21. Структурная схема построения многоканальной системы передачи данных

Аппаратура ОУП и НУП служит не только для усиления аналогового сигнала, но и для коррекции (выравнивания) амплитудно-частотных и фазочастотных характеристик линейного тракта.

Аппаратура НРП и ОРП предназначена для восстановления амплитуды, длительности и временного интервала между импульсами сигнала цифровых систем.

Основной тенденцией развития телекоммуникаций во всем мире является ***цифровизация*** сетей связи, предусматривающая построение сети на базе цифровых методов передачи и коммутации. Это объясняется следующими существенными преимуществами цифровых методов передачи перед аналоговыми:

Высокая помехоустойчивость. Представление информации в цифровой форме позволяет осуществлять регенерацию (восстановление) этих символов

при передаче их по линии связи, что резко снижает влияние помех и искажений на качество передачи информации.

Слабая зависимость качества передачи от длины линии связи. В пределах каждого регенерационного участка искажения передаваемых сигналов оказываются ничтожными. Длина регенерационного участка и оборудование регенератора при передаче сигналов на большие расстояния остаются практически такими же, как и в случае передачи на малые расстояния. Так, при увеличении длины линии в 100 раз для сохранения неизменным качества передачи информации достаточно уменьшить длину регенерационного участка лишь на несколько процентов.

Стабильность параметров каналов цифровых систем передачи данных (ЦСПД) Стабильность и идентичность параметров каналов (остаточного затухания, частотной и амплитудной характеристик и др.) определяются в основном устройствами обработки сигналов в аналоговой форме. Поскольку такие устройства составляют незначительную часть оборудования ЦСПД, стабильность параметров каналов в таких системах значительно выше, чем в аналоговых. Этому также способствует отсутствие в ЦСПД влияния загрузки системы на параметры отдельных каналов.

Эффективность использования пропускной способности каналов для передачи дискретных сигналов. При вводе дискретных сигналов непосредственно в групповой тракт ЦСПД скорость их передачи может приближаться к скорости передачи группового сигнала. Если, например, при этом будут использоваться временные позиции, соответствующие только одному каналу ТЧ, то скорость передачи будет близка к 64 кбит/с, в то время как в аналоговых системах она обычно не превышает 33,6 кбит/с.

Возможность построения цифровой сети связи. Цифровые системы передачи в сочетании с цифровыми системами коммутации являются основой цифровой сети связи, в которой передача, транзит и коммутация сигналов осуществляются в цифровой форме. При этом параметры каналов практически не зависят от структуры сети, что обеспечивает возможность построения гибкой разветвленной сети, обладающей высокими надежностными и качественными показателями.

Высокие технико-экономические показатели. Передача и коммутация сигналов в цифровой форме позволяют реализовывать оборудование на единых аппаратных платформах. Это позволяет резко снижать трудоемкость изготовления оборудования, значительно снижать его стоимость, потребляемую энергию и габариты. Кроме того, существенно упрощается эксплуатация систем и повышается их надежность.

Требования к цифровым системам передачи определены в рекомендациях МСЭ-Т серии G.

Структура первичной сети предопределяет объединение и разделение потоков передаваемой информации, поэтому используемые на ней системы передачи строятся по ***иерархическому принципу.*** Применительно к цифровым системам этот принцип заключается в том, что число каналов цифровых систем

передачи данных, соответствующее данной ступени иерархии, больше числа каналов предыдущей ступени в целое число раз.

Аналоговые системы передачи с частотным разделением каналов также строятся по иерархическому принципу, но в отличие от цифровых систем передачи данных для них ступенями иерархии являются не сами системы передачи, а типовые группы каналов.

Цифровая система передачи, соответствующая первой ступени иерархии, называется ***первичной,*** где осуществляется прямое преобразование относительно небольшого числа первичных сигналов в первичный цифровой поток. Системы передачи второй ступени иерархии объединяют определенное число первичных потоков во ***вторичный цифровой поток*** и т.д.

В рекомендациях ***МСЭ-Т*** представлено два типа иерархий цифровых систем передачи данных: ***плезиохронная цифровая иерархия (ПЦИ)*** и ***синхронная цифровая иерархия (СЦИ)***. Первичным сигналом для *всех* типов является цифровой поток со скоростью передачи 64 кбит/с, называемый ***основным цифровом каналом***. Для объединения сигналов основного цифрового канала в групповые высокоскоростные цифровые сигналы используется принцип ***временного разделения каналов.***

> ***МСЭ-Т*** – это Сектор стандартизации электросвязи Международного союза электросвязи. Он действует в качестве форума, на котором представители правительств и частного сектора могут координировать стандарты глобальных сетей и служб электросвязи.

Появившаяся исторически первой плезиохронная цифровая иерархия имеет *европейскую*, *североамериканскую* и *японскую* разновидности. Для цифровых потоков ПЦИ применяют соответствующие обозначения. Для североамериканской и японской ПЦИ применяется обозначение Т (иногда DS), для европейской ПЦИ - Е. Цифровые потоки первого уровня обозначаются соответственно Т-1 и Е-1, второго Т-2 и Е-2 и т.д.

К использованию на сетях связи РФ принята европейская плезиохронная цифровая иерархия.

Аналоговая модуляция

В настоящее время все чаще данные, изначально имеющие аналоговую форму (речь, телевизионное изображение), передаются по каналам связи в дискретном (цифровом) виде, то есть в виде последовательности единиц и нулей. Процесс представления аналоговой информации в дискретной форме называется ***дискретной модуляцией.*** Термины «модуляция» и «кодирование» часто используют как синонимы.

Аналоговая модуляция применяется для передачи дискретных данных по каналам с узкой полосой частот, типичным представителем которых является

***канал тональной частоты*,** предоставляемый в распоряжение пользователям общественных телефонных сетей. Этот канал передает частоты в диапазоне от 300 до 3400 Гц, таким образом, его полоса пропускания равна 3100 Гц. Хотя человеческий голос имеет гораздо более широкий спектр - примерно от 100 Гц до 10 кГц, - для приемлемого качества передачи речи диапазон в 3100 Гц является хорошим решением. Строгое ограничение полосы пропускания тонального канала связано с использованием аппаратуры уплотнения и коммутации каналов в телефонных сетях.

Устройство, которое выполняет функции модуляции несущей синусоиды на передающей стороне и демодуляции на приемной стороне, носит название ***модем* (*мод*улятор - *дем*одулятор).**

Методы модуляции аналогового сигнала

Аналоговая модуляция является таким способом физического кодирования, при котором информация кодируется изменением амплитуды, частоты или фазы синусоидального сигнала несущей частоты. Основные способы модуляции аналогового сигнала показаны на рис. 21. На диаграмме (рис. 21, а) показана последовательность бит исходной информации, представленная потенциалами высокого уровня для логической единицы и потенциалом нулевого уровня для логического нуля. Такой способ кодирования называется потенциальным кодом, который часто используется при передаче данных между блоками компьютера.

При ***амплитудной модуляции*** (рис. 21, б) для логической единицы выбирается один уровень амплитуды синусоиды несущей частоты, а для логического нуля - другой. Этот способ редко используется в чистом виде на практике из-за низкой помехоустойчивости, но часто применяется в сочетании с другим видом модуляции - *фазовой модуляцией*.

При ***частотной модуляции*** (рис.21, в) значения 0 и 1 исходных данных передаются синусоидами с различной частотой - f_0 и f_1. Этот способ модуляции не требует сложных схем в модемах и обычно применяется в низкоскоростных модемах, работающих на скоростях 300 или 1200 бит/с.

При ***фазовой модуляции*** (рис. 21, г) значениям данных 0 и 1 соответствуют сигналы одинаковой частоты, но с различной фазой, например 0 и 180 градусов или 0,90,180 и 270 градусов.

В скоростных модемах часто используются комбинированные методы модуляции, как правило, амплитудная в сочетании с фазовой.

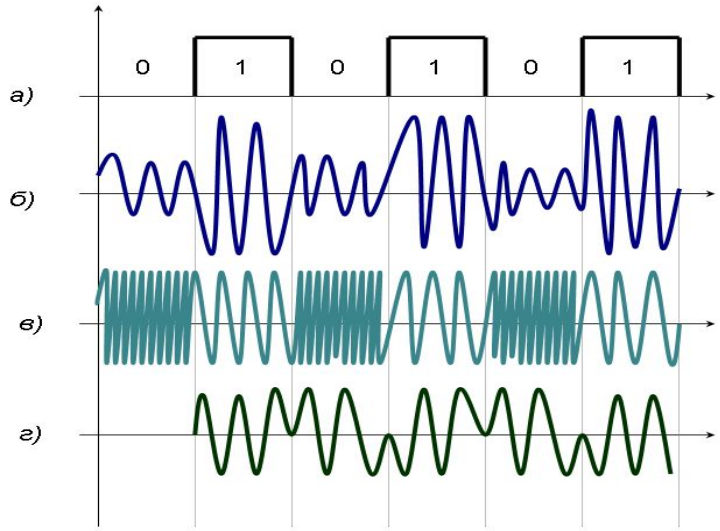


Рис. 22. Типы аналоговой модуляции

Дискретная модуляция аналоговых сигналов

По мере развития техники съема и передачи аналоговых данных выяснилось, что передача их в аналоговой форме не позволяет улучшить качество принятых на другом конце линии данных, если они существенно исказились при передаче. Сам аналоговый сигнал не дает никаких указаний ни о том, что произошло искажение, ни о том, как его исправить, поскольку форма сигнала может быть любой, в том числе и такой, которую зафиксировал приемник. Улучшение же качества линий, требует огромных усилий и капиталовложений. Поэтому на смену аналоговой технике записи и передачи звука и изображения пришла цифровая техника. Эта техника использует так называемую ***дискретную модуляцию*** исходных непрерывных во времени аналоговых процессов.

Поскольку человеку наиболее привычны представление и арифметика в десятичной системе счисления, а для компьютера - двоичное представление и двоичная арифметика, была введена компромиссная система **двоично-десятичной записи чисел**.

Преобразование десятичных чисел в двоичные:

Допустим, нам нужно перевести число 22 в двоичное. Можно воспользоваться следующей процедурой :

22 /2 = 11 с остатком 0
11 /2 = 5 с остатком 1
5 /2 = 2 с остатком 1
2 /2 = 1 с остатком 0
1 /2 = 0 с остатком 1

Итак, мы делим каждое частное на 2 и записываем остаток в начало двоичной записи. Продолжаем деление до тех пор, пока в делимом не будет 0. В результате получаем число 22 в двоичной записи: 10110.

Для **преобразования из двоичной системы в десятичную** используем следующую таблицу степеней основания 2:

512	256	128	64	32	16	8	4	2	1

Начиная с цифры 1 все цифры умножаются на два. Точка, которая стоит после 1, называется двоичной точкой.

В нашем примере , переведём число 10110 в десятичный вид используя эту таблицу :

512	256	128	64	32	16	8	4	2	1
					1	0	1	1	0
					16	0	4	2	0

Дискретные способы модуляции основаны на дискретизации непрерывных процессов, как по амплитуде, так и по времени (рис. 23). Рассмотрим принципы дискретной модуляции на примере ***импульсно-кодовой модуляции, ИКМ (Pulse Amplitude Modulation, PAM),*** которая широко применяется в цифровой телефонии. При использовании ИКМ процесс преобразования включает три этапа: отображение, квантование и кодирование

Первый этап – отображение. Амплитуда исходного непрерывного сигнала измеряется с заданным периодом, за счет чего происходит дискретизация

по времени. На этом этапе аналоговый сигнал преобразуется в сигналы импульсно-амплитудной модуляции (ИАМ). Выполнение этапа базируется на теории отображения Найквиста-Котельникова, основное положение которой гласит: если аналоговый сигнал отображается (т. е. представляется в виде последовательности ее дискретных по времени значений) на регулярном интервале с частотой не менее чем в два раза выше частоты самой высокой гармоники спектра исходного непрерывного сигнала, то отображение будет содержать информацию, достаточную для восстановления исходного сигнала.

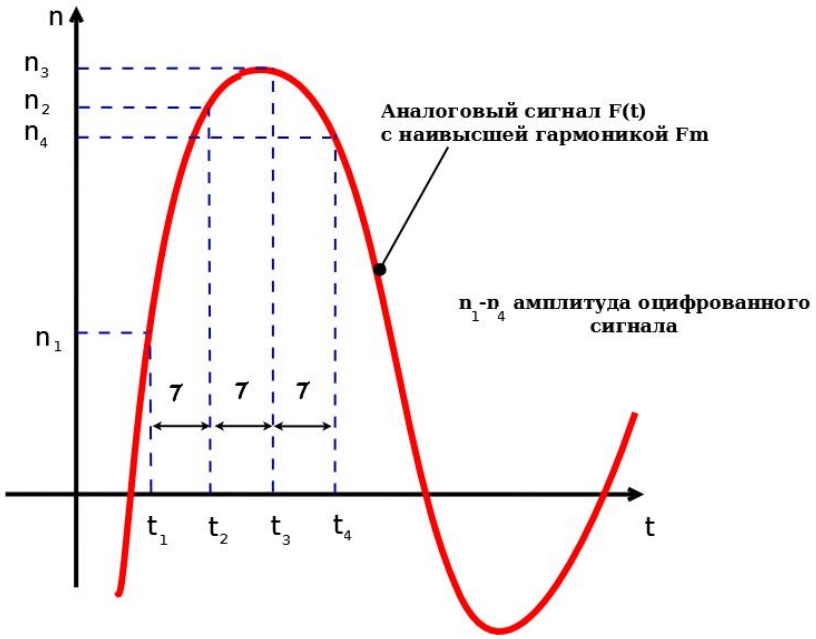


Рис. 23. . Дискретная модуляция непрерывного процесса

На ***этапе квантования*** каждому сигналу ИАМ придается квантованное значение, соответствующее ближайшему уровню квантования. Весь диапазон изменения амплитуды сигналов ИАМ разбивается на 128 или 256 уровней квантования. Чем больше уровней квантования, тем точнее амплитуда ИАМ – сигнала представляется квантованным уровнем.

На ***этапе кодирования*** каждому квантованному отображению ставится в соответствие 7-разрядный (если число уровней квантования равно 128) или 8-разрядный (при 256-шаговом квантовании) двоичный код. На рис. 24 показаны сигналы 8-элементного двоичного кода 00101011, соответствующего квантованному сигналу с уровнем 43. При кодировании 7-элементными кодами скорость передачи данных по каналу должна составлять 56 Кбит/с (это произведение частоты отображения на разрядность двоичного кода), а при кодировании 8-элементными кодами – 64 Кбит/с.

8000x7 = 56000 бит/с или 56 Кбит/с;

8000x8 = 64000 бит/с или 64 Кбит/с.

Стандартным является цифровой канал 64 Кбит/с, который называется также *элементарным каналом цифровых телефонных сетей.*

Устройство, которое выполняет указанные этапы преобразования аналоговой величины в цифровой код, называется ***аналого-цифровым преобразователем (АЦП).*** На приемной стороне с помощью ***цифро-аналогового преобразователя (ЦАП)*** осуществляется обратное преобразование, т. е. производится демодуляция оцифрованных амплитуд непрерывного сигнала, восстановление исходной непрерывной функции времени.

Для качественной передачи голоса в методе ИКМ используется частота квантования амплитуды звуковых колебаний в 8000 Гц. Это связано с тем, что в аналоговой телефонии для передачи голоса был выбран диапазон от 300 до 3400 Гц, который достаточно качественно передает все основные гармоники собеседников. В соответствии с теоремой Найквиста - Котельникова для качественной передачи голоса достаточно выбрать частоту дискретизации, в два раза превышающую самую высокую гармонику непрерывного сигнала, то есть 2 x 3400 = 6800 Гц. Выбранная в действительности частота дискретизации 8000 Гц обеспечивает некоторый запас качества.

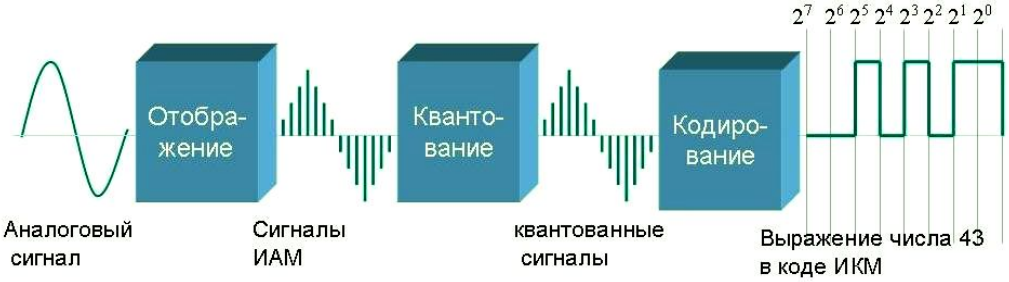


Рис. 24. Преобразование аналогового сигнала в 8-ми элементный цифровой код

Передача непрерывного сигнала в дискретном виде требует от сетей жесткого соблюдения временного интервала в 125 мкс (соответствующего частоте дискретизации 8000 Гц) между соседними замерами, то есть требует синхронной передачи данных между узлами сети. При несоблюдении синхронности прибывающих замеров исходный сигнал восстанавливается неверно, что приводит к искажению голоса, изображения или другой мультимедийной информации, передаваемой по цифровым сетям. Так, искажение синхронизации в 10 мс может привести к эффекту «эха», а сдвиги между замерами в 200 мс приводят к потере распознаваемости произносимых слов. В то же время потеря одного замера при соблюдении синхронности между остальными замерами практически не сказывается на воспроизводимом звуке. Это происходит за счет сглаживающих устройств в цифро-аналоговых преобразователях, которые основаны на свойстве инерционности любого физического сигнала - амплитуда звуковых колебаний не может мгновенно измениться на большую величину.

На качество сигнала после ЦАП влияет не только синхронность поступления на его вход замеров, но и погрешность дискретизации амплитуд этих заме-

ров. В теореме Найквиста - Котельникова предполагается, что амплитуды функции измеряются точно, в то же время использование для их хранения двоичных чисел с ограниченной разрядностью несколько искажает эти амплитуды. Соответственно искажается восстановленный непрерывный сигнал, что называется шумом дискретизации (по амплитуде).

Существуют и другие методы дискретной модуляции, позволяющие представить замеры голоса в более компактной форме, например в виде последовательности 4-битных или 2-битных чисел. При этом один голосовой канал требует меньшей пропускной способности, например 32 Кбит/с, 16 Кбит/с или еще меньше. Используется и такая концепция преобразования аналоговых сигналов в цифровые, при которой квантуются и затем кодируются не сами сигналы ИАМ, а лишь их изменения, причем число уровней квантования принимается таким же. Очевидно, что такая концепция позволяет производить преобразование сигналов с большей точностью.

Представленные в цифровой форме непрерывные данные легко можно передать через компьютерную сеть. Для этого достаточно поместить несколько замеров в кадр какой-нибудь стандартной сетевой технологии, снабдить кадр правильным адресом назначения и отправить адресату. Адресат должен извлечь из кадра замеры и подать их с частотой квантования (для голоса - с частотой 8000 Гц) на цифро-аналоговый преобразователь. По мере поступления следующих кадров с замерами голоса операция должна повториться. Если кадры будут прибывать достаточно синхронно, то качество голоса может быть достаточно высоким. Однако, как мы уже знаем, кадры в компьютерных сетях могут задерживаться как в конечных узлах (при ожидании доступа к разделяемой среде), так и в промежуточных коммуникационных устройствах - мостах, коммутаторах и маршрутизаторах. Для качественной передачи оцифрованных непрерывных сигналов - голоса, изображения - сегодня используют специальные цифровые сети, такие как ISDN, ATM, и сети цифрового телевидения. А также применяются различные программно-аппаратные способы, в частности реализация ***QoS.***

QoS (англ. Quality of Service - качество обслуживания). Предоставление приоритезации различным приложениям, пользователям или потокам трафика, или гарантия определенного уровня производительности потока данных.

Сети, которые связывают хосты, используют разнообразные сетевые устройства, включая сетевые адаптеры хостов, маршрутизаторы, коммутаторы и хабы. Каждый из них имеет сетевые интерфейсы. Каждый сетевой интерфейс может принять и передать трафик с конечной скоростью. Если скорость, с которой трафик направлен на интерфейс, выше, чем скорость, с которой интерфейс передает трафик дальше, то возникает перегрузка.

Сетевые устройства могут обработать состояние перегрузки, организуя очередь трафика в памяти устройства (в буфере), пока перегрузка не пройдет. В других случаях сетевое оборудование может отказаться от трафика, чтобы облегчить перегрузку. В результате приложения сталкиваются с изменением времени ожидания (так как трафик сохраняется в очередях на интерфейсах) или с потерей трафика.

Способность сетевых интерфейсов к пересылке трафика и наличие памяти для сохранения трафика в сетевых устройствах (до тех пор, пока трафик не может быть послан дальше) составляют фундаментальные ресурсы, требующиеся для обеспечения QoS для потоков трафика приложений.

Устройства, поддерживающие QoS, разумно используют ресурсы сети для передачи трафика. То есть трафик приложений, более терпимых к задержкам, становится в очередь (сохраняется в буфере в памяти), а трафик приложений, критичных к задержкам, передается далее.

Для выполнения этой задачи сетевое устройство должно идентифицировать трафик путем классификации пакетов, а также иметь очереди и механизмы их обслуживания.

Механизм обработки трафика включает в себя:

- 802.1p
- Дифференцированные услуги per-hop-behaviors (diffserv PHB).
- Интегрированные услуги (intserv).
- ATM и др.

Большинство локальных сетей основано на технологии IEEE 802, включая Ethernet, Token Ring и др. ***IEEE802.1p*** — это механизм обработки трафика для поддержки QoS в таких сетях.

IEEE 802.1p определяет поле (уровень 2 в сетевой модели OSI) в заголовке пакета 802, которое может нести одно из восьми значений приоритета. Как правило, хосты или маршрутизаторы, посылая трафик в локальную сеть, маркируют каждый посланный пакет, присваивая ему определенное значение приоритета. Предполагается, что сетевые устройства, такие, как коммутаторы, мосты и хабы, обработают пакеты соответствующим образом, используя механизмы организации очередей. Область применения IEEE 802.1p ограничена локальной сетью (LAN). Как только пакет пересекает локальную сеть (через уровень 3 OSI), приоритет 802.1p удаляется.

Diffserv (англ. Differentiated Services) - простой метод классификации, управления и предоставления качества обслуживания в современных IP сетях. Он определяет поле в уровне 3 заголовка пакетов IP, названных ***diffserv codepoint (DSCP).***

Intserv (англ. integrated services) - метод классификации, управления и предоставления гарантированного качества обслуживания в современных IP сетях. Гарантированный сервис обещает нести некоторый объем трафика с измеримой и ограниченной задержкой. Сервис, управляющий загрузкой, соглашается нести некоторый объем трафика с «появлением легкой загруженности сети». Это - измеримые услуги в том смысле, что они определены, чтобы обеспечить измеримый QoS к определенному количеству трафика.

ATM (***англ. Asynchronous Transfer Mode— асинхронный способ передачи данных)*** — сетевая технология, основанная на передаче данных в виде ячеек фиксированного размера (53 байта), из которых 5 байтов используется под заголовок.

Сеть строится на основе ATM. коммутатора и ATM. маршрутизатора. Технология реализуется как в локальных, так и в глобальных сетях. Допускается совместная передача различных видов информации, включая видео, голос. Ячейки данных, используемые в ATM, меньше в сравнении с элементами данных, которые используются в других технологиях.

Небольшой, постоянный размер ячейки, используемый в ATM, позволяет:

- передавать данные по одним и тем же физическим каналам, причём как при низких, так и при высоких скоростях;
- работать с постоянными и переменными потоками данных;
- интегрировать любые виды информации: тексты, речь, изображения, видеофильмы;
- поддерживать соединения типа точка-точка, точка-многоточка, многоточка-многоточка.

QoS имеет еще много разных сложных механизмов, обеспечивающих работу этой технологии. Отметим лишь один важный момент: для того, чтобы QoS заработала, необходима поддержка этой технологии и соответствующая настройка на всем протяжении передачи от начальной точки до конечной.

Передача дискретных данных на канальном уровне

Канальный уровень обеспечивает передачу пакетов данных, поступающих от протоколов верхних уровней, узлу назначения, адрес которого также указывает протокол верхнего уровня. Протоколы канального уровня обеспечивают передачу пакетов данных адресату, причем каждый пакет оформляется в кадр собственного формата (отдельные поля кадра заполняются адресом назначения и контрольной суммой для выявления искаженных кадров). Доставка кадров данных осуществляется в пределах сетей с простой топологией связей и однотипной или близкой технологией. Например, это односегментные сети Ethernet или многосегментные сети Ethernet и Token Ring иерархической топологии,

разделенных мостами и коммутаторами. В более сложных структурах сетей задача передачи кадров между узлами осуществляется с помощью протоколов сетевого уровня.

Протоколы, работающие на канальном уровне, обеспечивают передачу данных:

- в асинхронном и синхронном режимах;
- с предварительным установлением соединения и без предварительного установления соединения (дейтаграммную);
- с обнаружением искаженных данных и без обнаружения;
- с обнаружением потерянных данных и без обнаружения;
- с восстановлением искаженных и потерянных данных и без восстановления;
- с поддержкой динамической компрессии данных и без поддержки.

Многие из этих свойств и возможностей характерны и для протоколов более высоких уровней.

Асинхронная и синхронная передачи

Синхронизация между приемником и передатчиком в основном обеспечивается средствами физического уровня (на этом уровне единицей информации является ***бит*** и средства этого уровня поддерживают ***побитовую синхронизацию***) и канального уровня (на этом уровне единицей информации является ***кадр*** и средства этого уровня поддерживают ***покадровую синхронизацию***).

При покадровой синхронизации приемник обязан обеспечить распознавание начала первого байта поступившего кадра, границ полей кадра и признака окончания кадра. При плохом качестве линии связи кроме побитовой и покадровой синхронизации для повышения надежности передачи данных используются дополнительные средства синхронизации на уровне байт, и тогда такой режим работы называется асинхронным или стартстопным. Его использование объясняется еще и тем, что в составе компьютера есть устройства, которые генерируют байты в случайные моменты времени (например, клавиатура, с которой вводятся данные в компьютер).

В асинхронном режиме передача осуществляется небольшими блоками фиксированной длины (обычно байтами). Каждый байт обрамляется двумя сигналами – стартбит и стопбит. Синхронизация приемника обеспечивается сигналом стартбит. Асинхронным такой режим называется потому, что каждый байт может быть несколько смещен относительно побитовых тактов предыдущего байта.

DTM (англ. Dynamic synchronous Transfer Mode, динамический режим синхронной передачи) — альтернативная ATM коммуникационная технология, созданная фирмой Dynarc, которая базируется в Швеции и США.

В синхронном режиме пользовательские данные передаются покадрово, причем каждый кадр обрамляется байтами синхронизации (старт-стопные биты для каждого байта отсутствуют). Байт синхронизации – это заранее оговоренный 8-разрядный двоичный код, который оповещает приемник о приходе очередного кадра данных. При передаче длинных кадров может произойти рассинхронизация приемника, и тогда используются самосинхронизирующие коды.

Асинхронные протоколы канального уровня оперируют со стандартными наборами символов (ASCII или EBCDIC) или кадрами, концевик которых содержит контрольную сумму для обнаружения искаженных кадров. Так как первые 32 (ASCII) или 27 (EBCDIC) кодов в этих наборах являются специальными кодами, которые не отображаются на дисплее или принтере, то они использовались асинхронными протоколами для управления режимом обмена данными. В самих пользовательских данных, которые представляли собой буквы, цифры, а также такие знаки, как @, %, $ и т. п., специальные символы никогда не встречались, так что проблемы их отделения от пользовательских данных не существовало.

В синхронных протоколах между пересылаемыми символами (байтами) нет стартовых и стоповых сигналов, поэтому отдельные символы в этих протоколах пересылать нельзя. Все обмены данными осуществляются кадрами, которые имеют в общем случае заголовок, поле данных и концевик (рис. 25). Все биты кадра передаются непрерывным синхронным потоком, что значительно ускоряет передачу данных.

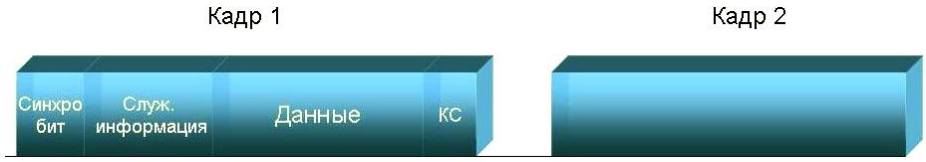


Рис. 25. Кадры синхронных протоколов

Так как байты в этих протоколах не отделяются друг от друга служебными сигналами, то одной из первых задач приемника является распознавание границы байт. Затем приемник должен найти начало и конец кадра, а также определить границы каждого поля кадра - адреса назначения, адреса источника, других служебных полей заголовка, поля данных и контрольной суммы, если она имеется. Большинство протоколов допускает использование в кадре поля данных переменной длины. Иногда и заголовок может иметь переменную длину. Обычно протоколы определяют максимальное значение, которое может иметь длина поля данных. ***Эта величина называется максимальной единицей передачи данных (Maximum Transfer Unit, MTU).*** В некоторых протоколах задается также минимальное значение, которое может иметь длина поля данных. Например, протокол Ethernet требует, чтобы поле данных содержало, по крайней мере, 46 байт данных (если приложение хочет отправить меньшее количество

байт, то оно обязано дополнить их до 46 байт любыми значениями). Есть протоколы с кадрами фиксированной длины, например, 53 байта в протоколе ATM.

Синхронные протоколы канального уровня бывают двух типов:

- ***символьно-ориентированные (байт-ориентированные),*** используемые для передачи в основном текстовых файлов;
- ***бит-ориентированные***, применяемые при передаче как двоичных, так и символьных данных, т. е. являющиеся более универсальными протоколами.

Протоколы с гибким форматом кадра

Для большей части протоколов характерны кадры, состоящие из служебных полей фиксированной длины. Исключение делается только для поля данных, с целью экономной пересылки, как небольших квитанций, так и больших файлов. Способ определения окончания кадра путем задания длины поля данных, рассмотренный выше, как раз рассчитан на такие кадры с фиксированной структурой и фиксированными размерами служебных полей.

Однако существует ряд протоколов, в которых кадры имеют гибкую структуру. Например, к таким протоколам относятся очень популярный прикладной протокол управления сетями SNMP, а также протокол канального уровня PPP, используемый для соединений типа «точка-точка». Кадры таких протоколов состоят из неопределенного количества полей, каждое из которых может иметь переменную длину. Начало такого кадра отмечается некоторым стандартным образом, например, с помощью флага, а затем протокол последовательно просматривает поля кадра и определяет их количество и размеры. Каждое поле обычно описывается двумя дополнительными полями фиксированного размера. Например, если в кадре встречается поле, содержащее некоторую символьную строку, то в кадр вставляются три поля:

Тип	Длина	Значение
String	6	public

Дополнительные поля «Тип» и «Длина» имеют фиксированный размер в один байт, поэтому протокол легко находит границы поля «Значение». Так как количество таких полей также неизвестно, для определения общей длины кадра используется либо общее поле «Длина», которое помещается в начале кадра и относится ко всем полям данных, либо закрывающий флаг.

Протоколами канального уровня (с участием протоколов более высоких уровней) реализуются два способа связи между отправителем и получателем

данных: ***без установления логического соединения*** между ними *(рис.26,а)* и ***с предварительным установлением логического соединения*** *(рис. 26, б)*.

Способ связи ***без установления логического соединения*** характеризуется следующим:

- он используется в сетях с коммутацией пакетов, причем каждый пакет рассматривается как индивидуальный объект, независимая единица передачи информации;
- пакеты от отправителя можно передавать в произвольные моменты, а также одновременно множеству адресатов по различным маршрутам;
- перед передачей данных сквозная связь между отправителем и получателем заранее не устанавливается, не требуется также синхронизация аппаратуры связи на передающем и приемном пунктах;
- из-за занятости отдельных участков маршрута может осуществляться буферизация пактов в промежуточных узлах связи (такой способ не гарантирует доставку пакета);
- передача сигнала к отправителю от адресата, подтверждающего получение информации, не производится.

Это один из первых и простейших способов обмена данными в коммуникационной технологии. Он широко используется в *дейтаграммных сетях*, в которых реализуются ***дейтаграммные*** протоколы информационного обмена.

Дейтаграммные сети можно рассматривать как аналог обычных (не электронных) почтовых служб. Когда мы хотим отправить письмо, мы пишем на конверте почтовый адрес получателя и опускаем конверт в почтовый ящик. Почтовый адрес имеет иерархическую структуру и включает в себя, например, страну, город, улицу и номер дома. Почтовая служба обрабатывает каждое из полей в порядке иерархии, начиная с самого «общего» - страны адресата. В первую очередь, письмо передается в нужную страну, затем - в нужный город, а далее местные почтовые службы доставляют письмо непосредственно по месту назначения.

Способ связи (или режим связи), ориентированный на логическое соединение, относится к более поздней технологии. Он обеспечивает более высокий уровень сервиса по сравнению с дейтаграммной связью.

Особенности организации обмена данными с установлением логического соединения:

перед передачей информации между взаимодействующими абонентами (отправителем и получателем) устанавливается логический (виртуальный) канал, причем технология создания (установления) канала такова: отправитель посылает запрос на соединение удаленному адресату через ряд промежуточных узлов связи;

адресат, получив этот запрос, в случае «согласия» на установление логического канала посылает отправителю сигнал подтверждения; после получения сигнала подтверждения отправителем начинается обмен данными с управлением потоком, сегментацией и исправлением ошибок;

после завершения обмена данными адресат посылает пакет подтверждения этого события отправителю (клиенту – инициатору установления логического канала), который воспринимается как сигнал для разъединения канала. Следовательно, при использовании этого способа связи выделяются три этапа: установление канала, обмен данными, разъединение канала.

Рис. 26. способы установления логической связи

Режим «с соединением» целесообразно использовать для тех применений, где взаимодействие имеет долговременный характер, конфигурация взаимодействующих объектов постоянна, а поток данных не имеет больших пауз. Протоколы с установлением соединения обладают рядом дополнительных свойств, например, способностью обнаруживать и восстанавливать искаженные кадры. Для обнаружения искаженных кадров используется ряд методов, в частности методы, основанные на циклических избыточных кодах, которые выявляют многократные ошибки. Восстановление кадров основано на использовании метода повторной передачи кадров.

Режим «без соединения» больше подходит там, где взаимодействие имеет кратковременный характер, при котором объем передаваемых данных невелик, а интервалы между передачами значительны (относительно скорости передачи). Кроме того, его целесообразно использовать в системах с повышенными требованиями к надежности доставки данных адресату, так как эти требования можно удовлетворить путем тиражирования данных и передачи адресату по разным маршрутам.

Цифровое кодирование

Цифровое кодирование (Digital Encoding), иногда не совсем корректно называемое модуляцией, определяет способ представления битов в физическом канале передачи данных. Простейший метод NRZ используется в протоколах на базе интерфейса RS-232, в сетях Ethernet применяется кодирование PE, а в телефонии используется алгоритм HDB3 (этот метод служит для кодирования сигналов в потоках E1 и E2). Выбор метода кодирования зависит от полосы канала связи, используемой кабельной системы, скорости передачи данных и других параметров.

Цифровое кодирование - представление информации прямоугольными

Именно благодаря своей простоте и дешевизне реализации, цифровое кодирование завоевало очень большую популярность при передаче данных. В виду своей малой чувствительности к помехам на линии цифровое кодирование в последнее время применяют даже там, где раньше использовали только аналоговые передачи.

Для цифрового кодирования используют ***потенциальные*** и ***импульсные*** коды.

В потенциальных кодах для представления логических единиц и нулей используются только значение потенциала сигнала в период такта, а его перепады, формирующие законченные импульсы, во внимание не принимаются. Важно только какое значение в период такта имеет результирующий сигнал.

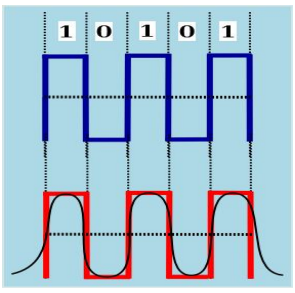


Рис. 27.Потенциальное кодирование

Импульсные коды представляют логический ноль и логическую единицу либо импульсами определенной полярности, или частью импульса - перепадом потенциала определенного направления. В значение импульсного кода включается весь импульс вместе с его перепадами.

Итак, данные можно «закодировать» потенциальными или импульсными кодами, чтобы передать по линии связи от приемника к источнику. Конечно, на самом деле под словом «закодировать» скрывается большое количество возможных методов цифрового кодирования, которые позволяют проводить кодирование данных с тем или иным результатам.

Давайте посмотрим, как самым простым способом можно закодировать дискретные данные. Самый простой способ: закодировать логическую единицу одним уровнем напряжения (высоким), а логический ноль другим (низким), то есть применить для кодирования последовательности двоичных данных обыкновенный потенциальный код. Как оказалось этот метод кодирования имеет специфическое название - потенциальный код без возвращения к нулю, сокращенно ***NRZ.***

Потенциальный код без возвращения к нулю NRZ

Этот код получил такое название потому, что при передаче последовательности единиц сигнал не возвращается к нулю в течение такта (как мы увидим ниже, в других методах кодирования возврат к нулю в этом случае происходит).

Код NRZ (Non Return to Zero) - без возврата к нулю - это простейший двухуровневый код. Результирующий сигнал имеет два уровня потенциала: Нулю соответствует нижний уровень, единице - верхний. Информационные переходы происходят на границе битов.

Рассмотрим три частных случая передачи данных кодом NRZ: чередующаяся последовательность нулей и единиц, последовательность нулей и последовательность единиц, Рис.28.

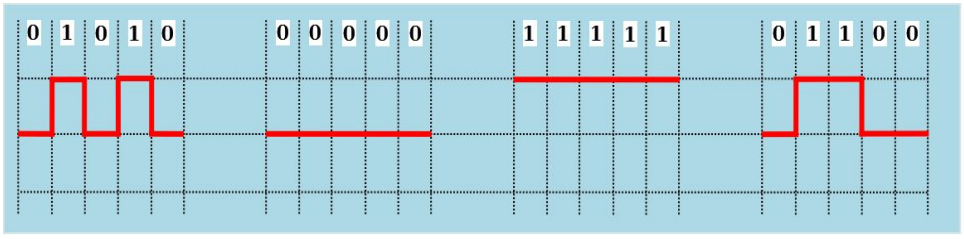


Рис. 28.Применение кода NRZ

Прежде всего, нам нужно попытаться угадать первую синусоиду и определить основную гармонику спектра при потенциальном кодировании в каждом из этих случаев, чтобы точнее определить какие код NRZ имеет требования к используемой линии связи.

Первый случай - передается информация, состоящая из бесконечной последовательности чередующихся единиц и нулей. Этот рисунок показывает, что

при чередовании единиц и нулей за один такт будет передаваться два бита 0 и 1. Можем мы угадать форму синусоиды? Да можем. Следовательно, при N - битовой скорости передачи период этой синусоиды равен T = 2N. Частота основная гармоника в этом случае равна f0 = N/2.

Таким образом, наибольшая частота для потенциального кода NRZ наблюдается при передаче чередующейся последовательности нулей и единиц и она равна f0 = N/2. Эта частота еще хороша, тем, что она низкая, т.е. может пропускаться всеми основными типами линий связи. Как видно, при такой последовательности этого кода скорость передачи данных вдвое превышает частоту сигнала.

А что же происходит при передаче последовательностей нулей и единиц? При передаче только единиц, или только нулей результирующий сигнал - постоянный ток, а значит при передаче последовательности одинаковых битов частота изменения сигнала равна нулю f0 = 0. Помимо этого, если учитывать, что спектр реального сигнала постоянно меняется в зависимости от того, какие данные передаются по линии связи, то следует опасаться передач длинных последовательностей нулей или единиц, которые сдвигают спектр сигнала в сторону низких частот. Другими словами код NRZ при передаче длинных последовательностей нулей или единиц имеет постоянную составляющую. И это очень плохо.

Дело в том, что к спектру передаваемого сигнала помимо требований к ширине, выдвигают еще одно очень важное требование - отсутствие постоянной составляющей (наличия постоянного тока между приемником и передатчиком), потому как применение различных трансформаторных развязок в линии связи не пропускает постоянный ток. Из-за этого многие линии связи, не обеспечивающие прямого гальванического соединения между приемником и источником, этот вид кодирования не поддерживают. Так, к примеру, одним из условий реализации балансной передачи по витым парам является применение в приемопередатчиках сетевого оборудования развязывающих согласующих трансформаторов, передача постоянной составляющей сигнала через которые невозможна. Следовательно, часть информации просто будет игнорироваться этой линией связи. Поэтому на практике всегда стараются избавиться от присутствия постоянной составляющей в спектре несущего сигнала уже на этапе кодирования.

Ещё один момент, который обращает внимание при передаче длинной последовательности единиц или нулей - отсутствие синхронизации. И это очень существенный недостаток этого кода.

В этом случае помогут только дополнительные методы синхронизации, о которых поговорим ниже.

И всё же, несмотря на все трудности и недостатки кода NRZ его несомненное достоинство - простота. К тому же потенциальный сигнал не надо кодировать и декодировать, поскольку такой же способ применяется и для передачи

данных внутри компьютера. Но все-таки, эти достоинства не перевешивают его недостатков, разве только один - дешевизна реализации.

плюсы и минусы кода NRZ**:**

- очень прост в реализации, обладает хорошей распознаваемостью ошибок (из-за двух резко отличающихся потенциалов).
- имеет постоянную составляющую при передаче нулей и единиц, что делает его невозможным для передачи в линиях с трансформаторными развязками.
- не самосинхронизирующийся код и это усложняет его передачу в любой линии.

Привлекательность кода NRZ, из-за которой имеет смысл заняться его улучшением, состоит в достаточно низкой частоте основной гармоники fo, которая равна N/2 Гц, как это было показано выше. Таким образом, код NRZ работает на низких частотах от 0 до N/2 Гц. В результате в чистом виде код NRZ в сетях не используется. Тем не менее, используются его различные модификации, в которых с успехом устраняют как плохую самосинхронизацию кода NRZ, так и наличие постоянной составляющей.

Следующие методы цифрового кодирования разрабатывались с целью каким-то образом улучшить возможности кода NRZ. Как пример, следующий метод.

Метод биполярного кодирования с альтернативной инверсией AMI

Метод биполярного кодирования с альтернативной инверсией (Bipolar Alternate Mark Inversion, AMI) является модификацией метода NRZ. В этом методе используются три уровня потенциала - отрицательный, нулевой и положительный. Три уровня сигнала это недостаток кода, потому что требуются лучшее (чем в предыдущем случае) соотношение сигнал/шум на входе приемного устройства.

Дополнительный уровень требует увеличение мощности передатчика примерно на 3 дБ для обеспечения той же достоверности приема бит на линии, что является общим недостатком кодов с несколькими состояниями сигнала по сравнению с двухуровневыми кодами.

Для кодирования логического нуля используется нулевой потенциал, логическая единица кодируется либо положительным потенциалом, либо отрицательным, при этом потенциал каждой новой единицы противоположен потенциалу предыдущей.

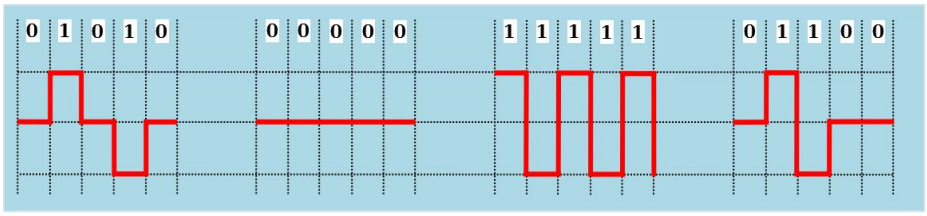


Рис. 29.Применение метода кодирования AMI

Как видно из рисунка, код AMI частично ликвидирует проблемы постоянной составляющей и отсутствия самосинхронизации, присущие коду NRZ при передаче длинных последовательностей единиц. Давайте снова рассмотрим частные случаи работы кода, и угадаем основную гармонику спектра результирующего сигнала для каждого из них. Как и в случае с NRZ при последовательности нулей - сигнал - постоянный ток - fo = 0

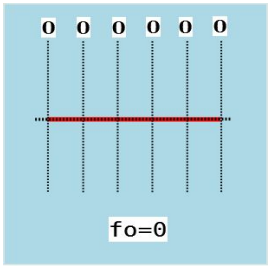


Рис. 30.Постоянный ток - fo = 0

Поэтому и код AMI требует дальнейшего улучшения, хотя задача упрощается - осталось справиться только с последовательностями нулей.

При передаче последовательности единиц сигнал на линии представляет собой последовательность разнополярных импульсов с тем же спектром, что и у кода NRZ, передающего чередующиеся нули и единицы, то есть без постоянной составляющей и с основной гармоникой fo = N/2

Теперь давайте посмотрим сигнал в случае чередующегося набора единиц и нулей. При передаче чередующихся единиц и нулей основная гармоника fo = N/2 Гц, что в два раза меньше чем у кода NRZ. В целом, для различных комбинаций бит на линии использование кода AMI приводит к более узкому спектру сигнала, чем для кода NRZ, а значит, и к более высокой пропускной способности линии.

Код AMI предоставляет также некоторые возможности по распознаванию ошибочных сигналов. Так, нарушение строгого чередования полярности сигналов говорит о ложном импульсе или исчезновении с линии корректного импульса. Сигнал с некорректной полярностью называется запрещенным сигналом (signal violation).

Вывод таков - код AMI ликвидирует постоянную составляющую при передаче последовательности единиц, имеет узкий спектр - от N/4 - N/2, частично ликвидирует проблемы синхронизации, по сравнению с кодом NRZ, но он использует не два, а три уровня сигнала на линии и это его недостаток. Но его удалось устранить следующему методу.

Потенциальный код с инверсией при единице NRZI

Этот код полностью похож на код AMI, но только использует два уровня сигнала. При передаче нуля он передает потенциал, который был установлен в предыдущем такте (то есть не меняет его), а при передаче единицы потенциал инвертируется на противоположный.

Этот код называется потенциальным кодом с инверсией при единице (Non Return to Zero with ones Inverted, NRZI). Он удобен в тех случаях, когда использование третьего уровня сигнала весьма нежелательно, например, в оптических кабелях, где устойчиво распознаются два состояния сигнала - свет и темнота.

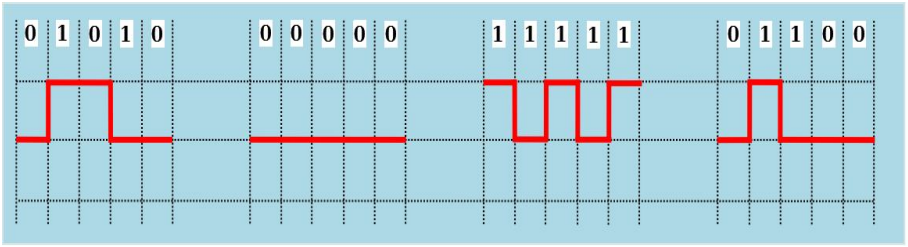


Рис. 31.Применение метода кодирования NRZI

Этот код немного отличается по форме результирующего сигнала от кода AMI, но если вычислить основные гармоники, для каждого случая, то окажется, что они такие же. Для последовательности чередующихся единиц и нулей основная частота сигнала fo=N/4(рис.31) ;

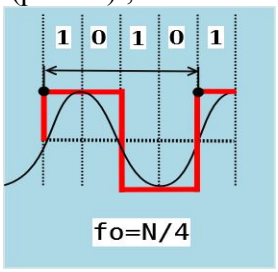


Рис. 32

при последовательности единиц - fo=N/2(рис.32);

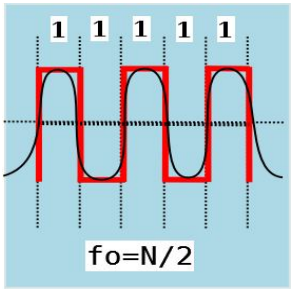


Рис. 33

При последовательности нулей сохраняется тот же недостаток fo=0 - постоянный ток в линии.

Из всего выше сказанного, складывается такая картина:

NRZ - простой код, но без синхронизации вообще, медленный, и имеет постоянные составляющие, как при передаче нулей, так и при передаче единиц. Он не используется в чистом виде, но послужил основой для создания последующих кодов;

AMI - этот код немного улучшил ситуацию, тут ликвидировали постоянную составляющую при передаче единиц, но она осталась при передаче нулей, благодаря сужению спектра несущего сигнала увеличилась скорость передачи в два раза, но он требует трех уровней сигнала, что усложняет его реализацию.

NRZI - обеспечивает те же возможности, что и код AMI, но использует для этого только два уровня сигнала и поэтому более приемлем для дальнейшего усовершенствования. Этот код всем хорош, он и быстрый и двухуровневый, осталась только побороть две его проблемы - постоянную составляющую при последовательности нулей, и обеспечить синхронизацию при передаче. Как мы потом убедимся, код NRZI стал основным при разработке более улучшенных методов кодирования на более высоких уровнях.

Биполярный импульсный код

Мы уже с вами говорили о том, что в сетях кроме потенциальных кодов используются и импульсные коды, когда данные представлены полным импульсом или же его частью - фронтом.

Наиболее простым случаем такого подхода является биполярный импульсный код, в котором единица представлена импульсом одной полярности, а ноль - другой. Каждый импульс длится половину такта. Биполярный импульсный код - трехуровневый код. Давайте посмотрим результирующие сигналы при передаче данных биполярным кодированием в следующих частных случаях.

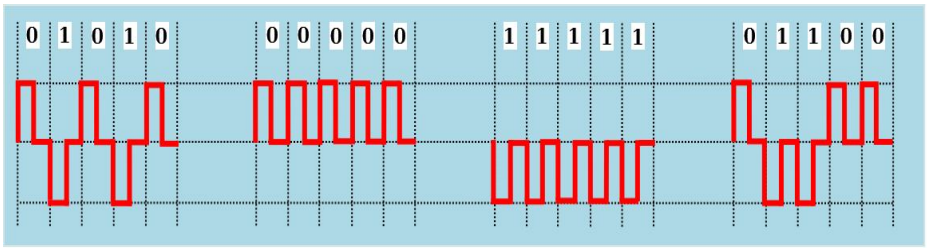


Рис. 34.Применение метода биполярного кодирования

Как видим, во всех этих случаях, особенностью кода является то, что в центре бита всегда есть переход (положительный или отрицательный). Следовательно, каждый бит обозначен. Приемник может выделить синхроимпульс (строб), имеющий частоту следования импульсов, из самого сигнала. Привязка производится к каждому биту, что обеспечивает синхронизацию приемника с передатчиком.

Такие коды, несущие в себе строб, называют самосинхронизирующимися.

И это бесспорное преимущество биполярного кодирования. Давайте теперь рассмотрим спектр сигналов для каждого рассматриваемого случая. При передаче всех нулей или единиц частота основной гармоники кода fo=N Гц, что в два раза выше основной гармоники кода NRZ и в четыре раза выше основной гармоники кода AMI при передаче чередующихся единиц и нулей. Этот недостаток кода не дает выигрыша в скорости передачи данных и явно свидетельствует о том, что импульсные коды медленнее потенциальных. Например, для передачи данных по линии со скоростью 10 Мбит/с, требуется частота несущего сигнала 10 МГц.

При передаче последовательности чередующихся нулей и единиц скорость возрастает, но не намного, частота основной гармоники кода fo=N/2 Гц.

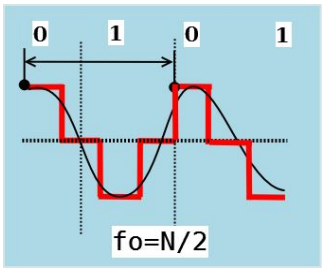


Рис. 35. Частота основной гармоники кода fo=N/2 Гц.

Биполярный импульсный код имеет большое преимущество, по сравнению с предыдущими кодами, - он самосинхронизирующийся. Но наряду с этим биполярные импульсные коды имеют широкий спектр сигнала, и поэтому очень медленные. Кроме этого, есть еще один его существенный недостаток биполярного кодирования - использование трех уровней. Из-за своего слишком широкого спектра биполярный импульсный код используется редко.

Манчестерский код

Манчестерский код был разработан, как усовершенствованный биполярный. Поэтому манчестерский код также относится к самосинхронизирующимся кодам, но в отличие от биполярного кода имеет не три, а только два уровня, что обеспечивает лучшую помехозащищенность.

В манчестерском коде для кодирования единиц и нулей используется перепад потенциала, то есть фронт импульса.

При манчестерском кодировании каждый такт делится на две части. Информация кодируется перепадами потенциала, происходящими в середине каждого такта. Это происходит следующим образом: Единица кодируется перепадом от низкого уровня сигнала к высокому, а ноль - обратным перепадом. В начале каждого такта может происходить служебный перепад сигнала, если нужно представить несколько единиц или нулей подряд.

Снова возьмем наш стандартный прием и рассмотрим частные случаи кодирования, а потом будем определять основные гармоники для каждой из последовательностей: нулей, единиц, чередующихся нулей и единиц.

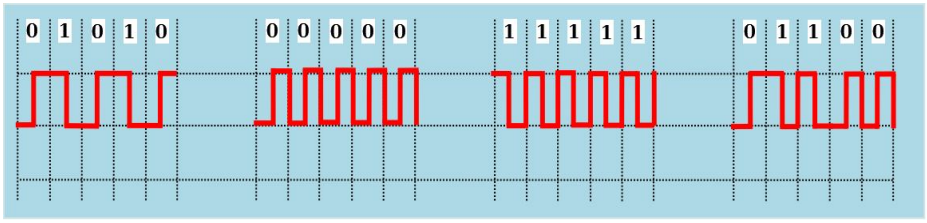


Рис. 36.Применение метода манчестерского кодирования

Во всех случаях можно заметить, что при манчестерском кодировании изменение сигнала в центре каждого бита, позволяет легко выделить синхросигнал. Поэтому манчестерский код и обладает хорошими самосинхронизирующимися свойствами. Самосинхронизация всегда дает возможность передачи больших пакетов информацию без потерь из-за различий тактовой частоты передатчика и приемника.

Определим основную частоту при передаче только единиц или только нулей. Как видно при передаче, как нулей, так и единиц, постоянная составляющая отсутствует. Частота основной гармоники fo=N Гц, как и при биполярном кодировании. Благодаря этому гальваническая развязка сигналов в линиях связи может выполняться простейшими способами, например, с помощью импульсных трансформаторов. При передаче чередующихся единиц и нулей частота основной гармоники равна fo=N/2Гц.

Таким образом, манчестерский код это улучшенный биполярный код, улучшенный за счет использования для передачи данных только двух уровней

сигнала, а в не трех, как в биполярном. Но этот код по-прежнему остается медленным по сравнению с NRZI, который в два раза быстрее.

В качестве примера возьмем для передачи данных линию связи с полосой пропускания 100 МГц и скоростью 100 Мбит. Исходя из этого, определяем, что для передачи данных кодом NRZI нам достаточно диапазона частоты от N/2-N/4 - это частоты от 25 -50 МГц, эти частоты входят в полосу пропускания нашей линии - 100 МГц.

Для манчестерского кода нам нужен диапазон частот от N до N/2 - это частоты от 50 до 100 МГц, в этом диапазоне находятся основные гармоники спектра сигнала. Для кода Манчестера он не удовлетворяет полосе пропускания нашей линии, и, следовательно, такой сигнал линия будет передавать с большими искажениями (такой код нельзя использовать на этой линии).

Дифференциальный манчестерский (Differential Manchester) код.

Как это следует из его названия, является разновидностью манчестерского кодирования. Середину тактового интервала линейного сигнала он использует только для синхронизации, и на ней всегда происходит смена уровня сигнала. Логические 0 и 1 передаются наличием или отсутствием смены уровня сигнала в начале тактового интервала соответственно.

Этот код обладает теми же самыми преимуществами и недостатками, что и манчестерский. Но, на практике используется именно дифференциальный манчестерский код.

Не смотря на все недостатки код Манчестера раньше (когда высокоскоростные линии были большой роскошью для локальной сети) очень активно использовался в локальных сетях, из-за своей самосинхронизации и отсутствия постоянной составляющей. Он и сейчас находит широкое применение в оптоволоконных и электропроводных сетях.

Но в последнее время разработчики пришли к выводу, что лучше все-таки применять потенциальное кодирование, ликвидируя его недостатки средствами, так называемого логического кодирования.

Логическое кодирование

Логическое кодирование выполняется до физического кодирования. Здесь следует подчеркнуть, что на этапе логического кодирования уже не формируется форма сигналов. Здесь просто борются с недостатками методов физического цифрового кодирования - отсутствие синхронизации, наличие постоянной составляющей. Таким образом, сначала с помощью средств логического кодиро-

вания формируются исправленные последовательности двоичных данных, которые потом с помощью методов физического кодирования они передаются по линиям связи.

Логическое кодирование подразумевает замену бит исходной информации новой последовательностью бит, несущей ту же информацию, но обладающей, кроме этого, дополнительными свойствами, например возможностью для приемной стороны обнаруживать ошибки в принятых данных.

Сопровождение каждого байта исходной информации одним битом четности - это пример очень часто применяемого способа логического кодирования при передаче данных с помощью модемов.

Другим примером логического кодирования может служить шифрация данных, обеспечивающая их конфиденциальность при передаче через общественные каналы связи.

Разделяют два метода логического кодирования:

- избыточные коды
- скрэмблирование.

Оба метода относятся к логическому, а не физическому кодированию, так как форму сигналов на линии они не определяют.

Избыточные коды

Избыточные коды основаны на разбиении исходной последовательности бит на порции, которые часто называют символами. Затем каждый исходный символ заменяется на новый, который имеет большее количество бит, чем исходный.

Явный пример избыточного кода - логический код ***4B/5B.***

Логический код 4B/5B заменяет исходные символы длиной в 4 бита на символы длиной в 5 бит. Так как результирующие символы содержат избыточные биты, то общее количество битовых комбинаций в них больше, чем в исходных. Таким образом, пяти-битовая схема дает 32 (два в пятой степени) двухразрядных буквенно-цифровых символа, имеющих значение в десятичном коде от 00 до 31. В то время как исходные данные могут содержать только четыре бита или 16 (два в четвертой степени) символов.

Поэтому в результирующем коде можно подобрать 16 таких комбинаций, которые не содержат большого количества нулей, а остальные считать запрещенными кодами (code violation).

Очевидно, что в этом случае длинные последовательности нулей прерываются, и код становится самосинхронизирующимся для любых передаваемых данных. Исчезает также постоянная составляющая, а значит, еще более сужается спектр сигнала. Но этот метод снижает полезную пропускную способность линии, так как избыточные единицы пользовательской информации не несут.

Избыточные коды позволяют приемнику распознавать искаженные биты. Если приемник принимает запрещенный код, значит, на линии произошло искажение сигнала.

Давайте, еще раз рассмотрим работу логического кода 4B/5B.

Преобразованный сигнал имеет 16 значений для передачи информации и 16 избыточных значений. В декодере приемника пять битов расшифровываются как информационные и служебные сигналы.

Для служебных сигналов отведены девять символов, семь символов - исключены.

Исключены комбинации, имеющие более трех нулей (01 - 00001, 02 - 00010, 03 - 00011, 08 - 01000, 16 - 10000). Такие сигналы интерпретируются символом V и командой приемника VIOLATION - сбой. Команда означает наличие ошибки из-за высокого уровня помех или сбоя передатчика. Единственная комбинация из пяти нулей (00 - 00000) относится к служебным сигналам, означает символ Q и имеет статус QUIET - отсутствие сигнала в линии.

Такое кодирование данных решает две задачи - синхронизации и улучшения помехоустойчивости. Синхронизация происходит за счет исключения последовательности более трех нулей, а высокая помехоустойчивость достигается приемником данных на пяти-битовом интервале. Цена за эти достоинства при таком способе кодирования данных - снижение скорости передачи полезной информации.

К примеру, В результате добавления одного избыточного бита на четыре информационных, эффективность использования полосы частот в протоколах с кодом MLT-3 и кодированием данных 4B/5B уменьшается соответственно на 25%.

Таблица 1.Схема кодирования 4B/5B

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

Соответственно этой таблице формируется код 4B/5B, затем передается по линии с помощью физического кодирования по одному из методов потенциального кодирования, чувствительному только к длинным последовательностям нулей - например, с помощью цифрового кода NRZI. Символы кода 4B/5B длиной 5 бит гарантируют, что при любом их сочетании на линии не могут встретиться более трех нулей подряд.

Буква B в названии кода означает, что элементарный сигнал имеет 2 состояния (от английского binary – двоичный). Имеются также коды и с тремя состояниями сигнала, например, в коде 8B/6T для кодирования 8 бит исходной информации используется код из 6 сигналов, каждый из которых имеет три состояния.

Как мы говорили, логическое кодирование происходит до физического, следовательно, его осуществляют оборудование канального уровня сети: сетевые адаптеры и интерфейсные блоки коммутаторов и маршрутизаторов. Поскольку, как вы сами убедились, использование таблицы перекодировки является очень простой операцией, поэтому метод логического кодирования избыточными кодами не усложняет функциональные требования к этому оборудованию.

Единственное требование - для обеспечения заданной пропускной способности линии передатчик, использующий избыточный код, должен работать с повышенной тактовой частотой. Так, для передачи кодов 4B/5B со скоростью 100 Мб/с передатчик должен работать с тактовой частотой 125 МГц. При этом

спектр сигнала на линии расширяется по сравнению со случаем, когда по линии передается чистый, не избыточный код. Тем не менее, спектр избыточного потенциального кода оказывается уже спектра манчестерского кода, что оправдывает дополнительный этап логического кодирования, а также работу приемника и передатчика на повышенной тактовой частоте.

В результате выше изложенного можно сделать вывод:

В основном для локальных сетей проще, надежней, качественней, быстро действенней -

использовать логическое кодирование данных с помощью избыточных кодов, например, кода 4B/5B, которое устранит длительные последовательности нулей и обеспечит синхронизацию сигнала, потом на физическом уровне использовать для передачи быстрый цифровой код NRZI, нежели без предварительного логического кодирования использовать для передачи данных медленный, но самосинхронизирующийся манчестерский код.

Например, для передачи данных по линии с пропускной способностью 100М бит/с и полосой пропускания 100 МГц, кодом NRZI необходимы частоты 25 - 50 МГц, это без кодирования 4B/5B. А если применить для NRZI еще и кодирование 4B/5B, то теперь полоса частот расширится от 31,25 до 62,5 МГц. Что входит в заданную полосу пропускания линии. А для манчестерского кода без применения всякого дополнительного кодирования необходимы частоты от 50 до 100 МГц, и это частоты основного сигнала, но они уже не будут пропускаться линией на 100 МГц.

Скрэмблирование

Перемешивание данных перед передачей их в линию с помощью потенциального кода является другим способом логического кодирования. Устройства, или блоки, выполняющие такую операцию, называются ***скремблерами*** (scramble - свалка, беспорядочная сборка).

При скремблировании используется определенный алгоритм, поэтому приемник, получив двоичные данные, передает их на дескремблер, который восстанавливает исходную последовательность бит. Избыточные биты при этом по линии не передаются.

Суть скремблирования заключается просто в побитном изменении проходящего через систему потока данных.

Практически единственной операцией, используемой в скремблерах, является XOR - «побитное исключающее ИЛИ», или еще говорят - сложение по модулю 2. В таком методе, при сложении двух единиц исключающим ИЛИ отбрасывается старшая единица и результат записывается - 0.

Метод скрэмблирования очень прост. Сначала придумывают скремблер. Другими словами придумывают по какому соотношению перемешивать биты в исходной последовательности с помощью «исключающего ИЛИ».

Затем согласно этому соотношению из текущей последовательности бит выбираются значения определенных разрядов и складываются по XOR между собой. При этом все разряды сдвигаются на 1 бит, а только что полученное значение («0» или «1») помещается в освободившийся самый младший разряд.

Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом. Затем эта последовательность выдается в линию, где с помощью методов физического кодирования передается к узлу-получателю, на входе которого эта последовательность дескрэмблируется на основе обратного отношения.

Рассмотрим один из примеров скрэмблирования. Например, скремблер может реализовывать следующее соотношение:

$$B_i = A_i \oplus B_{i-3} \oplus B_{i-5}$$

где Bi - двоичная цифра результирующего кода, полученная на i-м такте работы скремблера,

Ai - двоичная цифра исходного кода, поступающая на i-м такте на вход скремблера,

Bi-3 и Bi-5 - двоичные цифры результирующего кода, полученные на предыдущих тактах работы скремблера, соответственно на 3 и на 5 тактов ранее текущего такта. Члены выражения объединены знаком операции исключающего ИЛИ (сложение по модулю 2).

Теперь давайте, определим закодированную последовательность, например, для такой исходной последовательности 110110000001.

Скремблер, определенный выше даст следующий результирующий код:

B1 = A1 = 1 (первые три цифры результирующего кода будут совпадать с исходным, так как еще нет нужных предыдущих цифр)

$$B_1 = A_1 = 1$$
$$B_2 = A_2 = 1$$
$$B_3 = A_3 = 0$$
$$B_4 = A_4 \oplus B_1 = 1 \oplus 1 = 0$$
$$B_5 = A_5 \oplus B_2 = 1 \oplus 1 = 0$$
$$B_6 = A_6 \oplus B_3 \oplus B_1 = 0 \oplus 0 \oplus 1 = 1$$
$$B_7 = A_7 \oplus B_4 \oplus B_2 = 0 \oplus 0 \oplus 1 = 1$$
$$B_8 = A_8 \oplus B_5 \oplus B_3 = 0 \oplus 0 \oplus 0 = 0$$
$$B_9 = A_9 \oplus B_6 \oplus B_4 = 0 \oplus 1 \oplus 0 = 1$$
$$B_{10} = A_{10} \oplus B_7 \oplus B_5 = 0 \oplus 1 \oplus 0 = 1$$
$$B_{11} = A_{11} \oplus B_8 \oplus B_6 = 0 \oplus 0 \oplus 1 = 1$$
$$B_{12} = A_{12} \oplus B_9 \oplus B_7 = 1 \oplus 1 \oplus 1 = 1$$

Таким образом, на выходе скремблера появится последовательность 110001101111. В которой нет последовательности из шести нулей, присутствовавшей в исходном коде!

После получения результирующей последовательности приемник передает ее дескремблеру, который восстанавливает исходную последовательность на основании обратного соотношения.

$$C_i = B_i \oplus B_{i-3} \oplus B_{i-5} = (A_i \oplus B_{i-3} \oplus B_{i-5}) \oplus B_{i-3} \oplus B_{i-5} = A_i$$

Существуют другие различные алгоритмы скрэмблирования, они отличаются количеством слагаемых, дающих цифру результирующего кода, и сдвигом между слагаемыми.

Как видим, устройство скремблера предельно просто. Более того, тот факт, что каждый бит выходной последовательности зависит только от одного входного бита, еще более упрочило положение скремблеров в защите потоковой передачи данных.

Главная проблема кодирования на основе скремблеров - синхронизация передающего (кодирующего) и принимающего (декодирующего) устройств. При пропуске или ошибочном вставлении хотя бы одного бита вся передаваемая информация необратимо теряется. Поэтому, в системах кодирования на основе скремблеров очень большое внимание уделяется методам синхронизации.

На практике для этих целей обычно применяется комбинация двух методов:

а) добавление в поток информации синхронизирующих битов, заранее известных приемной стороне, что позволяет ей при не нахождении такого бита активно начать поиск синхронизации с отправителем,

б) использование высокоточных генераторов временных импульсов, что позволяет в моменты потери синхронизации производить декодирование принимаемых битов информации «по памяти» без синхронизации.

Существуют и более простые методы борьбы с последовательностями единиц, также относимые к классу скрэмблирования. Напомню, что все методы логического кодирования направлены на устранение недостатков методов физического цифрового кодирования.

Для улучшения кода Bipolar AMI используются два метода, основанные на искусственном искажении последовательности нулей запрещенными символами.

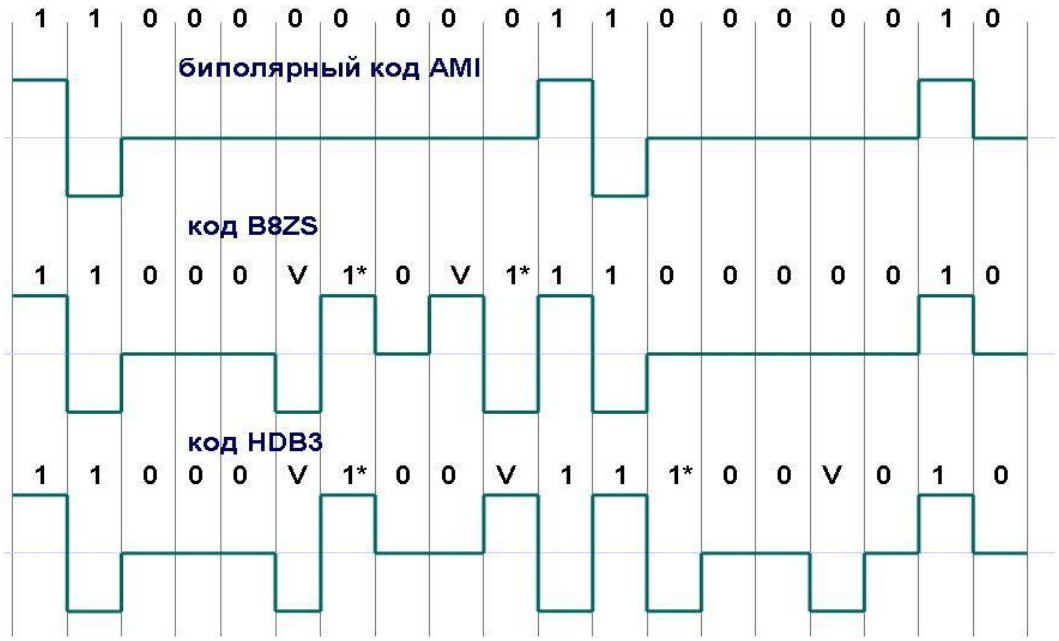


Рис. 37. Использование метода B8ZS и метода HDB3 для корректировки кода AMI

Исходный код состоит из двух длинных последовательностей нулей: в первом случае - из 8, а во втором - из 5.

Код B8ZS (Bipolar with 8-Zeros Substitution) исправляет только последовательности, состоящие из 8 нулей. Для этого он после первых трех нулей вместо оставшихся пяти нулей вставляет пять цифр: V-1*-0-V-1*.

V здесь обозначает сигнал единицы, запрещенной для данного такта полярности, то есть сигнал, не изменяющий полярность предыдущей единицы, 1* - сигнал единицы корректной полярности, а знак звездочки отмечает тот факт, что в исходном коде в этом такте была не единица, а ноль.

В результате на 8 тактах приемник наблюдает 2 искажения - очень маловероятно, что это случилось из-за шума на линии или других сбоев передачи. Поэтому приемник считает такие нарушения кодировкой 8 последовательных нулей, и после приема заменяет их на исходные 8 нулей.

Код B8ZS построен так, что его постоянная составляющая равна нулю при любых последовательностях двоичных цифр.

Код HDB3 (High-Density Bipolar 3-Zeros) исправляет любые четыре подряд идущих нуля в исходной последовательности.

Правила формирования кода HDB3 более сложные, чем кода B8ZS. Каждые четыре нуля заменяются четырьмя сигналами, в которых имеется один сигнал V. Для подавления постоянной составляющей полярность сигнала V чередуется при последовательных заменах.

Кроме того, для замены используются два образца четырехтактовых кодов. Если перед заменой исходный код содержал нечетное число единиц, то используется последовательность 000V, а если число единиц было четным - последовательность 1*00V.

Улучшенные потенциальные коды обладают достаточно узкой полосой пропускания для любых последовательностей единиц и нулей, которые встречаются в передаваемых данных. В результате коды, полученные из потенциального путем логического кодирования, обладают более узким спектром, чем манчестерский, даже при повышенной тактовой частоте. Этим объясняется применение потенциальных избыточных и скрэмблированных кодов в современных технологиях вместо манчестерского и биполярного импульсного кодирования.

Компрессия данных

Компрессия (сжатие) данных применяется для сокращения времени их передачи. Так как на компрессию данных передающая сторона тратит дополнительное время, к которому нужно еще прибавить аналогичные затраты времени на декомпрессию этих данных принимающей стороной, то выгоды от сокращения времени на передачу сжатых данных обычно бывают заметны только для низкоскоростных каналов. Этот порог скорости для современной аппаратуры составляет около 64 Кбит/с. Многие программные и аппаратные средства сети способны выполнять динамическую компрессию данных в отличие от статической, когда данные предварительно компрессируются (например, с помощью

популярных архиваторов типа WinZip, WinRAR и т.п.), а уже затем отсылаются в сеть.

На практике может использоваться ряд алгоритмов компрессии, каждый из которых применим к определенному типу данных. Некоторые модемы (называемые интеллектуальными) предлагают адаптивную компрессию, при которой в зависимости от передаваемых данных выбирается определенный алгоритм компрессии. Рассмотрим некоторые из общих алгоритмов компрессии данных.

Десятичная упаковка.

Когда данные состоят только из чисел, значительную экономию можно получить путем уменьшения количества используемых на цифру бит с 7 до 4, используя простое двоичное кодирование десятичных цифр вместо кода ASCII. Просмотр таблицы ASCII показывает, что старшие три бита всех кодов десятичных цифр содержат комбинацию 011. Если все данные в кадре информации состоят из десятичных цифр, то, поместив в заголовок кадра соответствующий управляющий символ, можно существенно сократить длину кадра.

Относительное кодирование.

Альтернативой десятичной упаковке при передаче числовых данных с небольшими отклонениями между последовательными цифрами является передача только этих отклонений вместе с известным опорным значением. Такой метод используется, в частности, в методе цифрового кодирования голоса ADPCM, передающем в каждом такте только разницу между соседними замерами голоса.

Символьное подавление.

Часто передаваемые данные содержат большое количество повторяющихся байт. Например, при передаче черно-белого изображения черные поверхности будут порождать большое количество нулевых значений, а максимально освещенные участки изображения - большое количество байт, состоящих из всех единиц. Передатчик сканирует последовательность передаваемых байт и, если обнаруживает последовательность из трех или более одинаковых байт, заменяет ее специальной трехбайтовой последовательностью, в которой указывает значение байта, количество его повторений, а также отмечает начало этой последовательности специальным управляющим символом.

Коды переменной длины.

В этом методе кодирования используется тот факт, что не все символы в передаваемом кадре встречаются с одинаковой частотой. Поэтому во многих схемах кодирования коды часто встречающихся символов заменяют кодами

меньшей длины, а редко встречающихся - кодами большей длины. Такое кодирование называется также ***статистическим кодированием***. Из-за того, что символы имеют различную длину, для передачи кадра возможна только бит-ориентированная передача.

При статистическом кодировании коды выбираются таким образом, чтобы при анализе последовательности бит можно было бы однозначно определить соответствие определенной порции бит тому или иному символу или же запрещенной комбинации бит. Если данная последовательность бит представляет собой запрещенную комбинацию, то необходимо к ней добавить еще один бит и повторить анализ. Например, если при неравномерном кодировании для наиболее часто встречающегося символа «Р» выбран код 1, состоящий из одного бита, то значение 0 однобитного кода будет запрещенным. Иначе мы сможем закодировать только два символа. Для другого часто встречающегося символа «О» можно использовать код 01, а код 00 оставить как запрещенный. Тогда для символа «А» можно выбрать код 001, для символа «П» - код 0001 и т. п.

Вообще, неравномерное кодирование наиболее эффективно, когда неравномерность распределения частот передаваемых символов достаточна велика, как при передаче длинных текстовых строк. Напротив, при передаче двоичных данных, например кодов программ, оно малоэффективно, так как 8-битовые коды при этом распределены почти равномерно.

Одним из наиболее распространенных алгоритмов, на основе которых строятся неравномерные коды, является алгоритм Хаффмана, позволяющий строить коды автоматически, на основании известных частот символов. Существуют адаптивные модификации метода Хаффмана, которые позволяют строить дерево кодов «на ходу», по мере поступления данных от источника.

Многие модели коммуникационного оборудования, такие как модемы, мосты, коммутаторы и маршрутизаторы, поддерживают протоколы динамической компрессии, позволяющие сократить объем передаваемой информации в 4, а иногда и в 8 раз. В таких случаях говорят, что протокол обеспечивает коэффициент сжатия 1:4 или 1:8. Существуют стандартные протоколы компрессии, например V.42bis, а также большое количество нестандартных, фирменных протоколов. Реальный коэффициент компрессии зависит от типа передаваемых данных, так, графические и текстовые данные обычно сжимаются хорошо, а коды программ - хуже.

Обеспечение достоверности передачи информации

Проблема обеспечения безошибочности (***достоверности)*** передачи информации в сетях имеет очень большое значение. Если при передаче обычной телеграммы возникает в тексте ошибка или при разговоре по телефону слышен треск, то в большинстве случаев ошибки и искажения легко обнаруживаются по

смыслу. Но при передаче данных одна ошибка (искажение одного бита) на тысячу переданных сигналов может серьезно отразиться на качестве информации.

Существует множество методов обеспечения достоверности передачи информации (методов защиты от ошибок), отличающихся по используемым для их реализации средствам, по затратам времени на их применение на передающем и приемном пунктах, по затратам дополнительного времени на передачу фиксированного объема данных (оно обусловлено изменением объема трафика пользователя при реализации данного метода), по степени обеспечения достоверности передачи информации. Практическое воплощение методов состоит из двух частей – программной и аппаратной. Соотношение между ними может быть самым различным, вплоть до почти полного отсутствия одной из частей. Чем больше удельный вес аппаратных средств по сравнению с программными, тем при прочих равных условиях сложнее оборудование, реализующее метод, и меньше затрат времени на его реализацию, и наоборот.

Выделяют две основные причины возникновения ошибок при передаче информации в сетях:

- сбои в какой-то части оборудования сети или возникновение неблагоприятных объективных событий в сети (например, коллизий при использовании метода случайного доступа в сеть). Как правило, система передачи данных готова к такого рода проявлениям и устраняет их с помощью планово предусмотренных средств;
- помехи, вызванные внешними источниками и атмосферными явлениями.

Помехи – это электрические возмущения, возникающие в самой аппаратуре или попадающие в нее извне.

Наиболее распространенными являются флуктуационные (случайные) помехи. Они представляют собой последовательность импульсов, имеющих случайную амплитуду и следующих друг за другом через различные промежутки времени. Примерами таких помех могут быть атмосферные и индустриальные помехи, которые обычно проявляются в виде одиночных импульсов малой длительности и большой амплитуды. Возможны и сосредоточенные помехи в виде синусоидальных колебаний. К ним относятся сигналы от посторонних радиостанций, излучения генераторов высокой частоты. Встречаются и смешанные помехи. В приемнике помехи могут настолько ослабить информационный сигнал, что он либо вообще не будет обнаружен, либо искажен так, что «единица» может перейти в «нуль» и наоборот.

Трудности борьбы с помехами заключаются в беспорядочности, нерегулярности и в структурном сходстве помех с информационными сигналами. Поэтому защита информации от ошибок и вредного влияния помех имеет большое

практическое значение и является одной из серьезных проблем современной теории и техники связи.

Среди многочисленных методов защиты от ошибок выделяются три группы методов: групповые методы, помехоустойчивое кодирование и методы защиты от ошибок в системах передачи с обратной связью.

Из групповых методов получили широкое применение ***мажоритарный метод***, реализующий принцип Вердана, и метод передачи информационными блоками с количественной характеристикой блока.

Суть ***мажоритарного метода***, давно используемого в телеграфии, состоит в следующем. Каждое сообщение ограниченной длины передается несколько раз, чаще всего три раза. Принимаемые сообщения запоминаются, а потом производится их поразрядное сравнение. Суждение о правильности передачи выносится по совпадению большинства из принятой информации методом «два из трех». Например, кодовая комбинация 01101 при трехразовой передаче была частично искажена помехами, поэтому приемник принял такие комбинации: 10101, 01110, 01001. В результате проверки каждой позиции отдельно правильной считается комбинация 01101.

Другой групповой метод, также не требующий перекодирования информации, предполагает передачу данных блоками с количественной характеристикой блока.

Такими характеристиками могут быть: число единиц или нулей в блоке, контрольная сумма передаваемых символов в блоке, остаток от деления контрольной суммы на постоянную величину и др. На приемном пункте эта характеристика вновь подсчитывается и сравнивается с переданной по каналу связи. Если характеристики совпадают, считается, что блок не содержит ошибок. В противном случае на передающую сторону передается сигнал с требованием повторной передачи блока.

Помехоустойчивое (избыточное) кодирование, предполагающее разработку и использование корректирующих (помехоустойчивых) кодов, применяется для защиты от ошибок при передаче информации между устройствами. Оно позволяет получить более высокие качественные показатели работы систем связи. Его основное назначение – в обеспечении малой вероятности искажений передаваемой информации, несмотря на присутствие помех или сбоев в работе сети.

Существует довольно большое количество различных помехоустойчивых кодов, отличающихся друг от друга по ряду показателей и. прежде всего по своим корректирующим возможностям.

К числу наиболее важных показателей корректирующих кодов относятся:

- значность кода, или длина кодовой комбинации, включающей информационные символы (m) и проверочные, или контрольные символы (К). Обычно значность кода n есть сумма m+К;

- избыточность кода Кизб, выражаемая отношением числа контрольных символов в кодовой комбинации к значности кода;
- корректирующая способность кода Ккс, представляющая собой отношение числа кодовых комбинаций L, в которых ошибки были обнаружены и исправлены, к общему числу переданных кодовых комбинаций M в фиксированном объеме информации.

При выборе кода надо стремиться, чтобы он имел меньшую избыточность. Чем больше коэффициент ***Кизб***, тем менее эффективно используется пропускная способность канала связи и больше затрачивается времени на передачу информации, но зато выше помехоустойчивость системы.

Корректирующие коды в основном применяются для обнаружения ошибок, исправление которых осуществляется путем повторной передачи искаженной информации. С этой целью в сетях используются системы передачи с обратной связью (наличие между абонентами дуплексной связи облегчает применение таких систем).

Системы передачи с обратной связью делятся на системы с решающей обратной связью и системы с информационной обратной связью.

Особенностью систем ***с решающей обратной связью (системы с переапросом)*** является то, что решение о необходимости повторной передачи информации (сообщения, пакета) принимает приемник. Здесь обязательно применяется помехоустойчивое кодирование, с помощью которого на приемной станции осуществляется проверка принимаемой информации. При обнаружении ошибки на передающую сторону по каналу обратной связи посылается сигнал пере запроса, по которому информация передается повторно. Канал обратной связи используется также для посылки сигнала подтверждения правильности приема, автоматически определяющего начало следующей передачи.

В системах ***с информационной обратной связью*** передача информации осуществляется без помехоустойчивого кодирования. Приемник, приняв информацию по прямому каналу и зафиксировав ее в своей памяти, передает ее в полном объеме по каналу обратной связи передатчику, где переданная и возвращенная информация сравниваются. При совпадении передатчик посылает приемнику сигнал подтверждения, в противном случае происходит повторная передача всей информации. Таким образом, здесь решение о необходимости повторной передачи принимает передатчик.

Обе рассмотренные системы обеспечивают практически одинаковую достоверность, однако, в системах с решающей обратной связью пропускная способность каналов используется эффективнее, поэтому они получили большее распространение.

1.13. Методы коммутации

Любые сети связи поддерживают некоторый способ коммутации своих абонентов между собой. Этими абонентами могут быть удаленные компьютеры, локальные сети, факс-аппараты или просто собеседники, общающиеся с помощью телефонных аппаратов. Практически невозможно предоставить каждой паре взаимодействующих абонентов свою собственную некоммутируемую физическую линию связи, которой они могли бы монопольно «владеть» в течение длительного времени. Поэтому в любой сети всегда применяется какой-либо способ коммутации абонентов, который обеспечивает доступность имеющихся физических каналов одновременно для нескольких сеансов связи между абонентами сети.

Коммутация— процесс соединения абонентов коммуникационной сети через транзитные узлы. **Коммуникационные сети** должны обеспечивать связь своих абонентов между собой. Абонентами могут выступать ЭВМ, сегменты локальных сетей, факс-аппараты или телефонные собеседники.

Сетевой коммутатор или свитч, свич (жарг. от англ. switch— переключатель)— устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. В отличие от **концентратора**, который распространяет трафик от одного подключенного устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю, исключение составляет широковещательный трафик (на MAC-адрес FF:FF:FF:FF:FF:FF) всем узлам сети. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Коммутатор работает на канальном уровне модели OSI, и потому в общем случае может только объединять узлы одной сети по их MAC-адресам.

Абоненты соединяются с коммутаторами индивидуальными линиями связи, каждая из которых используется в любой момент времени только одним, закрепленным за этой линией абонентом. Между коммутаторами линии связи разделяются несколькими абонентами, то есть используются совместно.

Существуют три принципиально различные схемы коммутации абонентов в сетях: **коммутация каналов (circuit switching), коммутация пакетов (packet switching) и коммутация сообщений (message switching).** Сети с коммутацией каналов имеют более богатую историю, они ведут свое происхождение от первых телефонных сетей. Сети с коммутацией пакетов сравнительно молоды, они появились в конце 60-х годов как результат экспериментов с первыми глобальными компьютерными сетями. Сети с коммутацией сообщений послужили прототипом современных сетей с коммутацией пакетов и сегодня

они в чистом виде практически не существуют. Каждая из этих схем имеет свои преимущества и недостатки, но по долгосрочным прогнозам многих специалистов будущее принадлежит технологии коммутации пакетов, как более гибкой и универсальной.

Как сети с ***коммутацией пакетов***, так и сети **с *коммутацией каналов*** можно разделить на два класса по другому признаку - на сети с ***динамической коммутацией*** и сети с ***постоянной коммутацией***.

В первом случае сеть разрешает устанавливать соединение по инициативе пользователя сети. Коммутация выполняется на время сеанса связи, а затем (опять же по инициативе одного из взаимодействующих пользователей) связь разрывается. В общем случае любой пользователь сети может соединиться с любым другим пользователем сети. Обычно период соединения между парой пользователей при динамической коммутации составляет от нескольких секунд до нескольких часов и завершается при выполнении определенной работы - передачи файла, просмотра страницы текста или изображения и т. п.

Во втором случае сеть не предоставляет пользователю возможность выполнить динамическую коммутацию с другим произвольным пользователем сети. Вместо этого сеть разрешает паре пользователей заказать соединение на длительный период времени. Соединение устанавливается не пользователями, а персоналом, обслуживающим сеть. Время, на которое устанавливается постоянная коммутация, измеряется обычно несколькими месяцами. Режим постоянной коммутации в сетях с коммутацией каналов часто называется сервисом ***выделенных (dedicated)*** или ***арендуемых (leased) каналов.***

Примерами сетей, поддерживающих режим динамической коммутации, являются телефонные сети общего пользования, локальные сети, сети TCP/IP.

Наиболее популярными сетями, работающими в режиме постоянной коммутации, сегодня являются сети технологии SDH, на основе которых строятся выделенные каналы связи с пропускной способностью в несколько гигабит в секунду.

Некоторые типы сетей поддерживают оба режима работы. Например, сети X.25 и ATM могут предоставлять пользователю возможность динамически связаться с любым другим пользователем сети и в то же время отправлять данные по постоянному соединению одному вполне определенному абоненту.

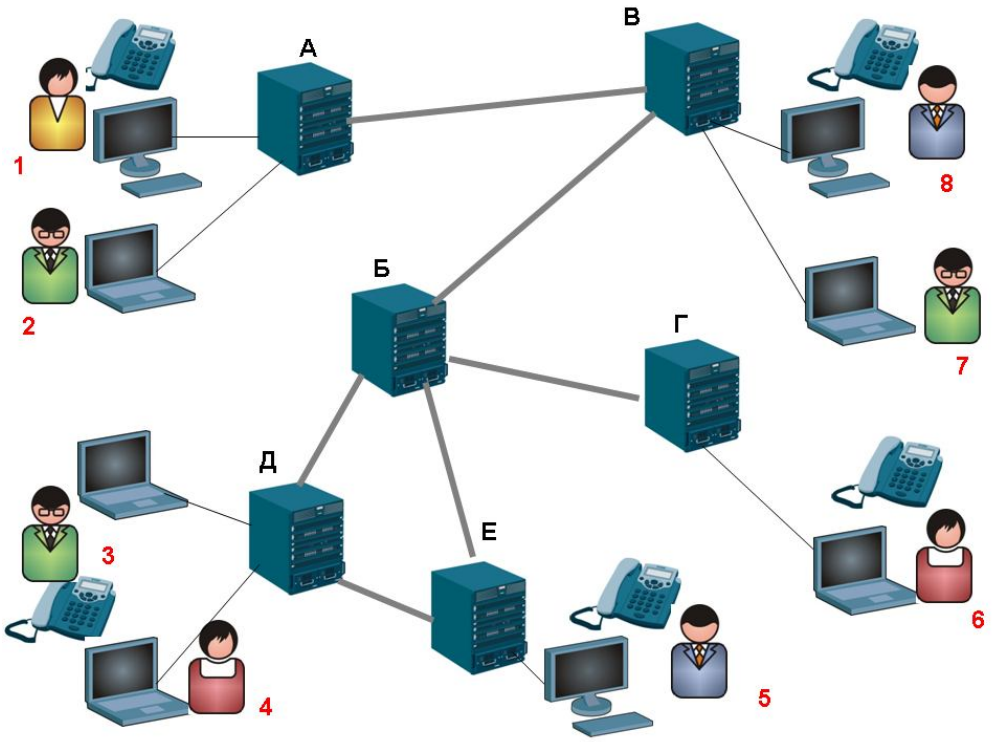


Рис. 38.Общая структура сети с коммутацией узлов (абонентов).

Коммутация каналов

Коммутация каналов подразумевает образование непрерывного составного физического канала из последовательно соединенных отдельных канальных участков для прямой передачи данных между узлами. Отдельные каналы соединяются между собой специальной аппаратурой - *коммутаторами,* которые могут устанавливать связи между любыми конечными узлами сети. В сети с коммутацией каналов перед передачей данных всегда необходимо выполнить процедуру установления соединения, в процессе которой и создается ***составной канал***.

Например, если сеть, изображенная на рис.38, работает по технологии коммутации каналов, то узел (абонент) 1, чтобы передать данные узлу (абоненту) 6, прежде всего, должен передать специальный запрос на установление соединения коммутатору А, указав адрес назначения 6. Коммутатор А должен выбрать маршрут образования составного канала, а затем передать запрос следующему коммутатору, в данном случае В. Затем коммутатор В передает запрос коммутатору Б, далее коммутатор Б передаёт запрос коммутатору Г, а тот, в свою очередь, передает запрос узлу (абоненту). Если узел (абонент) 6 принимает запрос на установление соединения, он направляет по уже установленному каналу ответ исходному узлу, после чего составной канал считается скомму-

тированным и узлы 1 и 6 могут обмениваться по нему данными, например, вести телефонный разговор.

Коммутаторы, а также соединяющие их каналы должны обеспечивать одновременную передачу данных нескольких абонентских каналов. Для этого они должны быть высокоскоростными и поддерживать какую-либо технику ***мультиплексирования абонентских каналов.***

В настоящее время для мультиплексирования абонентских каналов используются две техники:

- техника частотного мультиплексирования (Frequency Division Multiplexing, FDM);
- техника мультиплексирования с разделением времени (Time Division Multiplexing, TDM).

Мультиплексирование (англ. multiplexing, muxing)— уплотнение канала, т.е. передача нескольких потоков (каналов) данных с меньшей скоростью (пропускной способностью) по одному каналу, при помощи устройства под названием ***мультиплексор***.

Мультиплексор — комбинационное устройство, обеспечивающее передачу в желаемом порядке цифровой информации, поступающей по нескольким входам на один выход. Может быть реализован как аппаратно так и программно.

Технология TDM

Первой стали применять технологию TDM, которая широко используется в обычных системах электросвязи. Эта технология предусматривает объединение нескольких входных низкоскоростных каналов в один составной высокоскоростной канал.

Мультиплексирование с разделением времени (англ. Time Division Multiplexing, TDM)— технология аналогового или цифрового мультиплексирования в котором два и более сигнала или битовых потока передаются одновременно как подканалы в одном коммуникационном канале. Передача дан-

Аппаратура TDM-сетей (мультиплексоры, коммутаторы, демультиплексоры) - работает в режиме разделения времени, поочередно обслуживая в течение

цикла своей работы все абонентские каналы. Цикл работы оборудования TDM равен 125 мкс, что соответствует периоду следования замеров голоса в цифровом абонентском канале. Это значит, что мультиплексор или коммутатор успевает вовремя обслужить любой абонентский канал и передать его очередной замер далее по сети. Каждому соединению выделяется один квант времени цикла работы аппаратуры, называемый также тайм-слотом. Длительность тайм-слота зависит от числа абонентских каналов, обслуживаемых мультиплексором TDM или коммутатором.

Мультиплексор принимает информацию по N входным каналам от конечных абонентов, каждый из которых передает данные по абонентскому каналу со скоростью 64 Кбит/с - 1 байт каждые 125 мкс.

В каждом цикле мультиплексор выполняет следующие действия:

- прием от каждого канала очередного байта данных;
- составление из принятых байтов уплотненного кадра, называемого также обоймой;
- передача уплотненного кадра на выходной канал с битовой скоростью, равной N*64 Кбит/с.

Порядок байт в обойме соответствует номеру входного канала, от которого этот байт получен. Количество обслуживаемых мультиплексором абонентских каналов зависит от его быстродействия. Например, мультиплексор T1, представляющий собой первый промышленный мультиплексор, работавший по технологии TDM, поддерживает 24 входных абонентских канала, создавая на выходе обоймы стандарта T1, передаваемые с битовой скоростью 1,544 Мбит/с.

Демультиплексор выполняет обратную задачу - он разбирает байты уплотненного кадра и распределяет их по своим нескольким выходным каналам, при этом он считает, что порядковый номер байта в обойме соответствует номеру выходного канала.

Коммутатор принимает уплотненный кадр по скоростному каналу от мультиплексора и записывает каждый байт из него в отдельную ячейку своей буферной памяти, причем в том порядке, в котором эти байты были упакованы в уплотненный кадр. Для выполнения операции коммутации байты извлекаются из буферной памяти не в порядке поступления, а в таком порядке, который соответствует поддерживаемым в сети соединениям абонентов.

Однажды выделенный номер тайм-слота остается в распоряжении соединения «входной канал-выходной слот» в течение всего времени существования этого соединения, даже если передаваемый трафик является пульсирующим и не всегда требует захваченного количества тайм-слотов. Это означает, что соединение в сети TDM всегда обладает известной и фиксированной пропускной способностью, кратной 64 Кбит/с.

Работа оборудования TDM напоминает работу сетей с коммутацией пакетов, так как каждый байт данных можно считать некоторым элементарным пакетом. Однако, в отличие от пакета компьютерной сети, «пакет» сети TDM не имеет индивидуального адреса. Его адресом является порядковый номер в обойме или номер выделенного тайм-слота в мультиплексоре или коммутаторе. Сети, использующие технику TDM, требуют синхронной работы всего оборудования, что и определило второе название этой техники - синхронный режим передач (STM). Нарушение синхронности разрушает требуемую коммутацию абонентов, так как при этом теряется адресная информация. Поэтому перераспределение тайм-слотов между различными каналами в оборудовании TDM невозможно, даже если в каком-то цикле работы мультиплексора тайм-слот одного из каналов оказывается избыточным, так как на входе этого канала в этот момент нет данных для передачи (например, абонент телефонной сети молчит).

Существует модификация техники TDM, называемая статистическим разделением канала во времени (Statistical TDM, STDM). Эта техника разработана специально для того, чтобы с помощью временно свободных тайм-слотов одного канала можно было увеличить пропускную способность остальных. Для решения этой задачи каждый байт данных дополняется полем адреса небольшой длины, например в 4 или 5 бит, что позволяет мультиплексировать 16 или 32 канала. Однако техника STDM не нашла широкого применения и используется в основном в нестандартном оборудовании подключения терминалов к мэйнфреймам. Развитием идей статистического мультиплексирования стала технология асинхронного режима передачи - ATM, которая вобрала в себя лучшие черты техники коммутации каналов и пакетов.

Сети TDM могут поддерживать либо режим динамической коммутации, либо режим постоянной коммутации, а иногда и оба эти режима. Так, например, основным режимом цифровых телефонных сетей, работающих на основе технологии TDM, является динамическая коммутация, но они поддерживают также и постоянную коммутацию, предоставляя своим абонентам службу выделенных каналов.

Существует аппаратура, которая поддерживает только режим постоянной коммутации. К ней относится оборудование типа T1/E1, а также высокоскоростное оборудование SDH. Такое оборудование используется для построения первичных сетей, основной функцией которых является создание выделенных каналов между коммутаторами, поддерживающими динамическую коммутацию.

Сегодня практически все данные - голос, изображение, компьютерные данные - передаются в цифровой форме. Поэтому выделенные каналы TDM-технологии, которые обеспечивают нижний уровень для передачи цифровых данных, являются универсальными каналами для построения сетей любого типа: телефонных, телевизионных и компьютерных.

Использование технологии TDM при использовании волоконно-оптических линий позволило увеличить пропускную способность этих линий связи до 10 Гбит/с. Выше этой скорости некоторые основные характеристики оптического волокна (например: поляризационная модовая дисперсия, хроматическая дисперсия) начинают значительно влиять на качество передачи и должны приниматься во внимание при разработке систем связи. Это является серьезным препятствием для ведущихся в настоящее время разработок систем TDM со скоростями передачи 40 Гбит/с и выше. Кроме того, для дальнейшего увеличения скорости требуются новые методы модуляции лазерного излучения, что ведет к росту сложности и стоимости приемо-передающего оборудования.

Хроматической дисперсией называют как зависимость эффективного показателя преломления от длины волны, так и ее следствие – увеличение ширины оптических импульсов при их распространении по волокну.

Поляризационная модовая дисперсия PMD (Polarization Mode Dispersion), также как и хроматическая дисперсия, приводит к уширению импульсов и начинает заметно влиять на качество передачи при высоких скоростях (частотах модуляции). PMD возникает из-за того, что оптическое излучение с различными состояниями поляризации оптического сигнала SOP (State of Polarization) распространяется вдоль волокна с различными скоростями.

Применение методов, уменьшающих влияние хроматической дисперсии, ведет к увеличению потерь, стоимости и сложности системы. Для стандартного ступенчатого одномодового волокна (G.652 по классификации ITU) максимальная дальность передачи со скоростью 10 Гбит/с без компенсации и коррекции дисперсии составляет 50-75 км. Независимо от того, станет ли технология TDM универсальным протоколом, таким как IP, или будет адаптирована в соответствии со стандартами SONET/SDH, в ближайшие годы ее будут использовать многие операторы.

WDM системы

Для повышения пропускной способности, вместо увеличения скорости передачи в едином составном канале, как это реализовано в технологии TDM, в технологии WDM увеличивают число каналов (длин волн), применяемых в системах передачи по ВОЛС. Такая техника относится к методу FDM, однако для оптических кабелей она получила название разделения по длине волны ***(Wave Division Multiplexing, WDM).***

Исторически первыми возникли двухволновые WDM системы, работающие на центральных длинах волн из второго и третьего окон прозрачности кварцевого волокна (1310 и 1550 нм). Главным достоинством таких систем яв-

ляется то, что из-за большого спектрального разноса полностью отсутствует влияние каналов друг на друга. Это способ позволяет либо удвоить скорость передачи по одному оптическому волокну, либо организовать дуплексную связь.

Спектральное уплотнение каналов (англ. Wavelength-division multiplexing, WDM, буквально мультиплексирование с разделением по длине волны)— технология, позволяющая одновременно передавать несколько информационных каналов по одному оптическому волокну на разных несущих частотах.

Современные WDM системы на основе стандартного частотного плана (ITU-T Rec. G.692) можно подразделить на три группы:

грубые WDM (Coarse WDM— CWDM)— системы с частотным разносом каналов не менее 200 ГГц, позволяющие мультиплексировать не более 18 каналов. (Используемые в настоящее время CWDM работают в полосе от 1270нм до 1610нм, промежуток между каналами 20нм(200ГГц), можно мультиплексировать 16 спектральных каналов.)

плотные WDM (Dense WDM— DWDM)— системы с разносом каналов не менее 100 ГГц, позволяющие мультиплексировать не более 40 каналов.

высокоплотные WDM (High Dense WDM— HDWDM)— системы с разносом каналов 50 ГГц и менее, позволяющие мультиплексировать не менее 64 каналов.

Частотный план для CWDM систем определяется стандартом ITU G.694.2. Область применения технологии CWDM— городские сети с расстоянием до 50 км. Достоинством этого вида WDM систем является низкая (по сравнению с остальными типами) стоимость оборудования вследствие меньших требований к компонентам.

Частотный план для DWDM систем определяется стандартом ITU G.694.1. Область применения— магистральные сети. Этот вид WDM систем предъявляет более высокие требования к компонентам, чем CWDM (ширина спектра источника излучения, температурная стабилизация источника и т.д.). Толчок к бурному развитию DWDM сетей дало появление недорогих и эффективных волоконных эрбиевых усилителей (EDFA), работающих в промежутке от 1525 до 1565 нм (третье окно прозрачности кварцевого волокна).

Технология WDM позволяет существенно увеличить пропускную способность канала, причем она позволяет использовать уже проложенные волоконно-оптические линии. Благодаря WDM удается организовать двустороннюю многоканальную передачу трафика по одному волокну (в обычных линиях используется пара волокон— для передачи в прямом и обратном направлениях). Рост

пропускной способности при использовании технологии WDM осуществляется без дорогостоящей замены оптического кабеля. Применение технологии WDM позволяет сдавать в аренду не только оптические кабели или волокна, но и отдельные длины волн, то есть реализовать концепцию “виртуального волокна”. По одному волокну на разных длинах волн можно одновременно передавать самые разные приложения – кабельное телевидение, телефонию, трафик Интернет, “видео по требованию” и т.д. Как следствие этого, часть волокон в оптическом кабеле можно использовать для резерва.

Применение технологии WDM позволяет исключить дополнительную прокладку оптических кабелей в существующей сети. Даже если в будущем стоимость волокна уменьшится за счет использования новых технологий, волоконно-оптическая инфраструктура (проложенное волокно и установленное оборудование) всегда будет стоить достаточно дорого. Для ее эффективного использования, необходимо иметь возможность в течение долгого времени увеличивать пропускную способность сети и менять набор предоставляемых услуг без замены оптического кабеля. Технология WDM предоставляет именно такую возможность.

Совместное применение технологий TDM и WDM позволяет значительно расширить спектр предоставляемых услуг, оставляя практически без изменений большую часть имеющегося оборудования. Применение технологии WDM дает многочисленные преимущества, однако требует высокого уровня подготовки технического персонала и современного контрольно-измерительного оборудования.

Система DWDM во многом похожа на традиционную систему TDM. Сигналы разных длин волн, генерируемые одним или несколькими оптическими передатчиками, объединяются мультиплексором в многоканальный составной оптический сигнал, который далее распространяется по оптическому волокну. При больших расстояниях передачи на линии связи устанавливается один или несколько оптических повторителей. Демультиплексор принимает составной сигнал, выделяет из него исходные каналы разных длин волн и направляет их на соответствующие фотоприемники. На промежуточных узлах некоторые каналы могут быть добавлены или выделены из составного сигнала посредством мультиплексоров ввода/вывода или устройств кросс-коммутации.

Главным отличием систем DWDM от систем TDM является то, что в системе DWDM передача ведется на нескольких длинах волн. Важно отметить, что на каждой длине волны в системе DWDM может передаваться мультиплексированный сигнал систем TDM. Система DWDM в общем случае состоит из одного или нескольких лазерных передатчиков, мультиплексора, одного или нескольких усилителей EDFA, мультиплексоров ввода/вывода, оптического волокна (кабеля), демультиплексора и соответствующего числа фотоприемников, а также электронного оборудования, которое обрабатывает передаваемые данные в соответствии с используемыми протоколами связи, и системы сетевого управления.

Хотя к оконечному электронному оборудованию для отдельных каналов WDM и предъявляются определенные требования, как и в системах TDM, все остальное оборудование в канале может поддерживать только скорость передачи по этому каналу, а не полную скорость составного сигнала. Таким образом, полная пропускная способность линии связи не ограничена скоростью работы используемых электронных устройств. При необходимости, полную пропускную способность можно увеличить в любой момент, просто добавив в существующую систему WDM несколько каналов. Самую быструю линию связи TDM, которую только можно создать с использованием наиболее современной техники, в системе WDM можно передавать как один из многих каналов. Технология WDM позволяет достичь суммарной скорости передачи по линии связи, которая сопоставима с огромной пропускной способностью, предоставляемой оптическим волокном

Обеспечение дуплексного режима работы на основе технологий FDM, TDM и WDM.

В зависимости от направления возможной передачи данных способы передачи данных по линии связи делятся на следующие типы:

- *симплексный* - передача осуществляется по линии связи только в одном направлении;
- *полудуплексный* - передача ведется в обоих направлениях, но попеременно во времени.
- *дуплексный* - передача ведется одновременно в двух направлениях.

Дуплексный режим - наиболее универсальный и производительный способ работы канала. Самым простым вариантом организации дуплексного режима является использование двух независимых физических каналов (двух пар проводников или двух световодов) в кабеле, каждый из которых работает в симплексном режиме, то есть передает данные в одном направлении. Именно такая идея лежит в основе реализации дуплексного режима работы во многих сетевых технологиях, например Fast Ethernet или ATM.

Иногда такое простое решение оказывается недоступным или неэффективным. Чаще всего это происходит в тех случаях, когда для дуплексного обмена данными имеется всего один физический канал, а организация второго связана с большими затратами. Например, при обмене данными с помощью модемов через телефонную сеть у пользователя имеется только один физический канал связи с АТС - двухпроводная линия, и приобретать второй вряд ли целесообразно. В таких случаях дуплексный режим работы организуется на основе раз-

деления канала на два логических подканала с помощью техники FDM или TDM.

Модемы для организации дуплексного режима работы на двухпроводной линии применяют технику FDM. Модемы, использующие частотную модуляцию, работают на четырех частотах: две частоты - для кодирования единиц и нулей в одном направлении, а остальные две частоты - для передачи данных в обратном направлении.

При цифровом кодировании дуплексный режим на двухпроводной линии организуется с помощью техники TDM. Часть тайм-слотов используется для передачи данных в одном направлении, а часть - для передачи в другом направлении. Обычно тайм-слоты противоположных направлений чередуются, из-за чего такой способ иногда называют «пинг-понговой» передачей. TDM-разделение линии характерно, например, для цифровых сетей с интеграцией услуг (ISDN) на абонентских двухпроводных окончаниях.

Технология PON

Сеть PON – это пассивная оптическая сеть, которая использует пассивные оптические разветвители (сплиттеры) и оптические волновые мультиплексоры для концентрации абонентского трафика с множественным подключением абонентов к одному волокну. Система PON позволяет существенно уменьшить число оптических портов в узле доступа оператора и использовать кабельную систему с оптическими кабелями малой жильности. В то же время, технология PON дает возможность мультисервисного абонентского подключения (Triple Play) с гарантией качества сервисов.

В мире разработаны различные стандарты для сетей PON:

- EPON, он же GEPON, он же Ethernet PON;
- BPON – широкополосный (Broadband) PON на основе протокола ATM
- GPON – мультигигабитный PON на основе протокола GFP (не путать с протоколом GEPON).

В мире наиболее распространены технологии EPON (GEPON) и GPON. В странах Азиатско-Тихоокеанского региона (Япония, Китай, Корея и др.) развивают EPON, при этом Triple Play услуги выглядят как «данные по IP», «видео по IP», «голос по IP». США делают ставку на GPON. Оборудование GPON позволяет увеличить концентрацию абонентов на одно волокно до 64. Однако из-за меньшего объема производства цены на оборудование GPON пока значительно выше, чем цены на EPON.

Технология PON позволяет с использованием одного волокна организовать пассивную оптическую сеть доступа для 32 узлов в радиусе 20 км, предоставляя Ethernet и до 4 E1 в каждом узле. Одна из главных задач, стоящих перед современными телекоммуникационными сетями доступа – так называемая проблема «последней мили», предоставление как можно большей полосы пропускания индивидуальным и корпоративным абонентам при минимальных затратах.

Суть технологии PON заключается в том, что между центральным узлом и удаленными абонентскими узлами создается полностью пассивная оптическая сеть, имеющая топологию дерева. В промежуточных узлах дерева размещаются пассивные оптические разветвители (сплиттеры) – компактные устройства, не требующие питания и обслуживания.

Свойства сети PON

Древовидная архитектура с передачей по одному волокну на двух длинах волн навстречу друг другу: 1550 нм (от центрального узла к абонентам, нисходящий поток) и 1310 нм (от абонентов к центральному узлу, восходящий поток). На промежуточных узлах дерева, размещаются пассивные оптические разветвители.

Использование метода доступа TDMA позволяет гибко распределять полосу пропускания между абонентами. Абонентский узел рассчитан на обычный жилой дом или офисное здание и может охватывать сотни абонентов. По одному волокну обслуживаются до 32 абонентских узлов.

Технология ***GEPON***, несмотря на меньшую скорость связи абонент-сеть, имеет ряд серьезных преимуществ перед технологией GPON, а именно:

1.Высокая эффективность использования полосы услугами ТВ

GEPON использует стандартизированные IEEE механизмы предоставления широковещательных услуг: SCB (Single Copy Broadcast), IGMP Snooping, тогда как GPON доставляет трафик с помощью Unicast. Логично, что производители оборудования GPON реализуют функции multicast самостоятельной разработки, однако данная реализация неспособна обеспечить полную прозрачность сети на уровне «платформа – абонент» для протоколов multicast IEEE.

2.Эффективность «из конца-в-конец»

GEPON имеет симметричное соединение абонент-сеть, тогда как GPON имеет ассиметричную скорость соединения абонента сетью, что понижает эффективность использования портов на ядре сети.

3.Масштабируемость (возможность построения сетей любого масштаба), обеспечение совместимости с протоколами будущего (10GEPON)

Международные институты, занимающиеся стандартизацией технологий GEPON (IEEE) постоянно ведут модернизацию технологии и уже известен сле-

дующий шаг развития— 10GEPON, планируется его совместимость с уже построенными сетями GEPON.

Общие свойства сетей с коммутацией каналов

Сети с коммутацией каналов обладают несколькими важными общими свойствами независимо от того, какой тип мультиплексирования в них используется. Сети с динамической коммутацией требуют предварительной процедуры установления соединения между абонентами. Для этого в сеть передается адрес вызываемого абонента, который проходит через коммутаторы и настраивает их на последующую передачу данных. Запрос на установление соединения маршрутизируется от одного коммутатора к другому и, в конце концов, достигает вызываемого абонента. Сеть может отказать в установлении соединения, если емкость требуемого выходного канала уже исчерпана.

Для FDM-коммутатора емкость выходного канала равна количеству частотных полос этого канала, а для TDM-коммутатора - количеству тайм-слотов, на которые делится цикл работы канала. Сеть отказывает в соединении также в том случае, если запрашиваемый абонент уже установил соединение с кем-нибудь другим. В первом случае говорят, что занят коммутатор, а во втором - абонент. Возможность отказа в соединении является недостатком метода коммутации каналов.

Если соединение может быть установлено, то ему выделяется фиксированная полоса частот в FDM-сетях или же фиксированная пропускная способность в TDM-сетях. Эти величины остаются неизменными в течение всего периода соединения. Гарантированная пропускная способность сети после установления соединения является важным свойством, необходимым для таких приложений, как передача голоса, изображения или управления объектами в реальном масштабе времени. Однако динамически изменять пропускную способность канала по требованию абонента сети с коммутацией каналов не могут, что делает их неэффективными в условиях пульсирующего трафика.

Недостатком сетей с коммутацией каналов является невозможность применения пользовательской аппаратуры, работающей с разной скоростью. Отдельные части составного канала работают с одинаковой скоростью, так как сети с коммутацией каналов не буферизуют данные пользователей.

Сети с коммутацией каналов хорошо приспособлены для коммутации потоков данных постоянной скорости, когда единицей коммутации является не отдельный байт или пакет данных, а долговременный синхронный поток данных между двумя абонентами. Для таких потоков сети с коммутацией каналов добавляют минимум служебной информации для маршрутизации данных через сеть, используя временную позицию каждого бита потока в качестве его адреса назначения в коммутаторах сети.

Коммутация пакетов - это техника коммутации абонентов, которая была специально разработана для эффективной передачи компьютерного трафика. Эксперименты по созданию первых компьютерных сетей на основе техники коммутации каналов показали, что этот вид коммутации не позволяет достичь высокой общей пропускной способности сети. Суть проблемы заключается в пульсирующем характере трафика, который генерируют типичные сетевые приложения. Например, при обращении к удаленному файловому серверу пользователь сначала просматривает содержимое каталога этого сервера, что порождает передачу небольшого объема данных. Затем он открывает требуемый файл в текстовом редакторе, и эта операция может создать достаточно интенсивный обмен данными, особенно если файл содержит объемные графические включения. После отображения нескольких страниц файла пользователь некоторое время работает с ними локально, что вообще не требует передачи данных по сети, а затем возвращает модифицированные копии страниц на сервер - и это снова порождает интенсивную передачу данных по сети.

Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может составлять 1:50 или 1:100. Если для описанной сессии организовать коммутацию канала между компьютером пользователя и сервером, то большую часть времени канал будет простаивать. В то же время коммутационные возможности сети будут использоваться - часть тайм-слотов или частотных полос коммутаторов будет занята и недоступна другим пользователям сети.

При коммутации пакетов все передаваемые пользователем сети сообщения разбиваются в исходном узле на сравнительно небольшие части, называемые пакетами. Необходимо уточнить, что сообщением называется логически завершенная порция данных - запрос на передачу файла, ответ на этот запрос, содержащий весь файл, и т. п. Сообщения могут иметь произвольную длину, от нескольких байт до многих мегабайт. Напротив, пакеты обычно тоже могут иметь переменную длину, но в узких пределах, например от 46 до 1500 байт. Каждый пакет снабжается заголовком, в котором указывается адресная информация, необходимая для доставки пакета узлу назначения, а также номер пакета, который будет использоваться узлом назначения для сборки сообщения (рис. 39). Пакеты транспортируются в сети как независимые информационные блоки. Коммутаторы сети принимают пакеты от конечных узлов и на основании адресной информации передают их друг другу, а в конечном итоге - узлу назначения.

Рис. 39. Разбиение сообщения на пакеты

Коммутаторы пакетной сети отличаются от коммутаторов каналов тем, что они имеют внутреннюю буферную память для временного хранения пакетов, если выходной порт коммутатора в момент принятия пакета занят передачей другого пакета. В этом случае пакет находится некоторое время в очереди пакетов в буферной памяти выходного порта, а когда до него дойдет очередь, то он передается следующему коммутатору. Такая схема передачи данных позволяет сглаживать пульсации трафика на магистральных связях между коммутаторами и тем самым использовать их наиболее эффективным образом для повышения пропускной способности сети в целом.

Для пары абонентов наиболее эффективным было бы предоставление им в единоличное пользование скоммутированного канала связи, как это делается в сетях с коммутацией каналов. При этом способе время взаимодействия этой пары абонентов было бы минимальным, так как данные без задержек передавались бы от одного абонента другому. Простои канала во время пауз передачи абонентов не интересуют, для них важно быстрее решить свою собственную задачу. Сеть с коммутацией пакетов замедляет процесс взаимодействия конкретной пары абонентов, так как их пакеты могут ожидать в коммутаторах, пока по магистральным связям передаются другие пакеты, пришедшие в коммутатор ранее.

Тем не менее, общий объем передаваемых сетью компьютерных данных в единицу времени при технике коммутации пакетов будет выше, чем при технике коммутации каналов. Это происходит потому, что пульсации отдельных абонентов в соответствии с законом больших чисел распределяются во времени. Поэтому коммутаторы постоянно и достаточно равномерно загружены работой, если число обслуживаемых ими абонентов действительно велико.

Принцип работы коммутатора

Коммутатор хранит в памяти таблицу коммутации (хранящуюся в ассоциативной памяти), в которой указывается соответствие MAC-адреса узла порту коммутатора. При включении коммутатора эта таблица пуста, и он работает в режиме обучения. В этом режиме поступающие на какой-либо порт данные передаются на все остальные порты коммутатора. При этом коммутатор анализирует кадры и, определив MAC-адрес хоста-отправителя, заносит его в таблицу. Впоследствии, если на один из портов коммутатора поступит кадр, предназначенный для хоста, MAC-адрес которого уже есть в таблице, то этот кадр будет передан только через порт, указанный в таблице. Если MAC-адрес хоста-получателя ещё не известен, то кадр будет продублирован на все интерфейсы. Со временем коммутатор строит полную таблицу для всех своих портов, и в результате трафик локализуется.

Существует три способа коммутации.

С промежуточным хранением (Store and Forward). Коммутатор читает всю информацию в кадре, проверяет его на отсутствие ошибок, выбирает порт коммутации и после этого посылает в него кадр.

Сквозной (cut-through). Коммутатор считывает в кадре только адрес назначения и после выполняет коммутацию. Этот режим уменьшает задержки при передаче, но в нём нет метода обнаружения ошибок.

Бесфрагментный (fragment-free) или гибридный. Этот режим является модификацией сквозного режима. Передача осуществляется после фильтрации фрагментов коллизий (кадр размером 64 байта обрабатываются по технологии store-and-forward, остальные по технологии cut-through).

В современных коммутаторах вносится такие понятия, как симметричная и асимметричная коммутация.

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, когда все порты имеют ширину пропускания 10 Мб/с или 100 Мб/с.

Асимметричный коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мб/с и 100 Мб/с или 100 Мб/с и 1000 Мб/с. Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент-сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что тре-

бует большей ширины пропускания для того порта коммутатора, к которому подсоединен сервер, с целью предотвращения переполнения на этом порте. Для того, чтобы направить поток данных с порта 100 Мб/с на порт 10 Мб/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь ***буфер памяти***.

Для временного хранения пакетов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки пакетов — буферизация по портам и буферизация с общей памятью. При буферизации по портам, пакеты хранятся в очередях (queue), которые связаны с отдельными входными портами. Пакет передается на выходной порт только тогда, когда все пакеты, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один пакет задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные пакеты могут быть переданы на открытые порты их пунктов назначения.

При буферизации общей в памяти, все пакеты хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого пакеты, находившиеся в буфере, динамически распределяются по выходным портам. Это позволяет получить пакет на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить пакеты. Очистка этой карты происходит только после того, как пакет успешно отправлен.

Поскольку память буфера является общей, размер пакета ограничивается всем размером буфера, а не долей предназначенной для конкретного порта. Это означает, что крупные пакеты, могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, т. е. когда порт с шириной полосы пропускания 100 Мб/с должен отправлять пакеты на порт 10 Мб/с.

Асимметричный коммутатор также необходим для обеспечения большей ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения или каналов между сегментами магистрали.

Возможности и разновидности коммутаторов

Коммутаторы подразделяются на ***управляемые и неуправляемые***. Более сложные коммутаторы позволяют управлять коммутацией на канальном (втором) и сетевом (третьем) уровне модели OSI. Обычно их именуют соответственно, например Layer 2 Switch, Layer 3 Switch или просто, сокращенно L2, L3. Управление коммутатором может осуществляться посредством протокола Web-интерфейса, SNMP, и т. п.

Многие управляемые коммутаторы позволяют выполнять дополнительные функции: VLAN, QoS, агрегирование, зеркалирование. Сложные коммутаторы можно объединять в одно логическое устройство — ***стек***, с целью увеличения числа портов (например, можно объединить 4 коммутатора с 24 портами и получить логический коммутатор с (4*24-4=92) портами, либо с 96-ю портами (если для стекирования используются специальные порты)).

Рис. 40. Коммутатор DES-1005A.

Серии коммутаторов улучшенного дизайна DES-10xxD/RU и DGS-10xxD/RU включают коммутаторы с 5/8 портами Fast и Gigabit Ethernet соответственно.

Рис. 41.DGS-1016D/GE

Серия DGS-10xxD/GE включает в себя модели неуправляемых коммутаторов Gigabit Ethernet с различным количеством портов 10/100/1000 Мбит/с (от 5 до 24). Эти коммутаторы поддерживают стандарт IEEE 802.1p и четыре аппаратных очереди приоритетов на каждом физическом порте.

Коммутаторы серий DGS-10xxD/RU и DGS-10xxD/GE поддерживают технологию Green Ethernet. Эта энергосберегающая технология позволяет сократить расходы на электроэнергию, при этом, не оказывая влияния на производительность и функциональность устройств. Технология Green Ethernet может регулировать потребление электроэнергии, основываясь на определении

состояния канала связи и длины кабеля. Когда коммутатор с поддержкой этой технологии определяет, что питание, подключенного к нему компьютера отключено, то переводит соответствующий порт в режим сохранения энергии (power standby mode). Также коммутатор может регулировать энергопотребление путем анализа длины кабеля Ethernet. Т.к. в большинстве случаев для подключения пользователей домашних/офисных сетей используются кабели длиной менее 20 м, энергопотребление может быть снижено.

Благодаря уменьшению энергопотребления (до 80%), выделяется меньше тепла, что увеличивает срок эксплуатации устройства и снижает эксплуатационные расходы.

Также данная технология подразумевает использование материалов, не наносящих вред окружающей среде.

Помимо технологии Green Ethernet, в коммутаторах серий DGS-10xxD/RU и DGS-10xxD/GE реализована поддержка функции диагностики кабеля (Cable Diagnostic). Эта функция позволяет пользователям определять состояние кабеля по индикаторам, расположенным на передней панели коммутатора. С помощью нее можно определить следующие повреждения кабеля:

- разомкнутая цепь (Open Circuit) – оборванная жила кабеля Ethernet или кабель не подключен;
- короткое замыкание (Short Circuit) – закороченная пара кабеля (два проводника касаются друг друга);
- не правильная терминация кабеля (Improper Termination) – сопротивление между кабелем и его разъемом не совпадает или сопротивление больше чем 100 Ом.

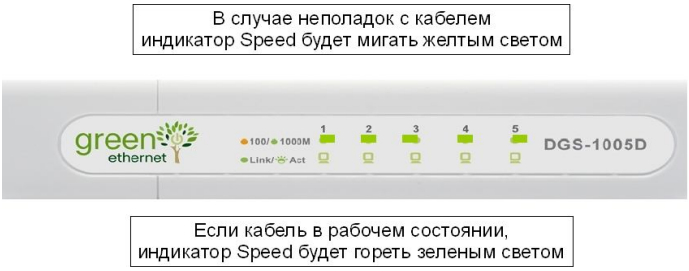


Рис. 42 Функция диагностики кабеля.

Функция диагностики кабеля сканирует все порты Ethernet и определяет состояние каждого подключенного кабеля. Во время этого процесса индикатор каждого порта последовательно мигает зеленым светом. Первоначальное сканирование порта требует около 10 секунд. Если обнаруживается повреждение кабеля, индикатор соответствующего порта будет мигать желтым светом около

5 секунд. Далее коммутатор автоматически перезагрузится и продолжит работу в обычном режиме. Этот процесс займет около 2-х секунд.

Традиционно разделяют только 2 категории коммутаторов: неуправляемые и управляемые. Однако D-Link предлагает еще одну, промежуточную категорию – **настраиваемые коммутаторы** (*smart switches*). Эти коммутаторы предназначены для использования на уровне доступа сетей малых и средних предприятий (*Small-to-Medium Business*, *SMB*).

Настраиваемые коммутаторы D-Link представлены двумя сериями: Easy Smart и Smart.

Коммутаторы Easy Smart в настоящее время включают две модели: DES-1100-16 и DES-1100-24. Эти коммутаторы помещены в металлический корпус компактного размера (11”) и оснащены 16 и 24 портами 10/100Base-TX соответственно. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных средств управления, например Web-интерфейса или утилиты SmartConsole. По сравнению с коммутаторами серии Smart, устройства Easy Smart обладают ограниченным функционалом.

Третье поколение коммутаторов серии Smart представлено продуктовыми линейками DES-1210-xx и DGS-1210-xx. Серия DES-1210-xx в настоящее время включает модели DES-1210-28 и DES-1210-52, оснащенные 24/48 портами 10/100 Мбит/с соответственно, 2 портами Gigabit Ethernet и 2 комбинированными uplink-портами 1000Base-T/SFP. Серия DGS-1210-xx включает четыре модели DGS-1210-10P, DGS-1210-16, DGS-1210-24 и DGS-1210-48. Модели DGS-1210-16, DGS-1210-24 и DGS-1210-48 оснащены 12/20/44 портами 1000Base-T и 4 комбинированными uplink-портами 1000Base-T/SFP. В модели DGS-1210-10P реализована поддержка технологии Power over Ethernet (PoE) (стандарты IEEE 802.3af и IEEE 802.3at (PoE+)), которая позволяет передавать питание по неиспользуемым парам кабеля Ethernet одновременно с передачей данных. Все устройства за исключением DGS-1210-10P помещены в металлический корпус размером для установки в стойку (19”). Размер корпуса DGS-1210-10P - 13”.

Рис. 43. Коммутатор DES-1210-28.

Коммутаторы серии Smart поддерживают функции обеспечения отказоустойчивости, безопасности, сегментации сети, качества обслуживания, мониторинга трафика и диагностики кабеля. Управление коммутаторами может

осуществляться через Web-интерфейс, утилиту SmartConsole, упрощенный интерфейс командной строки и протокол SNMP.

Помимо этого, коммутаторы серии DGS-1210-xx поддерживают технологию Green Ethernet и Jumbo-фреймы.

Управляемые коммутаторы, по сравнению с неуправляемыми и коммутаторами серии Smart, являются сложными устройствами, поддерживающими расширенный набор функций 2 и 3 уровня модели OSI. Такие устройства предоставляют большой выбор интерфейсов, обладают высокоскоростной внутренней магистралью, возможностью установки дополнительных модулей и физического стекирования. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

Серия бюджетных управляемых коммутаторов Fast Ethernet 2 уровня DES-1228/ME, DES-3028/52 может использоваться на уровне доступа сетей малых, средних и крупных предприятий, а также в сетях провайдеров для предоставления услуг Triple Play. Коммутаторы поддерживают базовый и расширенный функционал 2 уровня, обеспечивающий возможность управления доступом пользователей, контроля полосы пропускания, сегментации сети, управления широковещательными пакетами, многоадресной рассылкой. Коммутаторы DES-1228/ME также поддерживают функцию диагностики кабеля.

DES-1228/ME	24 порта 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3028	24 порта 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3028P	24 порта PoE 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3052	48 портов 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3052P	48 портов PoE 10/100Base-TX, 2 порта 10/100/1000Base-T, 2 комбо-порта 1000Base-T/SFP

Коммутаторы Fast Ethernet 2 уровня серии DES-3200-xx предназначены для использования на уровне доступа сетей провайдеров, предоставляющих услуги по подключению к сети Интернет посредством технологий Metro Ethernet (Ethernet-To-The-Home, ETTH и Fiber-To-The-Home, FTTH) и реализующих сервисы Triple Play.

Рис. 44. Коммутаторы серии DES-3200-xx.

DES-3200-10	8 портов 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-18	16 портов 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-26	24 порта 10/100Base-TX, 2 комбо-порта 1000Base-T/SFP
DES-3200-28	24 порта 10/100Base-TX, 4 комбо-порта 1000Base-T/SFP
DES-3200-28F	24 порта SFP, 4 комбо-порта 1000Base-T/SFP

Серия коммутаторов Fast Ethernet 2 уровня DES-3528/3552 предназначена для использования на уровне доступа сетей крупных предприятий и Metro Ethernet с сервисами Triple Play. Коммутаторы поддерживают физическое стекирование по Ethernet, статическую маршрутизацию, функции управления многоадресной рассылкой, расширенные функции безопасности и виртуальных локальных сетей VLAN. Устройства легко интегрируется с коммутаторами L3 уровня ядра для формирования многоуровневой сетевой структуры с высокоскоростной магистралью и централизованными серверами.

DES-3528	24 порта 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3528DC	24 порта 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP (питание 48В DC)
DES-3528P	24 порта PoE 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP
DES-3552	48 портов 10/100Base-TX, 2 порта 1000Base-T, 2 комбо-порта 1000Base-T/SFP

Коммутаторы Fast Ethernet 3 уровня серии DES-3810-xx являются новым поколением мультисервисных коммутаторов D-Link, предназначенным для использования на уровне доступа сетей крупных предприятий и Metro Ethernet, в которых реализованы сервисы Triple Play и VPN. В настоящее время серия

представлена моделью DES-3810-28. Одной из особенностей коммутаторов серии DES-3810-xx является то, что в них встроены два разных образа программного обеспечения: Standard Image (SI) и Enhanced Image (EI). В стандартной прошивке реализованы такие функции как качество обслуживания (QoS), включая механизм Traffic Shaping, Q-in-Q VLAN, маршрутизация пакетов IPv4, многоадресная рассылка, Ethernet OAM и множество функций безопасности. Расширенная прошивка включает поддержку маршрутизации IPv6, протоколов BGP и MPLS. Также коммутаторы серии DES-3810-xx поддерживают функцию Switch Resource Management (SRM), позволяющую администратору оптимизировать ресурсы коммутатора при его использовании в различных сетевых средах.

Рис. 45.Коммутатор DES-3810-28.

DES-3810-28	24 порта 10/100Base-TX, 4 комбо-порта 1000Base-T/SFP

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-3120-xx могут использоваться как на уровне доступа, так и на уровне субагрегации сетей SOHO/SMB и Metro Ethernet. В коммутаторах реализован базовый и расширенный функционал 2 уровня, поддерживается физическое стекирование через порты 10GE, подключение резервных источников питания, функция диагностики кабеля. Благодаря высокой плотности портов SFP коммутаторы DGS-3120-24SC и DGS-3120-24SC-DC обеспечивают возможность гибкого подключения по оптике к магистрали сети и серверам в сетях провайдеров услуг. Коммутаторы DGS-3120-24PC и DGS-3120-48PC поддерживают спецификацию передачи питания по Ethernet (стандарты IEEE 802.3af и IEEE 802.3at (PoE+)).

Рис. 46. Коммутаторы серии DGS-3120-xx.

DGS-3120-24TC	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-48TC	44 порта 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-24PC	20 портов PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP

DGS-3120-48PC	44 порта PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP
DGS-3120-24SC	8 комбо-портов 1000Base-T/ SFP, 16 слотов SFP
DGS-3120-24SC-DC	8 комбо-портов 1000Base-T/ SFP, 16 слотов SFP (питание 48В DC)

Малопортовые коммутаторы Gigabit Ethernet 2 уровня серии DGS-3200-xx обладают полным набором функций, позволяющим обеспечить безопасность, контроль доступа, отказоустойчивость и управляемость сети, и предназначены для использования на уровне доступа сетей средних и крупных предприятий. Коммутаторы DGS-3200-10 и DGS-3200-16 помещены в компактный корпус размером 11”. В коммутаторе DGS-3200-10 нет вентиляторов, благодаря чему он бесшумный. В коммутаторе DGS-3200-16 используется технология автоматической вентиляции.

Рис. 47. Коммутаторы серии DGS-3200-xx.

DGS-3200-10	8 портов 10/100/1000Base-T, 2 комбо-порта 1000Base-T/ SFP
DGS-3200-16	14 портов 10/100/1000Base-T, 2 комбо-порта 1000Base-T/ SFP

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-34xx предназначены для использования на уровне распределения сетей крупных предприятий и Metro Ethernet.

DGS-3426	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 2 слота расширения
DGS-3426G	20 слотов SFP, 4 комбо-порта 1000Base-T/ SFP, 2 слота расширения
DGS-3426P	20 портов PoE 10/100/1000Base-T, 4 комбо-порта 1000Base-T(PoE)/ SFP, 2 слота расширения
DGS-3427	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 3 слота расширения
DGS-3450	44 порта 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 2 слота расширения

Коммутаторы обеспечивают высокую плотность портов для подключения рабочих мест, оснащены слотами SFP для гибкого подключения по оптике, сло-

тами для установки модулей расширения с портами 10 Gigabit Ethernet, обладают высокопроизводительной внутренней магистралью и поддерживают возможность физического стекирования через порты 10 GE.

Среди функциональных возможностей можно выделить поддержку статической маршрутизации IPv4/IPv6, расширенные функции безопасности, качества обслуживания, виртуальных локальных сетей и управления.

Коммутаторы Gigabit Ethernet 2 уровня серии DGS-3700-xx спроектированы с учетом требований операторов телекоммуникационных услуг при построении сетей Metro Ethernet. Коммутаторы поддерживают широкий набор функций безопасности, качества обслуживания, управления многоадресными пакетами и обеспечивают расширенную поддержку VLAN. Коммутаторы обладают модульной архитектурой ядра, поддерживают возможность выбора источника питания (постоянного или переменного тока) и расширенный диапазон рабочих температур.

DGS-3700-12	8 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/SFP
DGS-3700-12G	8 слотов SFP, 4 комбо-порта 1000Base-T/SFP

Семейство маршрутизирующих управляемых коммутаторов Gigabit Ethernet 3 уровня с поддержкой портов 10 GE DGS-36xx обладает высокой производительностью и предназначено для использования на уровнях распределения и ядра крупных корпоративных сетей, сетей предприятий малого и среднего бизнеса (SMB) и городских сетей Metro Ethernet. Благодаря расширенной поддержке функций многоадресной передачи данных, среди которых IGMP v.3, PIM SM и PIM DM, коммутаторы позволяют значительно повысить эффективность предоставляемых операторами связи таких услуг, как видео по требованию (VoD), IP-телевидение (IPTV) и телевидение высокой четкости (HDTV). Коммутаторы поддерживают протоколы маршрутизации BGP, OSPF, RIP v.1/2, возможность создания статических и плавающих статических маршрутов IP v4/v6.

DGS-3612	8 портов 10/100/1000Base-T
DGS-3612G	8 слотов SFP, 4 комбо-порта SFP /1000Base-T
DGS-3627	20 портов 10/100/1000Base-T, 4 комбо-порта 1000Base-T/SFP, 3 слота расширения
DGS-3627G	20 портов SFP, 4 комбо-порта SFP /1000Base-T, 3 слота расширения
DGS-3650	44 порта 10/100/1000Base-T, 4 комбо-порта 1000Base-T/ SFP, 2 слота расширения

Высокопроизводительные коммутаторы Gigabit Ethernet 3 уровня с поддержкой портов 10 GE серии DGS-3610-xx обладают расширенным функционалом, включая поддержку BGP, и могут применяться на магистрали сетей Metro Ethernet и крупных предприятий, рис.49.

Рис. 48. Коммутатор DGS-3610-26.

DGS-3610-26	12 портов 10/100/1000Base-T, 12 комбо-портов 1000Base-T/ SFP, 2 слота расширения
DGS-3610-26G	12 слотов SFP, 12 комбо-портов 1000Base-T/ SFP, 2 слота расширения

Коммутаторы 3 уровня на основе шасси серии DES-72xx являются высокопроизводительными устройствами с высокой плотностью портов, предназначенными для уровня ядра сетей крупных предприятий и Metro Ethernet. Устанавливая в шасси модули расширения, пользователи могут получить до 384 гигабитных портов, до 64 портов 10GE, до 192 слотов SFP, или их комбинаций. Коммутаторы поддерживают богатый набор функций 2 и 3 уровня, включая поддержку протоколов BGP, MPLS (Multi-protocol Label Switching), функции IPFIX, позволяющей получать статистику о сетевом трафике.

Более полную информацию о возможностях коммутаторов и методов их применения можно получить, изучив учебный курс компании D-Link посвящённый этой теме.

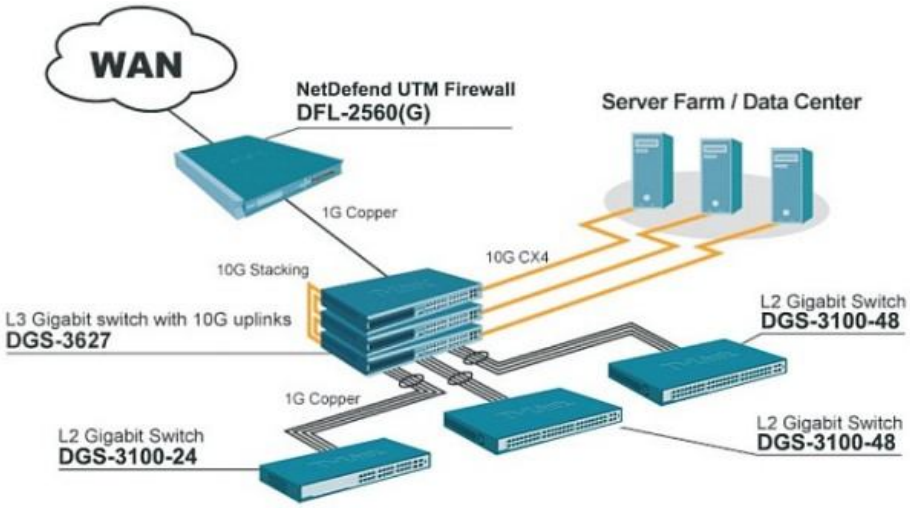


Рис. 49.Примерная схема применения коммутаторов D-Link

Виртуальные каналы в сетях с коммутацией пакетов

Описанный выше режим передачи пакетов между двумя конечными узлами сети предполагает независимую маршрутизацию каждого пакета. Такой режим работы сети называется дейтаграммным, и при его использовании коммутатор может изменить маршрут какого-либо пакета в зависимости от состояния сети - работоспособности каналов и других коммутаторов, длины очередей пакетов в соседних коммутаторах и т. п.

Существует и другой режим работы сети - передача пакетов по ***виртуальному каналу (virtual circuit или virtual channel)***. В этом случае перед тем, как начать передачу данных между двумя конечными узлами, должен быть установлен виртуальный канал, который представляет собой единственный маршрут, соединяющий эти конечные узлы. Виртуальный канал может быть динамическим или постоянным.

Динамический виртуальный канал устанавливается при передаче в сеть специального пакета - запроса на установление соединения. Этот пакет проходит через коммутаторы и «прокладывает» виртуальный канал. Это означает, что коммутаторы запоминают маршрут для данного соединения и при поступлении последующих пакетов данного соединения отправляют их всегда по проложенному маршруту.

Постоянные виртуальные каналы создаются администраторами сети путем ручной настройки коммутаторов. При отказе коммутатора или канала на пути виртуального канала соединение разрывается, и виртуальный канал прокладывается автоматически заново. При этом он, естественно, обойдет отказавшие участки сети.

Каждый режим передачи пакетов имеет свои преимущества и недостатки. Дейтаграммный метод не требует предварительного установления соединения и поэтому работает без задержки перед передачей данных. Это особенно выгодно для передачи небольшого объема данных, когда время установления соединения может быть соизмеримым со временем передачи данных. Кроме того, дейтаграммный метод быстрее адаптируется к изменениям в сети.

При использовании метода виртуальных каналов время, затраченное на установление виртуального канала, компенсируется последующей быстрой передачей всего потока пакетов. Коммутаторы распознают принадлежность пакета к виртуальному каналу по специальной метке - номеру виртуального канала, а не анализируют адреса конечных узлов, как это делается при дейтаграммном методе.

Пропускная способность сетей с коммутацией пакетов

Одним из отличий метода коммутации пакетов от метода коммутации каналов является неопределенность пропускной способности соединения между двумя абонентами. В методе коммутации каналов после образования составного канала пропускная способность сети при передаче данных между конечными узлами известна - это пропускная способность канала. Данные после задержки, связанной с установлением канала, начинают передаваться на максимальной для канала скорости (рис. 50, а). Время передачи сообщения в сети с коммутацией каналов $T_{к.к.}$ равно сумме задержки распространения сигнала по линии связи $t_{а.р.}$ и задержки передачи сообщения $t_{з.п.}$. Задержка распространения сигнала зависит от скорости распространения электромагнитных волн в конкретной физической среде, которая колеблется от 0,6 до 0,9 скорости света в вакууме. Время передачи сообщения равно V/C, где V - объем сообщения в битах, а C - пропускная способность канала в битах в секунду.

В сети с коммутацией пакетов наблюдается принципиально другая картина.

Процедура установления соединения в этих сетях, если она используется, занимает примерно такое же время, как и в сетях с коммутацией каналов, поэтому будем сравнивать только время передачи данных.

На рис. 50,б показан пример передачи в сети с коммутацией пакетов. Предполагается, что в сеть передается сообщение того же объема, что и сообщение, иллюстрируемое рис. 50,а, однако оно разделено на пакеты, каждый из которых снабжен заголовком. Время передачи сообщения в сети с коммутацией пакетов обозначено на рисунке $T_{к.п.}$. При передаче этого сообщения, разбитого на пакеты, по сети с коммутацией пакетов возникают дополнительные временные задержки.

Во-первых, это задержки в источнике передачи, который, помимо передачи собственно сообщения, тратит дополнительное время на передачу заголовков $t_{п.з.}$, плюс к этому добавляются задержки $t_{инт}$, вызванные интервалами между передачей каждого следующего пакета (это время уходит на формирование очередного пакета стеком протоколов).

Во-вторых, дополнительное время тратится в каждом коммутаторе. Здесь задержки складываются из времени буферизации пакета $t_{б.п.}$ (коммутатор не может начать передачу пакета, не приняв его полностью в свой буфер) и времени коммутации $t_{к.}$. Время буферизации равно времени приема пакета с битовой скоростью протокола. Время коммутации складывается из времени ожидания пакета в очереди и времени перемещения пакета в выходной порт. Если время перемещения пакета фиксировано и обычно невелико (от нескольких микросекунд до нескольких десятков микросекунд), то время ожидания пакета в очереди колеблется в очень широких пределах и заранее неизвестно, так как зависит от текущей загрузки сети пакетами.

Проведем грубую оценку задержки в передаче данных в сетях с коммутацией пакетов по сравнению с сетями с коммутацией каналов на простейшем

примере. Пусть тестовое сообщение, которое нужно передать в обоих видах сетей, составляет 200 Кбайт. Отправитель находится от получателя на расстоянии 5000 км. Пропускная способность линий связи составляет 2 Мбит/с.

Время передачи данных по сети с коммутацией каналов складывается из времени распространения сигнала, которое для расстояния 5000 км можно оценить примерно в 25 мс, и времени передачи сообщения, которое при пропускной способности 2 Мбит/с и длине сообщения 200 Кбайт равно примерно 800 мс, то есть всего передача данных заняла 825 мс.

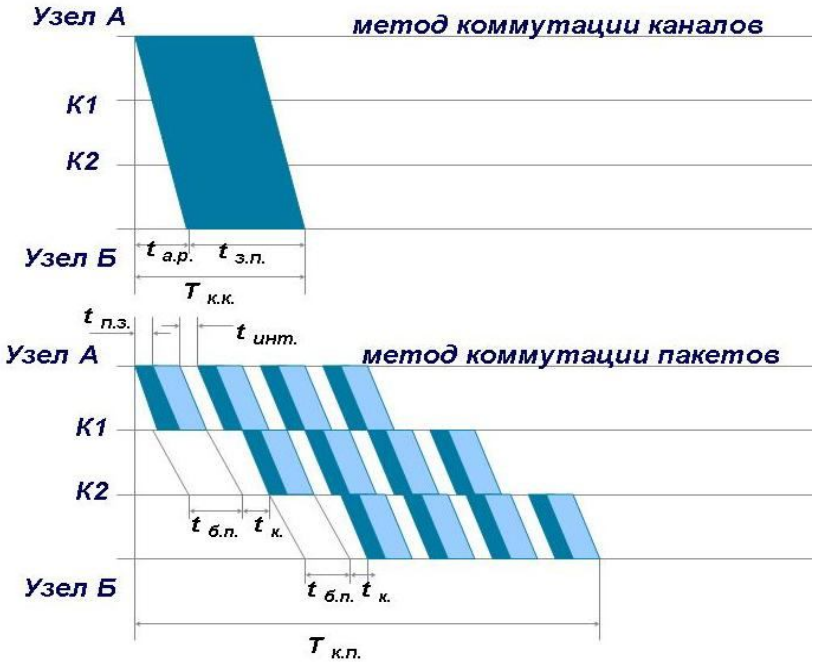


Рис. 50. Пропускная способность сетей с коммутацией пакетов

Оценим дополнительное время, которое потребуется для передачи этого сообщения по сети с коммутацией пакетов. Будем считать, что путь от отправителя до получателя пролегает через 10 коммутаторов. Исходное сообщение разбивается на пакеты в 1 Кбайт, всего 200 пакетов. Вначале оценим задержку, которая возникает в исходном узле. Предположим, что доля служебной информации, размещенной в заголовках пакетов, по отношению к общему объему сообщения составляет 10 %. Следовательно, дополнительная задержка, связанная с передачей заголовков пакетов, составляет 10 % от времени передачи целого сообщения, то есть 80 мс. Если принять интервал между отправкой пакетов равным 1 мс, тогда дополнительные потери за счет интервалов составят 200 мс. Итого, в исходном узле из-за пакетирования сообщения при передаче возникла дополнительная задержка в 280 мс.

Каждый из 10 коммутаторов вносит задержку коммутации, которая может иметь большой разброс, от долей до тысяч миллисекунд. В данном примере

примем, что на коммутацию в среднем тратится 20 мс. Кроме того, при прохождении сообщений через коммутатор возникает задержка буферизации пакета. Эта задержка при величине пакета 1 Кбайт и пропускной способности линии 2 Мбит/с равна 4 мс. Общая задержка, вносимая 10 коммутаторами, составит примерно 240 мс. В результате дополнительная задержка, созданная сетью с коммутацией пакетов, составила 520 мс. Учитывая, что вся передача данных в сети с коммутацией каналов заняла 825 мс, эту дополнительную задержку можно считать существенной.

Хотя приведенный расчет носит очень приблизительный характер, но он делает более понятными те причины, которые приводят к тому, что процесс передачи для определенной пары абонентов в сети с коммутацией пакетов является более медленным, чем в сети с коммутацией каналов.

Неопределенная пропускная способность сети с коммутацией пакетов - это плата за ее общую эффективность при некотором ущемлении интересов отдельных абонентов. Аналогично, в мультипрограммной операционной системе время выполнения приложения предсказать заранее невозможно, так как оно зависит от количества других приложений, с которыми делит процессор данное приложение.

На эффективность работы сети существенно влияют размеры пакетов, которые передает сеть. Слишком большие размеры пакетов приближают сеть с коммутацией пакетов к сети с коммутацией каналов, поэтому эффективность сети при этом падает. Слишком маленькие пакеты заметно увеличивают долю служебной информации, так как каждый пакет несет с собой заголовок фиксированной длины, а количество пакетов, на которые разбиваются сообщения, будет резко расти при уменьшении размера пакета. Существует некоторая золотая середина, которая обеспечивает максимальную эффективность работы сети, однако ее трудно определить точно, так как она зависит от многих факторов, некоторые из них к тому же постоянно меняются в процессе работы сети. Поэтому разработчики протоколов для сетей с коммутацией пакетов выбирают пределы, в которых может находиться длина пакета, а точнее его поле данных, так как заголовок, как правило, имеет фиксированную длину. Обычно нижний предел поля данных выбирается равным нулю, что разрешает передавать служебные пакеты без пользовательских данных, а верхний предел не превышает 4-х килобайт. Приложения при передаче данных пытаются занять максимальный размер поля данных, чтобы быстрее выполнить обмен данными, а небольшие пакеты обычно используются для квитанций о доставке пакета.

При выборе размера пакета необходимо учитывать также и интенсивность битовых ошибок канала. На ненадежных каналах необходимо уменьшать размеры пакетов, так как это уменьшает объем повторно передаваемых данных при искажениях пакетов.

Под коммутацией сообщений понимается передача единого блока данных между транзитными компьютерами сети с временной буферизацией этого блока на диске каждого компьютера (рис. 51). Сообщение в отличие от пакета имеет произвольную длину, которая определяется не n технологическими соображениями, а содержанием информации, составляющей сообщение. Например, сообщением может быть текстовый документ, файл с кодом программы, электронное письмо.

Рис. 51. Коммутация сообщений

Транзитные компьютеры могут соединяться между собой как сетью с коммутацией пакетов, так и сетью с коммутацией каналов. Сообщение хранится в транзитном компьютере на диске, причем время хранения может быть достаточно большим, если компьютер загружен другими работами или сеть временно перегружена.

По такой схеме обычно передаются сообщения, не требующие немедленного ответа, чаще всего сообщения электронной почты. Режим передачи с промежуточным хранением на диске называется режимом «хранение-и-передача» (store-and-forward).

Режим коммутации сообщений разгружает сеть для передачи трафика, требующего быстрого ответа, например трафика службы WWW или файловой службы.

Количество транзитных компьютеров стараются по возможности уменьшить. Если компьютеры подключены к сети с коммутацией пакетов, то число промежуточных компьютеров обычно уменьшается до двух. Например, пользователь передает почтовое сообщение своему серверу исходящей почты, а тот сразу старается передать сообщение серверу входящей почты адресата. Но если компьютеры связаны между собой телефонной сетью, то часто используется несколько промежуточных серверов, так как прямой доступ к конечному серверу может быть невозможен в данный момент из-за перегрузки телефонной сети (абонент занят) или экономически невыгоден из-за высоких тарифов на дальнюю телефонную связь.

Техника коммутации сообщений появилась в компьютерных сетях раньше техники коммутации пакетов, но потом была вытеснена последней, как более эффективной по критерию пропускной способности сети. Запись сообщения на диск занимает достаточно много времени, кроме того, наличие дисков предполагает специализированные компьютеры в качестве коммутаторов, что удорожает сеть. Сегодня коммутация сообщений работает только для некоторых не оперативных служб, причем чаще всего поверх сети с коммутацией пакетов, как служба прикладного уровня.

3. Модели сетевого взаимодействия

Представим себе средства сетевого взаимодействия, в виде иерархически организованного множества модулей. При этом модули нижнего уровня могут, например, решать все вопросы, связанные с надежной передачей электрических сигналов между двумя соседними узлами. Модули более высокого уровня организуют транспортировку сообщений в пределах всей сети, пользуясь для этого средствами упомянутого нижележащего уровня.

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

Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть ***интерфейсом. Интерфейс*** определяет набор сервисов, предоставляемый данным уровнем соседнему уровню. В сущности, протокол и интерфейс выражают одно и то же понятие, но традиционно в сетях за ними закрепили разные области действия: протоколы определяют правила взаимодействия модулей, предоставляющие пользователям доступ к различным службам - файловой, печати и т. п. одного уровня в разных узлах, а интерфейсы - модулей соседних уровней в одном узле.

Средства каждого уровня должны отрабатывать, во-первых, свой собственный протокол, а во-вторых, интерфейсы с соседними уровнями (рис.52).

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется **стеком коммуникационных протоколов.**

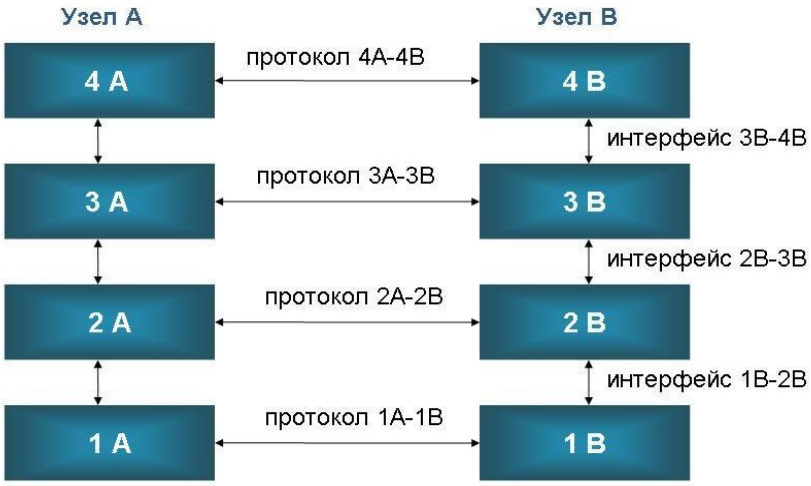


Рис. 52. Пример взаимодействия двух узлов в сети.

Коммуникационные протоколы могут быть реализованы как *программно*, так и *аппаратно*. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней - как правило, чисто программными средствами. Программный модуль, реализующий некоторый протокол, часто для краткости также называют ***«протоколом».***

Интерфейс (от англ. interface— поверхность раздела, перегородка)— совокупность средств и методов взаимодействия между элементами системы.

Пример:

электрические вилка и розетка— являются **интерфейсом энергоснабжения** большинства бытовых приборов;

клавиатура и мышь— являются **интерфейсом компьютера** в контексте «пользователь— ЭВМ»;

адрес электронной почты— является **коммуникационным интерфейсом** пользователя интернет;

протокол передачи данных— часть **интерфейса клиент-серверной архитектуры**;

Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами - мостами, коммутаторами, маршрутизаторами и т. д.

Любую систему (компьютер, вычислительная сеть, ОС, программный пакет, другие аппаратные и программные продукты), можно назвать открытой системой, если она построена в соответствии с ***открытыми спецификациями.*** Под термином ***«спецификация» (в вычислительной технике)*** понимают формализованное описание аппаратных или программных компонентов, способов

их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик.

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

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

Открытая система *в информатике*— аппаратура и/или программное обеспечение, которое обеспечивает переносимость и совместимость, а часто и их вместе с другими компьютерными системами.

Сетевая модель OSI (англ. Open Systems Interconnection Reference Model — модель взаимодействия открытых систем) — абстрактная модель для сетевых коммуникаций и разработки сетевых протоколов. Представляет уровневый подход к сети. Каждый уровень обслуживает свою часть процесса взаимодействия.

1.14. Модель OSI

В начале 80-х годов международная организация по стандартизации ***(International Standardization Organization - ISO***) разработала ***модель OSI***, которая сыграла значительную роль в развитии сетей.

Эталонная модель OSI, иногда называемая ***стеком OSI*** представляет собой 7-уровневую сетевую иерархию.

горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;

вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине;

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной - соседние уровни обмениваются данными с использованием интерфейсов API.

Представим, приложение обращается с запросом к прикладному уровню, например к файловой службе. На основании этого запроса программное обеспечение прикладного уровня формирует ***сообщение*** стандартного формата. Обычное сообщение состоит из заголовка и поля данных. Заголовок содержит служебную информацию, которую необходимо передать через сеть прикладно-

му уровню машины-адресата, чтобы сообщить ему, какую работу надо выполнить. В нашем случае заголовок, очевидно, должен содержать информацию о месте нахождения файла и о типе операции, которую необходимо над ним выполнить. Поле данных сообщения может быть пустым или содержать какие-либо данные, например те, которые необходимо записать в удаленный файл. Но для того чтобы доставить эту информацию по назначению, предстоит решить еще много задач, ответственность за которые несут нижележащие уровни.

После формирования сообщения прикладной уровень направляет его вниз по стеку представительному уровню. Протокол представительного уровня на основании информации, полученной из заголовка прикладного уровня, выполняет требуемые действия и добавляет к сообщению собственную служебную информацию - заголовок представительного уровня, в котором содержатся указания для протокола представительного уровня машины-адресата.

Полученное в результате сообщение передается вниз сеансовому уровню, который в свою очередь добавляет свой заголовок, и т. д. (Некоторые реализации протоколов помещают служебную информацию не только в начале сообщения в виде заголовка, но и в конце, в виде так называемого ***«концевика».)***

Наконец, сообщение достигает нижнего, физического уровня, который собственно и передает его по линиям связи машине-адресату. К этому моменту сообщение «обрастает» заголовками всех уровней *(рис. 53)*.

Когда сообщение по сети поступает на машину - адресат, оно принимается ее физическим уровнем и последовательно перемещается вверх с уровня на уровень. Каждый уровень анализирует и обрабатывает заголовок своего уровня, выполняя соответствующие данному уровню функции, а затем удаляет этот заголовок и передает сообщение вышележащему уровню.

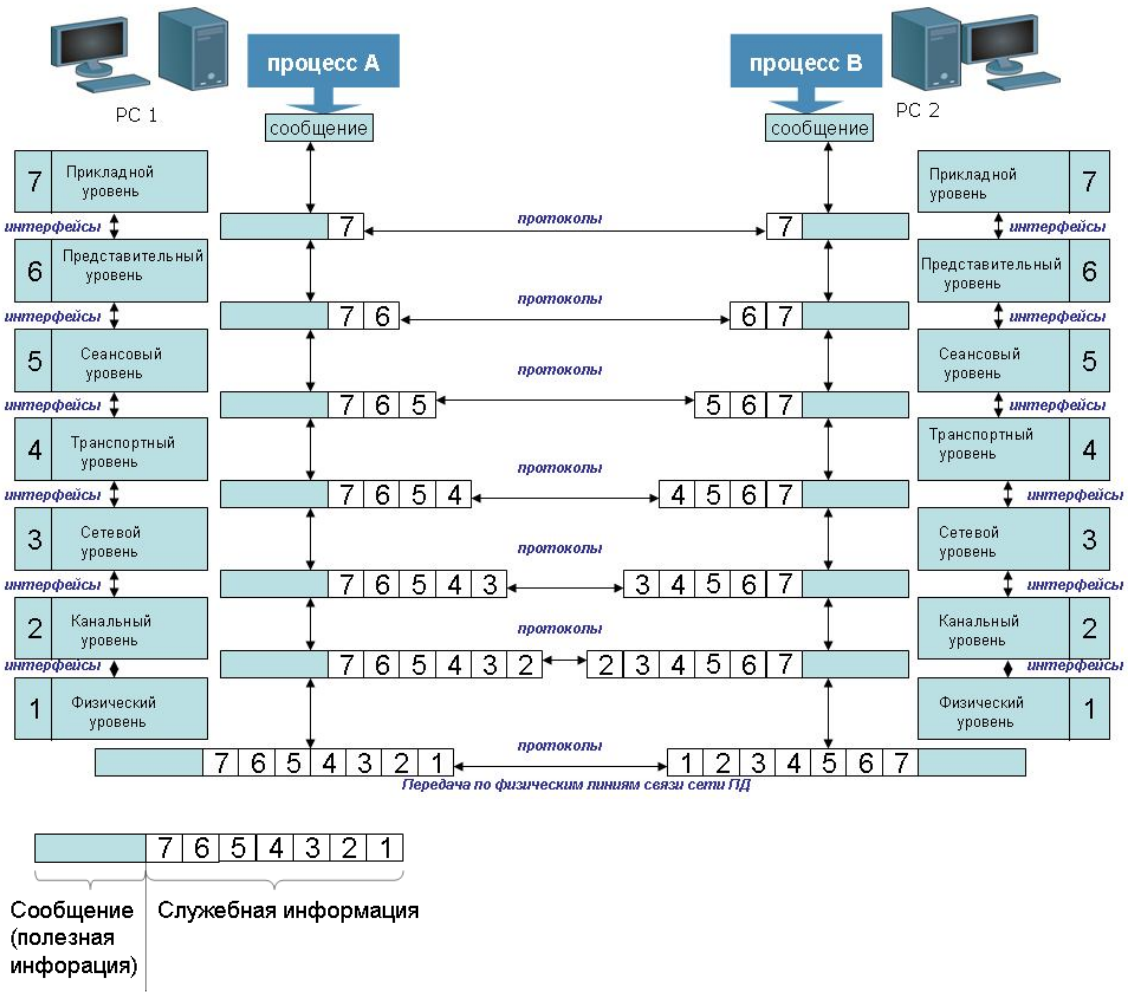


Рис. 53. Эталонная модель взаимодействия открытых систем (ISO/0SI).

Наряду с термином ***сообщение (message)*** существуют и другие термины, применяемые сетевыми специалистами для обозначения единиц данных в процедурах обмена. ***В стандартах ISO*** для обозначения единиц данных, с которыми имеют дело протоколы разных уровней, используется общее название ***протокольный блок данных (Protocol Data Unit, PDU)***. Для обозначения блоков данных определенных уровней часто используются специальные названия: ***кадр (frame), пакет (packet), дейтаграмма (datagram), сегмент (segment).***

Модель OSI описывает только системные средства взаимодействия, реализуемые операционной системой, системными утилитами, системными аппаратными средствами. Модель не включает средства взаимодействия приложений конечных пользователей. Свои собственные протоколы взаимодействия приложения реализуют, обращаясь к системным средствам. Поэтому необходимо различать уровень взаимодействия приложений и прикладной уровень.

Следует также иметь в виду, что приложение может взять на себя функции некоторых верхних уровней модели OSI. Например, некоторые СУБД имеют встроенные средства удаленного доступа к файлам. В этом случае приложение, выполняя доступ к удаленным ресурсам, не использует системную файловую службу; оно обходит верхние уровни модели OSI и обращается напрямую к системным средствам, ответственным за транспортировку сообщений по сети, которые располагаются на нижних уровнях модели OSI.

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

Вторая группа протоколов - ***протоколы без предварительного установления соединения.*** Такие протоколы называются также ***дейтаграммными протоколами***. Отправитель просто передает сообщение, когда оно готово. При взаимодействии компьютеров используются протоколы обоих типов.

Уровни модели OSI

Физический

На этом уровне модели OSI определяются следующие характеристики сетевых компонентов:

- типы соединений сред передачи данных, физические топологии сети, способы передачи данных (с цифровым или аналоговым кодированием сигналов), виды синхронизации передаваемых данных,
- разделение каналов связи с использованием частотного и временного мультиплексирования.

Реализации протоколов физического уровня модели OSI координируют правила передачи битов, т. е. отвечают за то, чтобы каждый переданный бит мог быть принят другим узлом сети.

Физический уровень не включает описание среды передачи. Однако реализации протоколов физического уровня специфичны для конкретной среды передачи. С физическим уровнем обычно ассоциируется подключение *сетевого оборудования*.

Канальный уровень

Этот уровень определяет логическую ***топологию*** сети, правила получения доступа к среде передачи данных, решает вопросы, связанные с адресацией физических устройств в рамках логической сети и управлением передачей информации (синхронизация передачи и сервис соединений) между сетевыми устройствами.

Протоколы канального уровня реализуются для достижения следующих основных целей:

- организации ***битов*** физического уровня (двоичные единицы и нули) в логические группы информации, называемые ***фреймами*** или кадрами. Фрейм является единицей данных канального уровня, состоящей из непрерывной последовательности сгруппированных битов, имеющей заголовок и окончание;
- обнаружения (а иногда и исправления) ошибок при передаче;
- управления потоками данных (для устройств, работающих на этом уровне модели OSI, например мостов (bridge));
- идентификации компьютеров в сети по их физическим адресам.

Подобно большинству других уровней, канальный уровень добавляет собственную управляющую информацию в начало пакета данных. Эта информация может включать адрес источника и адрес назначения (физический или аппаратный), информацию о длине фрейма и индикацию активных протоколов верхнего уровня. С канальным уровнем обычно связаны такие сетевые соединительные устройства – мосты (bridge), коммутаторы, сетевые интерфейсные платы (сетевые интерфейсные карты, адаптеры и т д.).

Сетевой уровень

Сетевой уровень служит для образования единой транспортной системы, объединяющей несколько сетей, причем эти сети могут использовать совершенно различные принципы передачи сообщений между конечными узлами и

обладать произвольной структурой связей. Функции сетевого уровня достаточно разнообразны.

Протоколы канального уровня локальных сетей обеспечивают доставку данных между любыми узлами только в сети с соответствующей ***типовой топологией***, например ***топологией типа «звезда»***. Это очень жесткое ограничение, которое не позволяет строить сети с развитой структурой, например, сети, объединяющие несколько сетей предприятия в единую сеть, или высоконадежные сети, в которых существуют избыточные связи между узлами. Можно было бы усложнять протоколы канального уровня для поддержания петлевидных избыточных связей, но принцип разделения обязанностей между уровнями приводит к другому решению. Чтобы с одной стороны сохранить простоту процедур передачи данных для типовых топологий, а с другой допустить использование произвольных топологий, вводится дополнительный ***сетевой уровень***.

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

В общем случае функции сетевого уровня шире, чем функции передачи сообщений по связям с нестандартной структурой. Сетевой уровень решает также задачи согласования разных технологий, упрощения адресации в крупных сетях и создания надежных и гибких барьеров на пути нежелательного трафика между сетями.

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

На сетевом уровне определяются два вида протоколов. Первый вид - сетевые протоколы - реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют ***протоколами разрешения адресов - Address Resolution Protocol, ARP.*** Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути. Примерами протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP и протокол межсетевого обмена пакетами IPX стека Novell.

Транспортный уровень

На пути от отправителя к получателю пакеты могут быть искажены или утеряны. Хотя некоторые приложения имеют собственные средства обработки ошибок, существуют и такие, которые предпочитают сразу иметь дело с надежным соединением. ***Транспортный уровень обеспечивает*** приложениям или верхним уровням стека - прикладному и сеансовому - передачу данных с той степенью надежности, которая им требуется.

Модель OSI определяет пять классов сервиса, предоставляемых транспортным уровнем. Эти виды сервиса отличаются качеством предоставляемых услуг: срочностью, возможностью восстановления прерванной связи, наличием средств мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол, а главное - способностью к обнаружению и исправлению ошибок передачи, таких как искажение, потеря и дублирование пакетов.

Выбор класса сервиса транспортного уровня определяется, с одной стороны, тем, в какой степени задача обеспечения надежности решается самими приложениями и протоколами более высоких, чем транспортный, уровней, а с другой стороны, этот выбор зависит от того, насколько надежной является система транспортировки данных в сети, обеспечиваемая уровнями, расположенными ниже транспортного - сетевым, канальным и физическим.

Как правило, все протоколы, начиная с транспортного уровня и выше, реализуются программными средствами конечных узлов сети - компонентами их сетевых операционных систем. В качестве примера транспортных протоколов можно привести протоколы TCP и UDP стека TCP/IP и протокол SPX стека Novell. Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Сеансовый уровень

Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в настоящий момент, предоставляет средства синхронизации. Последние позволяют вставлять контрольные точки в длинные передачи, чтобы в случае отказа можно было вернуться назад к последней контрольной точке, а не начинать все с начала. Сеансовый уровень реализует управление диалогом с использованием одного из трёх способов общения: ***симплекс (simplex), полудуплекс (half duplex) и полный дуплекс (full duplex).***

Симплексное общение предполагает только однонаправленную передачу от источника к приемнику информации. Никакой обратной связи (от приемника к источнику) этот способ общения не обеспечивает.

Полудуплекс позволяет использовать одну среду передачи данных для двунаправленной передачи информации, но в каждый момент времени информация может передаваться только в одну сторону.

Полный Дуплекс обеспечивает одновременную передачу информации в обе стороны по среде передачи данных.

Администрирование сеанса связи между двумя сетевыми объектами, состоящее из установления соединения, передачи данных, завершения соединения, также выполняется на этом уровне модели OSI. После установления сеанса программное обеспечение, реализующее функции данного уровня, может проверять работоспособность (поддерживать) соединения вплоть до его завершения.

Представительный уровень

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

Прикладной уровень

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

Существует очень большое разнообразие служб прикладного уровня. К числу наиболее распространенных протоколов верхних уровней относятся:

FTP - протокол переноса файлов;

TFTP - упрощенный протокол переноса файлов;

X.400 - электронная почта;

Telnet;

SMTP - простой протокол почтового обмена;

CMIP - общий протокол управления информацией;

SNMP - простой протокол управления сетью;
NFS - сетевая файловая система;

Разумеется, в настоящее время основным используемым семейством протоколов является TCP/IP, разработка которого не была связана с моделью OSI. За все время существования модели OSI она не была реализована (что говорится один-в-один), и, по-видимому, не будет реализована никогда. Сегодня используется только некоторое подмножество модели OSI. Считается, что модель слишком сложна, а её реализация займёт слишком много времени

1.15. Модель TCP/IP.

Для обеспечения сетевых взаимодействий между сетевыми объектами каждый из объектов должен понимать другой объект, говорить с ним на одном языке. Другими словами, сетевые объекты должны удовлетворять определенному ***протоколу, набору правил общения***. Поскольку сетевое общение между сетевыми объектами является достаточно сложным процессом, описываемым всеми уровнями модели OSI, то и набор правил для организации общения достаточно сложен. Для реализации данного набора правил разработаны наборы, или ***стеки,*** взаимосвязанных и логически сгруппированных протоколов. Существует достаточно большое количество стеков протоколов, однако наиболее широкое распространение в настоящее время получили два: ***стек TCP/IP и стек IPX/SPX***.

Стек протоколов TCP/IP является открытым для дополнения; большинство мировых производителей программного и аппаратного обеспечения поддерживают этот набор протоколов. Очень широкое распространение стек TCP/IP получил вследствие массовой (особенно в последние годы) популяризации глобальной сети Internet. Изначально данный стек протоколов разрабатывался и применялся при реализации проекта ***ARPAnet.*** В ходе реализации проекта ARPAnet разрабатывались новые протоколы стека TCP/IP, дополняя его, давая возможность использовать новые сервисы и технологии. Так как сеть ARPAnet явилась прародительницей сети ***Internet,*** то и стек протоколов TCP/IP получил очень широкое распространение. Этот стек не поддерживается каким-либо одним производителем, он модифицируется и дополняется многими компаниями и независимыми разработчиками, однако существует специальная координационная группа, принимающая решения о включении новых протоколов или возможностей в стек TCP/IP. В настоящее время стек TCP/IP являясь открытым,

стал «родным» для большого набора операционных систем. Одной из особенностей работы протоколов данного стека является отличная приспособленность для использования в глобальных сетях, возможность передачи данных на большие расстояния.

В недавнем прошлом, при построении локальных компьютерных сетей активно использовался стек протоколов ***IPX/SPX***, поддерживаемый фирмой ***Novell.*** Он является базовым для *операционных систем семейства* ***NetWare***, производимых Novell. Стек IPX/SPX также открыт для дополнений и расширений, но все изменения в рамках данного стека протоколов возможны только после их одобрения специальным подразделением Novell.

Кроме кратко рассмотренных стеков протоколов существуют и другие. Сетевые взаимодействия для аппаратных платформ ведущих производителей поддерживаются их собственными сетевыми архитектурами. Для организации взаимодействий между компьютерами, производимыми *корпорацией* ***DEC,*** была разработана архитектура ***DECnet***, включающая в себя протоколы, реализующие задачи, описанные на всех уровнях модели OSI. Другим крупным производителем вычислительных систем, поддерживающим собственные сетевые архитектуры - *корпорация* ***IBM***. Для организации сетевых взаимодействий специалисты IBM разработали архитектуру SNA (System Network Architecture) Именно эта сетевая архитектура и была взята за основу при создании модели описания сетевых взаимодействий - эталонной модели OSI.

Соответствие уровней стека TCP/IP уровням модели OSI

Структура IP-пакета

IP-пакет (IP-дейтаграмма) — форматированный блок информации, передаваемый по вычислительной сети. Соединения вычислительных сетей, которые не поддерживают пакеты, такие как традиционные соединения типа «точка-точка» в телекоммуникациях, просто передают данные в виде последовательности байтов, символов или битов. При использовании пакетного форматирования сеть может передавать длинные сообщения более надежно и эффективно.

В стеке TCP/IP определены четыре уровня. Каждый из них несет на себе некоторую долю нагрузки по решению основной задачи - организации надежной и производительной работы составной сети, части которой построены на основе разных сетевых технологий.

Так как стек TCP/IP был разработан до появления модели взаимодействия открытых систем OSI, то, хотя он также имеет многоуровневую структуру, со-

ответствие уровней стека TCP/IP уровням модели OSI достаточно условно (таблица 2).

Таблица 2. соответствие уровней стека TCP/IP уровням ISO/OSI

<table>
<tr><td>7</td><td rowspan="2">WWW, Gopher, WAIS</td><td>SNMP</td><td>FTP</td><td>Telnet</td><td>TFTP</td><td>SMTP</td><td rowspan="2">I</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td><td colspan="3" rowspan="2">TCP</td><td colspan="3" rowspan="2">UDP</td><td rowspan="2">II</td></tr>
<tr><td>4</td></tr>
<tr><td>3</td><td>IP</td><td>ICMP</td><td>RIP</td><td colspan="2">OSPF</td><td>ARP</td><td>III</td></tr>
<tr><td>2</td><td colspan="6" rowspan="2">не регламентируется: Ethernet, Gigabit Ethernet,
Token Ring, PPP, FDDI, X.25, SLIP,
Frame Relay...</td><td rowspan="2">IV</td></tr>
<tr><td>1</td></tr>
<tr><td>уровни OSI</td><td colspan="6"></td><td>уровни TCP/IP</td></tr>
</table>

Прикладной уровень

Прикладной уровень объединяет все службы, представляемые системой пользовательским приложениям. За долгие годы использования в сетях различных стран и организаций стек TCP/IP накопил большое число протоколов и служб прикладного уровня. Прикладной уровень реализуется программными системами, построенными в архитектуре клиент-сервер, базирующейся на протоколах нижних уровней.

В отличие от протоколов остальных трех уровней, протоколы прикладного уровня занимаются деталями конкретного приложения и «не интересуются» способами передачи данных по сети. Этот уровень постоянно расширяется за счет присоединения к старым, прошедшим многолетнюю эксплуатацию сетевым службам типа Telnet, FTP, TFTP, DNS, SNMP, HTTP, новых служб, таких, например, как протокол передачи HTTPS.

Основной уровень стека TCP/IP

Поскольку на сетевом уровне не устанавливается соединение, то нет никаких гарантий того, что все пакеты будут доставлены в место назначения целыми и невредимыми или придут в том же порядке, в котором они были отправлены. Эту задачу - обеспечение надежности информационной связи между двумя конечными узлами - решает основной уровень стека TCP/IP, называемый также транспортным.

На этом уровне функционируют протокол управления передачей TCP и протокол дейтаграмм пользователя UDP. Протокол TCP обеспечивает надежную передачу сообщений между удаленными прикладными процессами за счет образования логических соединений. Этот протокол позволяет равноранговым объектам на компьютере-отправителе и на компьютере-получателе поддерживать обмен данными в дуплексном режиме. TCP позволяет без ошибок доставлять сформированный на одном из компьютеров поток байт в любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части - сегменты и передает их нижележащему уровню межсетевого взаимодействия. После того, как эти сегменты будут доставлены в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

Протокол UDP обеспечивает передачу прикладных пакетов дейтаграммным способом, как и главный протокол уровня межсетевого взаимодействия IP, и выполняет только функции связующего звена (мультиплексора) между сетевым протоколом и многочисленными системами прикладного уровня, или пользовательскими процессами.

Уровень межсетевого взаимодействия

Стержнем всей архитектуры является уровень межсетевого взаимодействия, или сетевой уровень, который реализует концепцию передачи пакетов в режиме без установления соединений, то есть дейтаграммным способом. Именно этот уровень обеспечивает возможность перемещения пакетов по сети, используя тот маршрут, который в данный момент является наиболее рациональ-

ным. Этот уровень также называют уровнем Internet, указывая, тем самым, на основную его функцию - передачу данных через составную сеть.

Основным протоколом уровня (в терминологии модели OSI) в стеке TCP/IP является протокол IP. Этот протокол изначально проектировался как протокол передачи пакетов в составных сетях, состоящих из большого количества локальных сетей, объединенных как локальными, так глобальными связями. Поэтому протокол IP хорошо работает в сетях со множеством топологий, рационально используя наличие в них подсистем и экономно расходуя пропускную способность низкоскоростных линий связи. Так как протокол IP является дейтаграммным протоколом, он не гарантирует доставку пакетов до узла назначения, но старается это сделать.

К уровню межсетевого взаимодействия относятся все протоколы, связанные с состоянием и модификацией таблиц маршрутизации, такие как протоколы сбора маршрутной информации RIP и OSPF, а также протокол межсетевых управляющих сообщений ICMP. Последний протокол предназначен для обмена информацией об ошибках между маршрутизаторами сети и удаленным источником пакета. С помощью специальных пакетов ICMP сообщает о невозможности доставки пакета, о превышении времени жизни или продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Уровень сетевых интерфейсов

Идеологическим отличием архитектуры стека TCP/IP от многоуровневой организации других стеков является интерпретация функций самого нижнего уровня - уровня сетевых интерфейсов. Протоколы этого уровня должны обеспечивать интеграцию в составную сеть других сетей, причем задача ставится так: сеть TCP/IP должна иметь средства включения в себя любой другой сети, какую бы внутреннюю технологию передачи данных эта сеть не использовала. Отсюда следует, что этот уровень нельзя определить раз и навсегда. Для каждой технологии, включаемой в составную сеть подсети, должны быть разработаны собственные интерфейсные средства. К таким интерфейсным средствам относится протокол инкапсуляции IP-пакетов межсетевого взаимодействия в кадры локальных технологий.

Уровень сетевых интерфейсов в протоколах TCP/IP не регламентируется, но он поддерживает все популярные стандарты физического и канального уровней: для локальных сетей - это Ethernet, Token Ring, FDDI, Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN, для глобальных сетей - протоколы соединений «точка-точка» SLIP и PPP, протоколы территориальных сетей с коммутацией пакетов X.25, Frame Relay. Разработана также специальная спецификация, определяющая использование технологии ATM в качестве транспорта канального уровня.

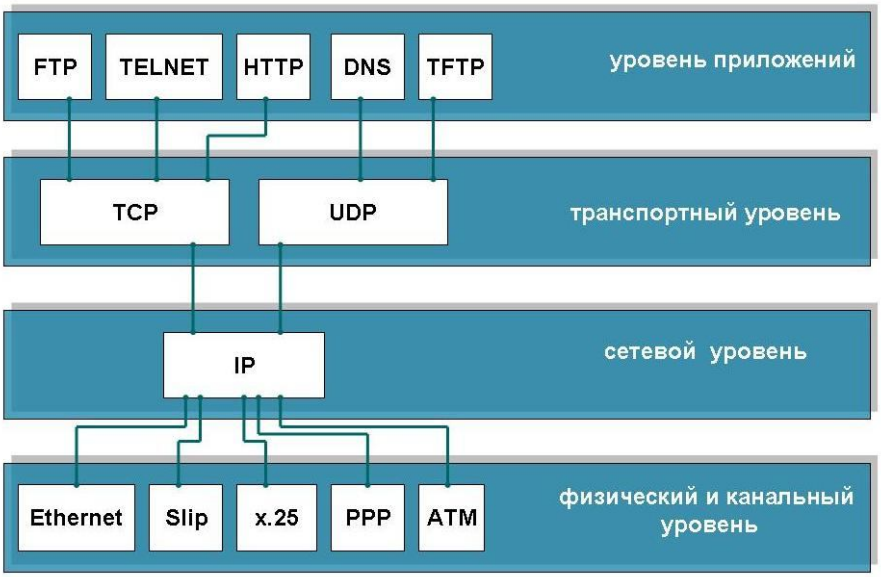


Рис. 54. Соответствие уровней стека TCP/IP уровням модели OSI

Рассматривая многоуровневую архитектуру TCP/IP, можно выделить в ней, подобно архитектуре OSI (рис.54), уровни, функции которых зависят от конкретной технологической реализации сети, и уровни, функции которых ориентированы на работу только с приложениями и не зависят от технологий сети.

Протоколы прикладного уровня стека TCP/IP работают на компьютерах, выполняющих приложения пользователей. Даже полная смена сетевого оборудования в общем случае не должна влиять на работу приложений, если они получают доступ к сетевым возможностям через протоколы прикладного уровня.

Протоколы транспортного уровня уже более зависимы от сети, так как они реализуют интерфейс к уровням, непосредственно организующим передачу данных по сети. Однако подобно протоколам прикладного уровня, программные модули, реализующие протоколы транспортного уровня, устанавливаются только на конечных узлах.

Протоколы двух нижних уровней являются сетезависимыми, программные модули протоколов межсетевого уровня и уровня сетевых интерфейсов устанавливаются как на конечных узлах составной сети, так и на маршрутизаторах.

Единицы данных протоколов стека TCP/IP

Данные передаются в пакетах. Пакеты имеют заголовок и окончание, которые содержат служебную информацию. Данные, более верхних уровней вставляются, в пакеты нижних уровней.

Рис. 55. Пример инкапсуляции пакетов в стеке TCP/IP

Инкапсуляция — свойство языка программирования, позволяющее объединить и защитить данные и код в объект и скрыть реализацию объекта от пользователя (прикладного программиста). При этом пользователю предоставляется только спецификация (интерфейс) объекта.

Каждый коммуникационный протокол оперирует с некоторой единицей передаваемых данных. Названия этих единиц иногда закрепляются стандартом, но чаще просто определяются традицией. В стеке TCP/IP за многие годы его эксплуатации образовалась устоявшаяся терминология в этой области (таблица 3).

Таблица 3. единицы передачи данных

I	ПРИКЛАДНЫЕ ПРОТОКОЛЫ (поток)	
II	UDP (дейтаграмма)	TCP (сегмент)
III	IP (пакет или IP-дейтаграмма)	
IV	СЕТЕВЫЕ ИНТЕРФЕЙСЫ (кадр(фрейм))	

Потоком называют данные, поступающие от приложений на вход транспортного уровня TCP или UDP. Протокол TCP нарезает из потока ***сегменты.*** Единицу данных протокола UDP часто называют ***дейтаграммой.***

Дейтаграмма - это общее название для единиц данных, которыми оперируют протоколы без установления соединений. К таким протоколам относится

и протокол межсетевого взаимодействия IP. Дейтаграмму протокола IP называют также ***пакетом.***

В стеке TCP/IP принято называть ***кадрами (фреймами)*** единицы данных протоколов, на основе которых IP-пакеты переносятся через подсети составной сети. При этом не имеет значения, какое название используется для этой единицы данных в локальной технологии.

1.16. Физические среды передачи данных информационно вычислительных сетей

Стандарты кабелей

Кабель - это изделие, состоящее из проводников (металлических или оптических), слоев экрана и изоляции. Для обеспечения быстрой перекоммутации кабелей и оборудования используются различные электромеханические устройства, называемые *кроссовыми секциями, кроссовыми коробками или шкафами.* В данном материале мы не будем рассматривать огромное количество модификаций кабелей применяемых сегодня. Остановимся на рассмотрении узкого спектра кабельной продукции, а именно — кабели, применяемые при построении вычислительных сетей.

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-568A, который был разработан совместными усилиями нескольких организаций: ANSI, EIA/TIA и лабораторией Underwriters Labs (UL). Стандарт EIA/TIA-568 разработан на основе предыдущей версии стандарта EIA/TIA-568 и дополнений к этому стандарту TSB-36 и TSB-40A.
- Международный стандарт ISO/IEC 11801.
- Европейский стандарт EN50173.

Эти стандарты близки между собой и по многим позициям предъявляют к кабелям идентичные требования. Однако есть и различия между этими стандартами, например, в международный стандарт 11801 и европейский EN50173

вошли некоторые типы кабелей, которые отсутствуют в стандарте EIA/TAI-568A.

Базовые международные и европейские стандарты совпадают практически буквально. Однако ISO/IEC и CENELEC разрабатывают собственные стандарты в смежных областях. В Европе, например, существует Директива ЭМС, определены собственные параметры экранированных и оптоволоконных кабелей. Международная организация стандартизации ведет разработку стандартов проектирования, монтажа, администрирования, измерений и внедрения приложений. Россия принимает участие в работе Международной организации стандартизации (ISO), но не входит в CENELEC.

При стандартизации кабелей принят протокольно-независимый подход. Это означает, что в стандарте отовариваются электрические, оптические и механические характеристики, которым должен удовлетворять тот или иной тип кабеля или соединительного изделия - разъема, кроссовой коробки и т. п. Однако для какого протокола предназначен данный кабель, стандарт не оговаривает.

В ранних версиях стандартов определялись только характеристики кабелей, без соединителей. В последних версиях стандартов появились требования к соединительным элементам, а также к *линиям (каналам)*, представляющим ***типовую сборку элементов кабельной системы***, состоящую из *патч-корда* от рабочей станции до розетки, самой розетки, основного кабеля (длиной до 90 м для витой пары), точки перехода (например, еще одной розетки или жесткого кроссового соединения) и *патч-корда* до активного оборудования, например концентратора или коммутатора.

Коммутационный шнур, коммутационный кабель *или* ***патч-корд (от англ. patching cord— соединительный шнур)***— одна из составных частей структурированной кабельной системы. Представляет собой электрический кабель для подключения одного электрического устройства к другому. Может быть любых типов и размеров, на одном или обоих концах кабеля обязательно присутствуют соответствующие соединяемым устройствам коннекторы.

Кроссовер— разновидность патч-корда витой пары, используемого в компьютерных сетях. Особенностью является перекрестное (кроссовое) соединение концов кабеля с коннекторами. Применяется для соединения однотипных сетевых устройств: ПК-ПК, свитч-свитч и т.п. Следует заметить, что многие современные устройства автоматически определяют тип патч-корда (прямой или кроссовый), и могут совместно работать на любом из типов кабеля.

Кабели на основе неэкранированной витой пары

Медный неэкранированный кабель UTP (англ. Unshielded Twisted Pair) в зависимости от электрических и механических характеристик разделяется на 5 категорий (Category 1 - Category 5). Кабели категорий 1 и 2 были определены в стандарте EIA/TIA-568, но в стандарт 568A уже не вошли, как устаревшие.

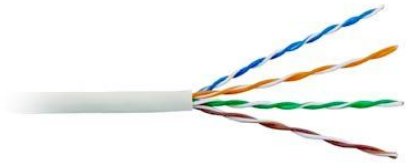


Рис. 56.кабель UTP 5 кат

Как видно на рисунке 56, конструктивно кабель состоит из 4-х скрученных между собой пар. Каждая пара состоит из 2-х металлических (как правило, медных) проводников в токонепроводящей оплётке, скрученных между собой.

Кроме того, металлический проводник в паре, может быть многожильным (patch) рис.57 или одножильным (solid)рис.58

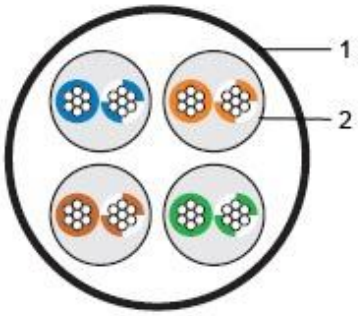


Рис. 57. кабель UTP в разрезе, с многожильными проводниками

1 - Внешняя оболочка
2 - Витая пара patch

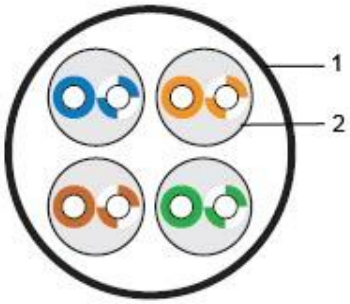


Рис. 58. кабель UTP в разрезе, с одножильными проводниками

1 - Внешняя оболочка
2 - Витая пара solid

В Росси аналоги кабеля U/UTP, F/UTP, принято маркировать КССПВ (UTP 4 Cat. 5), КВП-5е, КВПЭф-5е, КВПВП-5е, КВПЭфВП-5е.

Кабель симметричный для цифровых систем передачи данных с полиэтиленовой изоляцией, в оболочке из поливинилхлоридного пластиката ТУ16.К117-002-2003, ТУ16 К99-014-2004. Отвечает Международным стандартам ISO/IEC 11801, TIA/EIA 568A.

Кабели категории 1,CAT применяются там, где требования к скорости передачи минимальны. Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 Кбит/с) передачи данных. До недавнего времени это был основной тип кабеля для телефонной разводки.

Кабели категории 2,CAT2 были впервые применены фирмой IBM при построении собственной кабельной системы. Главное требование к кабелям этой категории - способность передавать сигналы со спектром до 1 МГц.

Кабели категории 3,CAT3 были стандартизованы в 1991 году, когда был разработан ***Стандарт телекоммуникационных кабельных систем для коммерческих зданий*** **(EIA-568),** на основе которого затем был создан действующий стандарт EIA-568A. Стандарт EIA-568 определил электрические характеристики кабелей категории 3 для частот в диапазоне до 16 МГц, поддерживающих, таким образом, высокоскоростные сетевые приложения. Кабель категории 3 предназначен как для передачи данных, так и для передачи голоса. Шаг скрутки проводов равен примерно 3 витка на 1 фут (30,5 см). Кабели категории 3 сейчас составляют основу многих кабельных систем зданий, в которых они используются для передачи и голоса, и данных.

Кабели категории 4,CAT4 представляют собой несколько улучшенный вариант кабелей категории 3. Кабели категории 4 обязаны выдерживать тесты на частоте передачи сигнала 20 МГц и обеспечивать повышенную помехоустойчивость и низкие потери сигнала. На практике используются редко.

Кабели категории 5,CAT5 были специально разработаны для поддержки высокоскоростных протоколов. Поэтому их характеристики определяются в диапазоне до 100 МГц. Большинство новых высокоскоростных стандартов ориентируются на использование витой пары 5 категории. На этом кабеле работают протоколы со скоростью передачи данных Fast Ethernet, l00VG-AnyLAN, а также Gigabit Ethernet на скорости 1000 Мбит/с. Кабель категории 5 пришел на замену кабелю категории 3, и сегодня все новые кабельные системы строятся именно на этом типе кабеля (в сочетании с волоконно-оптическим).

Наиболее важные электромагнитные характеристики кабеля категории 5:

- полное волновое сопротивление в диапазоне частот до 100 МГц равно 100 Ом (стандарт ISO 11801 допускает также кабель с волновым сопротивлением 120 Ом);
- величина перекрестных наводок NEXT в зависимости от частоты сигнала должна принимать значения не менее 74 дБ на частоте 150 кГц и не менее 32 дБ на частоте 100 МГц;

- затухание имеет предельные значения от 0,8 дБ (на частоте 64 кГц) до 22 дБ (на частоте 100 МГц);
- активное сопротивление не должно превышать 9,4 Ом на 100 м;
- емкость кабеля не должна превышать 5,6 нф на 100 м.

Кабели категории 5e, CAT5e (полоса частот 125 МГц)— 4-парный кабель, усовершенствованная категория 5. Скорость передач данных до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар. Кабель категории 5e является самым распространённым и используется для построения компьютерных сетей. Ограничение на длину кабеля между устройствами (компьютер-свитч, свитч-компьютер, свитч-свитч)— 100 м.

Кабели категории 6, CAT6 (полоса частот 250 МГц)— применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с. Добавлен в стандарт в июне 2002 года. По данным IEEE, 70% установленных сетей в 2004 году, использовали кабель категории CAT6.

Кабели категории, CAT6a (полоса частот 500 МГц)— применяется в сетях Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 10 гигабит/с и планируется использовать его для приложений, работающих на скорости до 40 гигабит/с. Добавлен в стандарт в феврале 2008 года.

Кабели категории,CAT7— спецификация на данный тип кабеля утверждена только международным стандартом ISO 11801, скорость передачи данных до 100 Гбит/с, частота пропускаемого сигнала до 600—700 МГц. Кабель этой категории имеет общий экран и экраны вокруг каждой пары. Седьмая категория, строго говоря, не UTP, а S/FTP (Screened Fully Shielded Twisted Pair).

Каждая отдельно взятая витая пара, входящая в состав кабеля, предназначенного для передачи данных, должна иметь волновое сопротивление 120 Ом ±20 Ом, в противном случае форма электрического сигнала будет искажена и передача данных станет невозможной. Причиной проблем с передачей данных может быть не только некачественный кабель, но также наличие «скруток» в кабеле и использование розеток более низкой категории, чем кабель.

Все кабели UTP независимо от их категории выпускаются в 4-парном исполнении. Каждая из четырех пар кабеля имеет определенный цвет и шаг скрутки.

Таблица 4. Цветовая маркировка жил в кабеле

Контакт	Сигнал	Цвет	
		MDI (TIA/EIA-	MDI-X (TIA/EIA-

		568-B)	568-A)
1	Передача +	 Белый/оранжевый	 Белый/зелёный
2	Передача -	 Оранжевый	 Зелёный
3	Приём +	 Белый/зелёный	 Белый/оранжевый
4	Не используется	 Синий	 Синий
5	Не используется	 Белый/синий	 Белый/синий
6	Приём -	 Зелёный	 Оранжевый
7	Не используется	 Белый/коричневый	 Белый/коричневый
8	Не используется	 Коричневый	 Коричневый

Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,4—0,6 мм. (Кроме метрической, применяется американская система AWG, в которой эти величины составляют 26AWG или 22AWG соответственно).

В стандартных 4-х парных кабелях в основном используются проводники диаметром 0,51 мм (24AWG). Толщина изоляции проводника— около 0,2 мм, материал обычно поливинилхлорид (английское сокращение PVC), для более качественных образцов 5 категории — полипропилен (PP), полиэтилен (PE). Особенно высококачественные кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрические потери, или тефлона, обеспечивающего высокий рабочий диапазон температур.

Также внутри кабеля встречается так называемая «разрывная нить» (обычно капрон), которая используется для облегчения разделки внешней оболочки— при вытягивании она делает на оболочке продольный разрез, который открывает доступ к кабельному сердечнику, гарантированно не повреждая изоляцию проводников. Также разрывная нить, ввиду своей высокой прочности на разрыв, выполняет защитную функцию.

Внешняя оболочка 4-х парных кабелей имеет толщину 5—9мм в зависимости от категории кабеля и обычно изготавливается из поливинилхлорида с добавлением мела, который повышает хрупкость. Это необходимо для точного облома по месту надреза лезвием отрезного инструмента. Кроме этого, для изготовления оболочки используются полимеры, которые не поддерживают горения и не выделяют при нагреве галогены (такие кабели маркируются как

LSZH— Low Smoke Zero Halogen). Кабели, не поддерживающие горение и не выделяющие дым, разрешается прокладывать и использовать в закрытых областях, где могут проходить воздушные потоки системы кондиционирования и вентиляции.

В общем случае, цвета не обозначают особых свойств, но их применение позволяет легко отличать коммуникации с разным функциональным назначением, как при монтаже, так и обслуживании. Самый распространённый цвет оболочки кабелей— серый. У внешних кабелей внешняя оболочка чёрного цвета. Оранжевая окраска, как правило, указывает на негорючий материал оболочки.

Отдельно нужно отметить маркировку. Кроме данных о производителе и типе кабеля, она обязательно включает в себя метровые или футовые метки.

Форма внешней оболочки кабеля витая пара может быть различной. Чаще других применяется круглая форма. Для прокладки под ковровым покрытием может использоваться плоский кабель.

Кабели для наружной прокладки обязательно имеют влагостойкую оболочку из полиэтилена, которая наносится (как правило) вторым слоем поверх обычной, поливинилхлоридной. Кроме этого, возможно заполнение пустот в кабеле водоотталкивающим гелем и бронирование с помощью гофрированной ленты или стальной проволоки.

8P8C (8 Position 8 Contact), часто ошибочно называемый ***RJ45 или RJ-45***— унифицированный разъём, используемый в телекоммуникациях, имеет 8 контактов и защёлку.

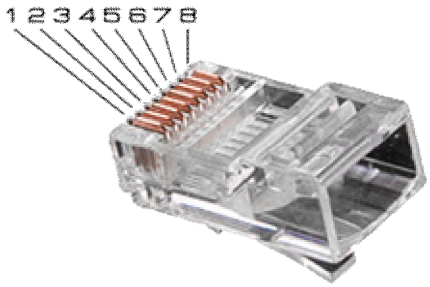


Рис. 59. вид разъёма 8P8C

Термин **«RJ45»** ошибочно употребляется для именования разъёма 8P8C, используемого в компьютерных сетях. На самом деле **настоящий RJ45 физически несовместим с 8P8C, так как использует схему 8P2C с ключом**. Ошибочное употребление термина «RJ45» вызвано, вероятно, тем, что настоящий RJ45 не получил широкого применения, а также их внешним сходством

Рис. 60. Обжимной инструмент, Crimping tool (кримпер)

Кримпер (рис.60), используется для создания ЛВС по технологиям 10BASE-T, 100BASE-T и 1000BASE-TX с использованием 4-парных кабелей витой пары. Также применяется во многих других областях и для построения иных сетей.

Registered jack (RJ, читается «ар-джей») — это стандартизированный физический интерфейс, используемый для соединения телекоммуникационного оборудования (обычно — телефонов) или в компьютерных сетях. Стандартные варианты этого разъёма называются RJ11, RJ14, RJ25, RJ45 и так да-

Рис. 61. разъём 6P6C (RG12)

Рис. 62. Разъём 4P4C (RG11)

Телефонный унифицированный разъём RJ-11 меньше по размеру и может вставляться в гнёзда 8P8C (для обратной совместимости).

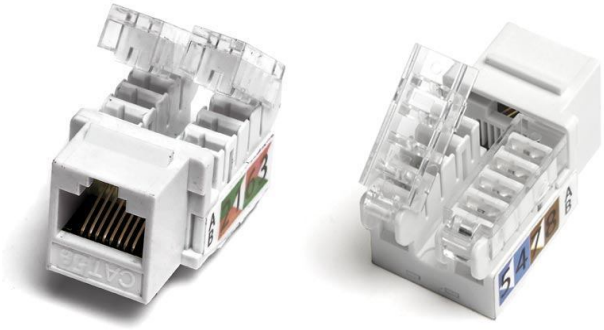


Рис. 63. розетка для разъёма 8P8C (RG45)

Особое место занимают кабели ***категорий 6 и 7***. Для кабеля категории 6 характеристики определяются до частоты 200 МГц, а для кабелей категории 7 - до 600 МГц. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель категории 6 может быть как экранированным, так и неэкранированным. Основное назначение этих кабелей - поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5. Некоторые специалисты сомневаются в необходимости применения кабелей категории 7, так как стоимость кабельной системы при их использовании получается соизмеримой по стоимости сети с использованием волоконно-оптических кабелей, а характеристики кабелей на основе оптических волокон выше.

Кабели на основе экранированной витой пары

Экранированная витая пара STP (англ. S*hielded Twisted Pair)* хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения, (рис.64). Наличие заземляемого экрана удорожает кабель и усложняет его прокладку, так как требует выполнения качественного заземления.

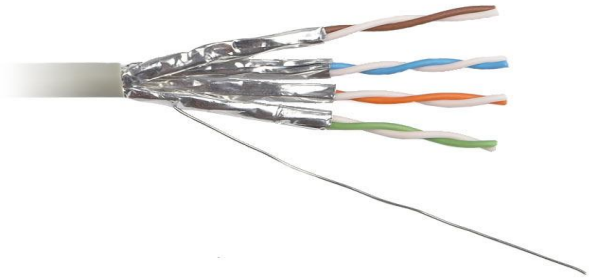


Рис. 64. кабель типа STP

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

Основным типом экранированного кабеля является кабель Type 1 стандарта IBM. Он состоит из 2-х пар скрученных проводов, экранированных проводящей оплеткой, которая заземляется. Электрические параметры кабеля Type 1 примерно соответствуют параметрам кабеля UTP категории 5. Однако волновое сопротивление кабеля Type 1 равно 150 Ом (UTP категории 5 имеет волновое сопротивление 100 Ом), поэтому простое «улучшение» кабельной проводки сети путем замены неэкранированной пары UTP на STP Type 1 невозможно. Трансиверы, рассчитанные на работу с кабелем, имеющим волновое сопротивление 100 Ом, будут плохо работать на волновое сопротивление 150 Ом. Поэтому при использовании STP Type 1 необходимы соответствующие трансиверы. Такие трансиверы имеются в сетевых адаптерах Token Ring, так как эти сети разрабатывались для работы на экранированной витой паре. Некоторые другие стандарты также поддерживают кабель STP Type I - например, l00VG-AnyLAN, а также Fast Ethernet (хотя основным типом кабеля для Fast Ethernet является UTP категории 5). В случае если технология может использовать UTP и STP, нужно убедиться, на какой тип кабеля рассчитаны приобретаемые трансиверы.

Сегодня кабель STP Type 1 включен в стандарты EIA/TIA-568A, ISO 11801 и EN50173, то есть приобрел международный статус. Разные авторы и производители кабеля по разному называют этот тип кабеля. Но общим во всех случаях является наличие экрана (вокруг каждой пары и/или вокруг всех пар), изготовленного из фольги, металлической оплётки и т.п.

Кроме того кабели UTP и STP могут быть конструктивно выполнены для внешней прокладки, и иметь отличную внешнюю оплётку, различную форму сечении (круглую или плоскую) различные варианты исполнения экрана и/или дополнительные усиливающие элементы (рисунок 65).

В зависимости от наличия защиты— электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

незащищенная витая пара (UTP— Unshielded twisted pair)— отсутствует защитный экран вокруг отдельной пары;

фольгированная витая пара (FTP— Foiled twisted pair)— также известна как F/UTP, присутствует один общий внешний экран в виде фольги;

защищенная витая пара (STP— Shielded twisted pair)— присутствует защита в виде экрана для каждой пары и общий внешний экран в виде сетки;

Рис. 65. Кабель STP для внешней прокладки, с несущей стальной жилой

фольгированная экранированная витая пара (S/FTP— Screened Foiled twisted pair)— внешний экран из медной оплетки и каждая пара в фольгированной оплетке;

незащищенная экранированная витая пара (SF/UTP— Screened Foiled Unshielded twisted pair)— двойной внешний экран из медной оплетки и фольги, каждая витая пара без защиты.

Волоконно-оптические кабели

Волоконно-оптические кабели состоят из центрального проводника света (сердцевины) - стеклянного волокна, окруженного другим слоем стекла - оболочкой, обладающей меньшим показателем преломления, чем сердцевина. Распространяясь по сердцевине, лучи света не выходят за ее пределы, отражаясь от покрывающего слоя оболочки.

Рис. 66. Волоконно-оптический кабель

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

- многомодовое волокно со ступенчатым изменением показателя преломления;

- многомодовое волокно с плавным изменением показателя преломления;
- одномодовое волокно.

В многомодовых кабелях во внутреннем проводнике одновременно существует несколько световых лучей, отражающихся от внешнего проводника под разными углами. Угол отражения луча называется ***модой луча***. В многомодовых кабелях с плавным изменением коэффициента преломления режим распространения каждой моды имеет более сложный характер.

Многомодовые волокна отличаются от одномодовых диаметром сердцевины, который составляет 50 микрон в европейском стандарте и 62,5 микрон в североамериканском и японском стандартах. Из-за большого диаметра сердцевины по многомодовому волокну распространяется несколько мод излучения— каждая под своим углом, из-за чего импульс света испытывает дисперсионные искажения и из прямоугольного превращается в колоколо-подобный.

Многомодовое волокно со ступенчатым изменением показателя преломления

В ступенчатом оптоволокне могут возбуждаться и распространяться до тысячи мод с различным распределением по сечению и длине оптоволокна. Моды имеют различные оптические пути и, следовательно, различные времена распространения по оптоволокну, что приводит к уширению импульса света по мере его прохождения по оптоволокну. Это явление называется межмодовой дисперсией и оно непосредственно влияет на скорость передачи информации по оптоволокну.

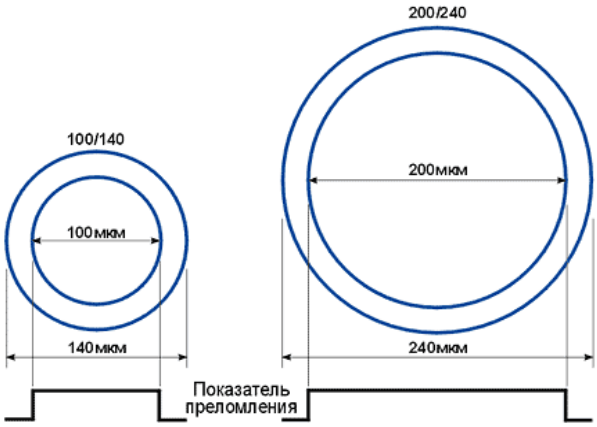


Рис. 67. Многомодовое волокно со ступенчатым изменением показателя преломления

Область применения ступенчатых оптоволокон короткие (до 1 км) линии связи со скоростями передачи информации до 100 Мбайт/с, рабочая длина волны излучения, как правило, 0,85 мкм.

Понятие **«мода»** описывает режим распространения световых лучей во внутреннем сердечнике кабеля.

Межмодовая дисперсия - дисперсия электромагнитного излучения, возникающая в многомодовых световодах из-за наличия в них большого числа мод с различным временем распространения

Многомодовое волокно с плавным изменением показателя преломления

Отличается от ступенчатого тем, что показатель преломления сердцевины плавно возрастает от края к центру. Это приводит к явлению рефракции в сердцевине, благодаря чему снижается влияние межмодовой дисперсии на искажение оптического импульса. Профиль показателя преломления градиентного волокна может быть параболическим, треугольным, ломаным и т.д.

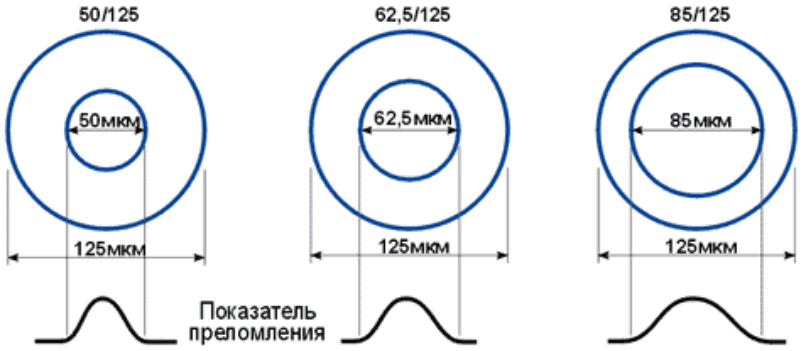


Рис. 68.Градиентное многомодовое оптоволокно

В ***многомодовых кабелях (Multi Mode Fiber, MMF)*** используются более широкие, чем в одномодовых, внутренние сердечники. В стандартах определены два наиболее употребительных многомодовых кабеля: 62,5/125 мкм и 50/125 мкм, где 62,5 мкм или 50 мкм - это диаметр центрального проводника, а 125 мкм - диаметр внешнего проводника.

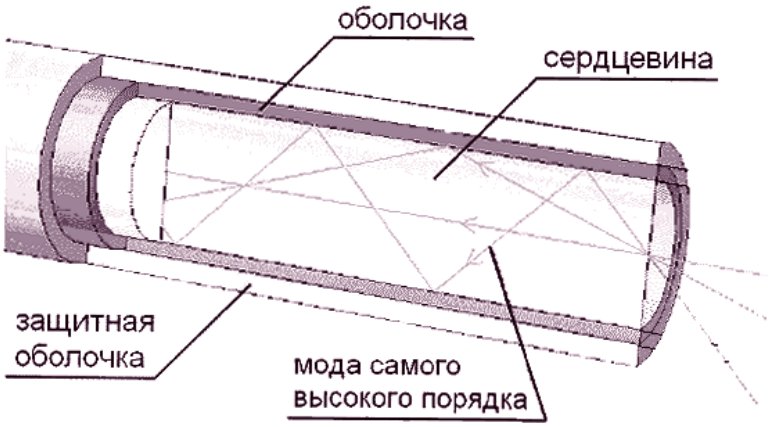


Рис. 69.Многомодовый оптический кабель в разрезе.

Многомодовые кабели имеют более узкую полосу пропускания - от 500 до 800 МГц/км. Сужение полосы происходит из-за потерь световой энергии при отражениях, а также из-за интерференции лучей разных мод.

Одномодовое волокно

Стандартное одномодовое оптическое волокно имеет диаметр сердцевины 7-9 мкм и диаметр оболочки 125 мкм. В этом оптоволокне существует и распространяется только одна мода (точнее две вырожденные моды с ортогональными поляризациями), поэтому в нем отсутствует межмодовая дисперсия, что позволяет передавать сигналы на расстояние до 50 км со скоростью до 2,5 Гбит/с и выше без регенерации. Рабочие длины волн $\lambda 1 = 1{,}31$ мкм и $\lambda 2 = 1{,}55$ мкм.

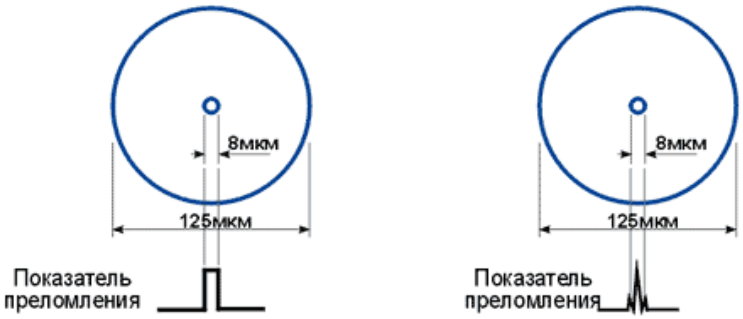


Рис. 70. Одномодовое оптоволокно

В одномодовом кабеле (Single Mode Fiber, SMF) используется центральный проводник очень малого диаметра, соизмеримого с длиной волны света - от 5 до 10 мкм. При этом практически все лучи света распространяются вдоль

оптической оси световода, не отражаясь от внешнего проводника. Полоса пропускания одномодового кабеля очень широкая - до сотен гигагерц на километр.

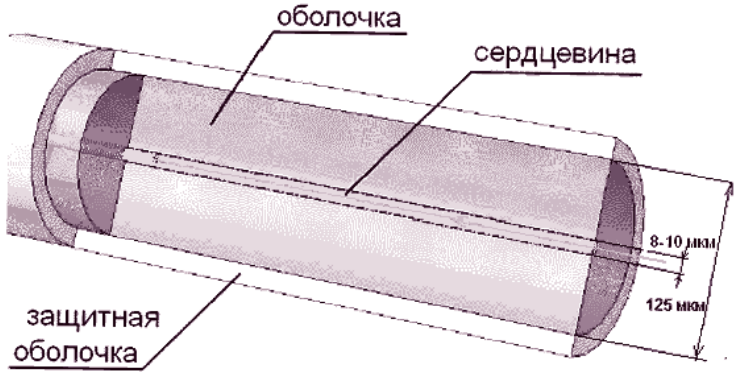


Рис. 71. Одномодовый оптический кабель в разрезе

Существует три основных типа одномодовых волокон:

Одномодовое ступенчатое волокно с несмещённой дисперсией (стандартное) (англ. SMF— Step Index Single Mode Fiber), определяется рекомендацией ITU-T G.652 и применяется в большинстве оптических систем связи.

Одномодовое волокно со смещённой дисперсией (англ. DSF— Dispersion Shifted Single Mode Fiber), определяется рекомендацией ITU-T G.653. В волокнах DSF с помощью примесей область нулевой дисперсии смещена в третье окно прозрачности, в котором наблюдается минимальное затухание.

Одномодовое волокно с ненулевой смещённой дисперсией (англ. NZDSF— Non-Zero Dispersion Shifted Single Mode Fiber), определяется рекомендацией ITU-T G.655.

Оптимизация трех перечисленных типов одномодовых волокон совершенно не означает, что они всегда должны использоваться исключительно под определенные задачи: SF - передача сигнала на длине волны 1310 нм, DSF - передача сигнала на длине волны 1550 нм, NZDSF - передача мультиплексного сигнала в окне 1530-1560 нм. Так, например, мультиплексный сигнал в окне 1530-1560 нм можно передавать и по стандартному ступенчатому одномодовому волокну SF. Однако длина безретрансляционного участка при использовании волокна SF будет меньше, чем при использовании NZDSF, или иначе потребуется очень узкая полоса спектрального излучения лазерных передатчиков для уменьшения результирующей хроматической дисперсии. Максимальное допустимое расстояние определяется техническими характеристиками как самого волокна (затуханием, дисперсией), так и приемо-передающего оборудования (мощностью, частотой, спектральным уширением излучения передатчика, чувствительностью приемника).

Окна прозрачности оптоволокна

Окно прозрачности - диапазон длин волн оптического излучения, в котором имеет место меньшее, по сравнению с другими диапазонами, затухание излучения в среде, в частности - в оптическом волокне. Стандартное ступенчатое оптическое волокно SMF имеет три окна прозрачности: 850 нм, 1310 нм и 1550 нм. К настоящему времени разработаны четвёртое (1580 нм) и пятое (1400 нм) окна прозрачности, а так же оптические волокна, имеющие относительно хорошую прозрачность во всём ближнем инфракрасном диапазоне.

Неоднородность затухания света в оптическом волокне в разных диапазонах длин волн обусловлено не идеальностью среды, наличием примесей, резонирующих на разных частотах.

Затухание в разных окнах прозрачности неодинаково: наименьшая его величина— 0,22 дБ/км наблюдается на длине волны 1550 нм, поэтому третье окно прозрачности используется для организации связи на большие расстояния. Во втором окне прозрачности (1310 нм) затухание выше, однако для этой длины волны характерна нулевая дисперсия, поэтому второе окно используется на городских и зоновых сетях небольшой протяжённости. Первое окно прозрачности используется в офисных оптических сетях.

Первоначально, в 70-х годах, системы волоконно-оптической связи использовали первое окно прозрачности, поскольку выпускаемые в то время GaAs-лазеры работали на длине волны 850 нм. В настоящее время этот диапазон из-за большого затухания используется только в локальных сетях.

В 80-х годах были разработаны лазеры на тройных и четверных гетероструктурах, способные работать на длине волны 1310 нм и второе окно прозрачности стало использоваться для дальней связи. Преимуществом данного диапазона явилась нулевая дисперсия на данной длине волны, что существенно уменьшало искажение оптических импульсов.

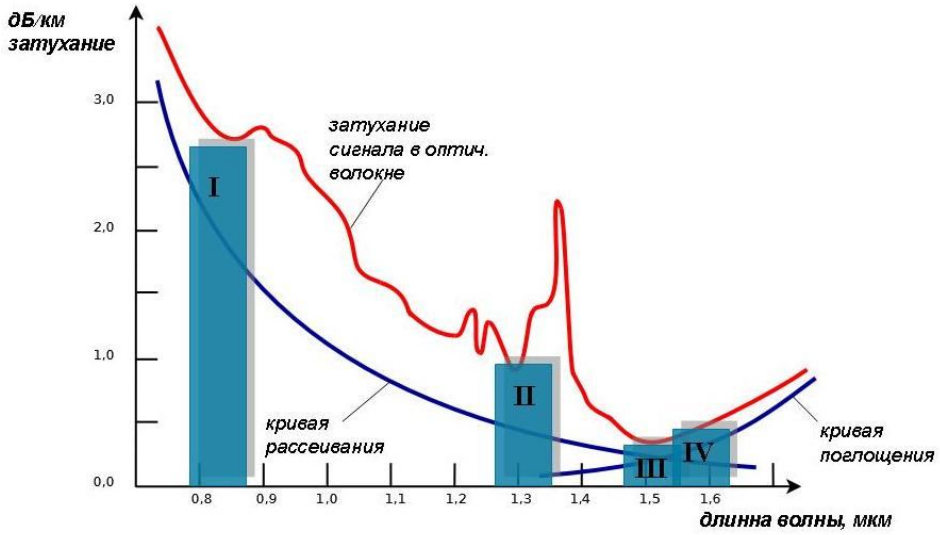


Рис. 72. Окна прозрачности оптоволокна.

Третье окно прозрачности было освоено в начале 90-х годов. Преимуществом третьего окна является не только минимум потерь, но и тот факт, что на длину волны 1550 нм приходится рабочий диапазон волоконно-оптических эрбиевых усилители (EDFA). Данный тип усилителей, имея способность усиливать все частоты рабочей области, предопределил использование третьего окна прозрачности для систем со спектральным уплотнением (WDM).

Четвёртое окно прозрачности простирается до длины волны 1620 нм, увеличивая рабочий диапазон систем WDM.

Пятое окно прозрачности появилось в результате тщательной очистки оптического волокна от посторонних примесей. Таким образом, было получено оптическое волокно AllWave, имеющее малые потери во всей области от 1280 нм до 1650 нм.

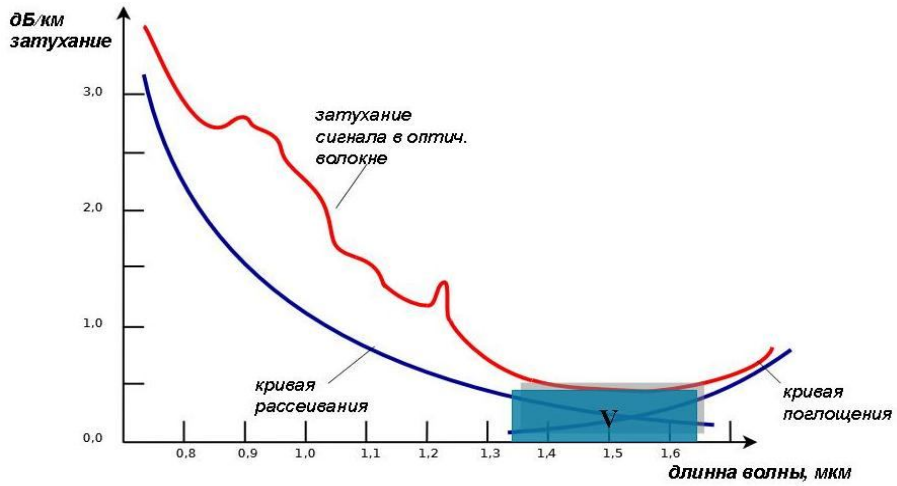


Рис. 73. Окна прозрачности оптоволокна.

Данный тип оптического волокна, производимый фирмой **Lucent** является достаточно интересным усовершенствованием стандартного одномодового волокна. В отличие от стандартного одномодового волокна данное оптическое волокно не имеет так называемого **«водяного пика»**, т. е. увеличения поглощения на длине волны 1,385 мкм, соответствующей спектру поглощения ионов OH. На этой длине волны поглощение составляет 0,31 дБ/км. Данный тип оптического волокна предлагается использовать в локальных и местных сетях связи с небольшой протяженностью *регенерационных участков*, но с одновременным использованием всего спектрального диапазона от 1,3 до 1,6 мкм.

В связи с расширением рабочего диапазона оптических волокон Международным союзом электросвязи были утверждены новые спектральные диапазоны в интервале 1260…1675 нм:

Таблица 5. Спектральные диапазоны

Обозначение	Диапазон, нм	Русское название	Английское название
O	1260…1360	Основной	Original
E	1360…1460	Расширенный	Extended
S	1460…1530	Коротковолновый	Short wavelength
C	1530…1565	Стандартный	Conventional
L	1565…1625	Длинноволновый	Long wavelength
U	1625…1675	Сверхдлинноволновый	Ultra-long wavelengh

Международный союз электросвязи сокращённо **МСЭ** (англ. International Telecommunication Union, ITU) — международная организация, определяющая рекомендации в области телекоммуникаций и радио, а также регулирующая вопросы международного использования радиочастот (распределение радиочастот по назначениям и по странам).

В качестве источников излучения света в волоконно-оптических кабелях применяются:

- светодиоды;
- полупроводниковые лазеры.

Для передачи информации применяется свет с длиной волны 1550 нм (1,55 мкм), 1300 нм (1,3 мкм) и 850 нм (0,85 мкм). Светодиоды могут излучать свет с длиной волны 850 нм и 1300 нм. Излучатели с длиной волны 850 нм существенно дешевле, чем излучатели с длиной волны 1300 нм, но полоса пропускания кабеля для волн 850 нм уже, например 200 МГц/км вместо 500 МГц/км.

Лазерные излучатели работают на длинах волн 1300 и 1550 нм. Быстродействие современных лазеров позволяет модулировать световой поток с частотами 10 ГГц и выше. Лазерные излучатели создают когерентный поток света, за счет чего потери в оптических волокнах становятся меньше, чем при использовании некогерентного потока светодиодов.

Использование только нескольких длин волн для передачи информации в оптических волокнах связанно с особенностью их амплитудно-частотной характеристики. Именно для этих дискретных длин волн наблюдаются ярко выраженные максимумы передачи мощности сигнала, а для других волн затухание в волокнах существенно выше.

Волоконно-оптические кабели присоединяют к оборудованию разъемами MTRJ, ST,FC, SC.

Рис. 74. Разъем FC

Рис. 75. Разъем SC

Рис. 76. Разъем MTRJ

Рис. 77. Разъем ST

Волоконно-оптические кабели обладают отличными характеристиками всех типов: электромагнитными, механическими (хорошо гнутся, а в соответствующей изоляции обладают хорошей механической прочностью). Однако у них есть один серьезный недостаток - сложность соединения волокон с разъемами и между собой при необходимости наращивания длины кабеля.

1.17. Организация локальной вычислительной сети (ЛВС)

Общие понятия

Не надо говорить о роли и важности грамотно организованной, безупречно работающей локальной вычислительной сети предприятия. Часто именно ЛВС является гарантом успешного бизнеса. И наоборот при плохой организации, недостаточном внимании к вопросам её построения и обновления, наступает коллапс в организации труда на предприятии. Если перефразировать известную поговорку, то можно сказать: «ЛВС — как воздух, её не замечают когда она есть, и задыхаются когда её нет».

Повсюду мы сталкиваемся с различными исполнениями локальных вычислительных сетей. Нередко из домовых ЛВС, разрастаясь до масштабов района или целого города, вычислительная сеть становится городской (MAN).

Локальная вычислительная сеть должна обладать рядом свойств:

Масштабируемость – на первоначальном этапе организация может вложить минимум средств на прокладку локальных сетей, которые бы отвечали ее текущим целям и задачам. В будущем, при возникновении необходимости, она всегда сможет с легкостью расширить сети и подключить дополнительное оборудование.

Гибкость – для своевременного реагирования на меняющиеся требования технологий к существующей локальной сети необходимо наличие ее гибкости. Другими словами, сеть должна быть адаптированной для большинства типов сетевых кабелей: витой пары, коаксиальной, а также оптоволоконной, причем желательно поддержка технологий, начиная от Ethernet, Fast Ethernet, до Gigabit Ethernet и выше.

Отказоустойчивость – система локальных сетей в обязательном порядке включает резервные линии на случай, если основные по ряду причин выйдут из строя. Например, можно подключить сервер (серверную ферму) к нескольким коммутаторам/маршрутизаторам, имеющим запасные пути – при сбое одного концентратора/маршрутизатора всегда можно быстро перейти на другой в автоматическом режиме, не прерывая сеанса связи.

Надежность – длительное использование локальной сети в соответствии с возрастающей потребностью в ней предполагает необходимость поиска оптимальных вариантов для повышения ее надежности, так как вынужденные простои обходятся для организации слишком дорого, когда ценна каждая минута. Поэтому нельзя пренебрегать существующими программно-аппаратными средствами и инструментами, позволяющими повысить надежность локальных сетей.

Защита – важным свойством является защищенность сетей от несанкционированного вторжения через Интернет, а также внутренние действия пользователей. Решается с помощью комплекса мер, в том числе программно аппаратных средств – концентратора, коммутатора, маршрутизатора, межсетевого экрана, сервера удаленного доступа, а также административных мер, что в целом дает возможность полного контроля над текущими процессами и гарантирует сохранность важнейших данных организации.

Управляемость – локальная сеть должна иметь мощные средства для ее мониторинга, для быстрого выявления помех и неисправностей, чтобы исключить возможные простои, упомянутые выше. Существует множество продуктов, рассчитанных на оперативный сбор технической информации о состоянии сети и ее параметрах – примером могут служить средства SNMP, RMON. Помимо этого, есть возможность управления сетью через Web-интерфейс, который может использоваться практически в любом месте для удаленного доступа.

В простейшем случае локальная вычислительная сеть состоит из двух компьютеров оснащённых сетевой картой, соединённых между собой соответствующим образом оконцованным кабелем (коаксиальный или витая пара). Нужно помнить, что в такой схеме используется не стандартный патч-корд, а так называемый ***кроссовер.*** И конечно же нужно не забывать о том, что расстояние между ПК должно быть не более 100 м.

Решение когда ЛВС состоит из двух ПК, может быть реализовано и по беспроводной технологии, в этом случае оба компьютера оснащаются беспроводными сетевыми картами(адаптерами), и соединяются в режиме «точка-точка».

Сетевая плата, также известная как сетевая карта, сетевой адаптер, Ethernet-адаптер, NIC (англ. network interface controller)— периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.
SNMP (англ. Simple Network Management Protocol— протокол простого управления сетями) — это протокол управления сетями связи на основе архитектуры TCP/IP.
RMON— протокол мониторинга компьютерных сетей, расширение SNMP, в основе которого, как и в основе SNMP, лежит сбор и анализ информации о характере информации, передаваемой по сети. Как и в SNMP, сбор информации осуществляется аппаратно-программными агентами, данные от которых поступают на компьютер, где установлено приложение управления сетью. Отличие RMON от своего предшественника состоит, в первую очередь, в характере собираемой информации— если в SNMP эта информация характеризует только события, происходящие на том устройстве, где установлен агент, то RMON требует, чтобы получаемые данные характеризовали трафик между сетевыми устройствами.

Указанный выше способ организации сети из двух компьютеров прост, и не требует особых затрат, такая реализация ЛВС, встречается всё реже и реже. Однако реалии сегодняшнего дня таковы, что ЛВС предприятий насчитывают в своём составе десятки и сотни компьютеров и сетевых устройств (коммутаторы, шлюзы, принт-серверы, серверы, сетевые устройства хранения информации и т.д.), кроме того практически все ЛВС имеют выход в глобальную сеть INTERNET.

Организация локальной сети (еще до настройки локальной сети) в обязательном порядке начинается с определения ключевых моментов. Вот некоторые из них:

- Определение количества станций (портов, хостов) будущей сети;
- Планирование общего хранилища данных;
- Предполагаемое программное обеспечение;
- Предполагаемые сервисы (IP-телефония, видео наблюдение, и пр.);
- Востребованность единого информационного пространства для структурных подразделений компании;
- Вероятность использования локальной сети для построения единой корпоративной информационной платформы (интранет).

Существует несколько вариантов организации локальной сети. В качестве среды передачи данных может использоваться витой кабель UTP/STP (как правило категории 5е и выше) или оптоволоконный кабель. Возможна и организация локальных сетей при помощи беспроводной технологии. При этом построение и настройка локальной сети будет сильно различаться в зависимости от используемой технологии - беспроводной и проводной.

Построение локальной сети будет в значительной степени обусловлено ее размерами и способом размещения компьютеров. Среди других факторов, влияющих на организацию и настройку локальной сети, стоит отметить наличие серверов, количество рабочих мест, а также количество зданий, в которых функционирует ЛВС.

На этапе создания локальной сети и настройки локальной сети важно иметь четкое представление об архитектуре (топологии) сети. Топология сети зависит от места нахождения ПК и их функционального назначения. Выбор топологии в процессе создания локальной сети и настройки локальной сети происходит индивидуально - под конкретный объект своя архитектура.

Для проведения монтажа локальной сети подбирается необходимое для каждого варианта сетевое оборудование, причем, желательно от одного надежного производителя.

Компания D-Link, предлагает весь спектр активного сетевого оборудования для построения (модернизации) локальных вычислительных сетей, любого уровня сложности. Кроме того немаловажным является факт наличия широко разветвлённого сервисного обслуживания оборудования D-Link.

После того как определены все ключевые моменты связанные с организацией будущей сети приступают к созданию кабельной системы (в случае проводного решения ЛВС).

Интранет (англ. Intranet, также употребляется термин интрасеть) - в отличие от сети Интернет, это внутренняя частная сеть организации. Как правило, Интранет - это Интернет в миниатюре, который построен на использовании протокола IP для обмена и совместного использования некоторой части информации внутри этой организации. Это могут быть списки сотрудников, списки телефонов партнеров и заказчиков. Чаще всего под этим термином имеют в виду только видимую часть Интранет - внутренний веб-сайт организации. Основанный на базовых протоколах HTTP и HTTPS и организованный по принципу клиент-сервер, интранет-сайт доступен с любого компьютера. Таким образом, Интранет - это как бы «частный» Интернет, ограниченный виртуальным пространством отдельно взятой организации. Intranet допускает использование публичных каналов связи, входящих в Internet, (VPN), но при этом обеспечивается защита передаваемых данных и меры по пресечению проникновения извне на корпоративные узлы.

Структурированная кабельная система (СКС)

Кабельная система — это система, элементами которой являются кабели и компоненты, которые связаны с кабелем. К кабельным компонентам относится все ***пассивное коммутационное оборудование***, служащее для соединения или физического окончания (терминирования) кабеля — ***телекоммуникационные розетки*** на рабочих местах, ***кроссовые и коммутационные панели*** (жаргон ***патч-панели***) в телекоммуникационных помещениях, муфты и сплайсы.

В последнее время при организации ЛВС, применительно к кабельной системе, чаще всего используют термин ***структурированная кабельная система (СКС).***

Структурированная кабельная система (СКС) — основа информационной инфраструктуры предприятия, позволяющая свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, видео наблюдения и т.д.

СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Она состоит из набора медных и оптических кабелей, кросс-панелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомога-

тельного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам.

Термин ***«структурированная»*** означает, с одной стороны, способность системы поддерживать различные телекоммуникационные приложения (передачу речи, данных и видеоизображений), с другой — возможность применения различных компонентов и продукции различных производителей, и с третьей — способность к реализации так называемой мультимедийной среды, в которой используются несколько типов передающих сред — коаксиальный кабель, UTP, STP и оптическое волокно. Структуру кабельной системы определяет инфраструктура информационных технологий (от англ. IT, Information Technology), именно она диктует содержание конкретного проекта кабельной системы в соответствии с требованиями конечного пользователя, независимо от активного оборудования, которое может применяться впоследствии.

Типовые работы по монтажу СКС включают:

- установку кабельных каналов (коробах, лотках, гофротрубе, трубах и т.п.);
- пробивку отверстий в стенах;
- прокладку кабеля в кабельных каналах;
- установку розеток и заделку кабеля модули розетки;
- сборку и установку монтажного шкафа;
- установку и набивку патч-панелей и органайзеров.

Этапы монтажа СКС:

- Изучение объекта для монтажа СКС;
- Разработка технического проекта;
- Подбор необходимого оборудования и монтаж на объекте;
- Тестирование и сертификация, сдача работ заказчику;
- После установочная поддержка и обучение

Компоненты СКС

При создании СКС применяются. ***Кабели***, ***разъёмы***, ***розетки и патч-корды*** используемые в вычислительных сетях. В вкратце напомним:

Медный неэкранированный кабель UTP (англ. Unshielded Twisted Pair) в зависимости от электрических и механических характеристик разделяется на 5 категорий (Category 1 - Category 5).

Экранированная витая пара STP (англ. Shielded Twisted Pair) хорошо защищает передаваемые сигналы от внешних помех, а также меньше излучает

электромагнитных колебаний вовне, что защищает, в свою очередь, пользователей сетей от вредного для здоровья излучения. Особое место занимают кабели ***категорий 6 и 7,*** которые промышленность начала выпускать сравнительно недавно. Для кабеля категории 6 характеристики определяются до частоты 200 МГц, а для кабелей категории 7 - до 600 МГц. Кабели категории 7 обязательно экранируются, причем как каждая пара, так и весь кабель в целом. Кабель категории 6 может быть как экранированным, так и неэкранированным. Основное назначение этих кабелей - поддержка высокоскоростных протоколов на отрезках кабеля большей длины, чем кабель UTP категории 5.

8P8C (8 Position 8 Contact), часто ошибочно называемый ***RJ45 или RJ-45***— унифицированный разъём, используемый в телекоммуникациях, имеет 8 контактов и защёлку.

Информационные розетки, как правило, универсальные, они служат точкой входа в кабельную систему для всей офисной техники, включающей не только компьютер и другие периферийные устройства, но и телефон (т.е. возможно подключение шнура с разъёмом RJ-11(12).

Коммутационная панель (кросс-панель, патч-панель) — одна из составных частей структурированной кабельной системы (СКС). Представляет из себя панель со множеством соединительных разъёмов, расположенных на лицевой стороне панели. На тыльной стороне панели находятся контакты, предназначенные для фиксированного соединения с кабелями, и соединённые с разъёмами электрически. Коммутационная панель относится к пассивному сетевому оборудованию. Коммутационные панели могут быть *фиксированными или наборными*. Если в первом случае, все разъемы выполняются однотипными, то в другом случае можно реализовать гибридную коммутационную панель, содержащую разъемы разных типов, в том числе медные типа RJ45 разной категорийности, волоконно-оптические разъемы различных типов, коаксиальные (например, типа BNC) и другие. Типы устанавливаемых видов разъемов зависят от вида решаемых задач. Наиболее распространенным видом данного вида устройств, в современных технологиях СКС, является 24-х портовая фиксированная коммутационная панель с неэкранированными разъемами RJ45 категории 5e или 6. С тыльной стороны панели располагаются так называемые ***IDC-разъемы (англ. Insulator Displacement Connector, разъем со смещением изоляции).***

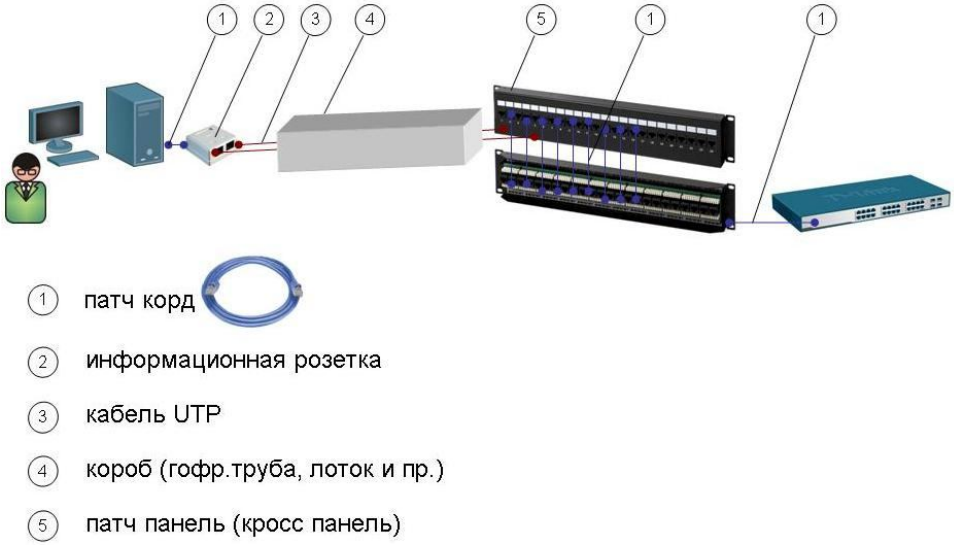


Рис. 78. Элементы СКС

Существует два типовых способа использования коммутационных панелей.

В первом случае, коммутационная панель используется как точка коммутации между портами активного сетевого оборудования (АСО) и портами рабочих мест, через кабель горизонтальной подсистемы СКС. Коммутация осуществляется коммутационными шнурами от панели до портов АСО.

Во втором случае, так называемое двойное представление порта, коммутационные панели используются попарно, одна из панелей представляет порты АСО, а вторая — порты рабочих мест. Коммутация осуществляется коммутационными шнурами между панелями.

Вместе с коммутационной панелью целесообразно использовать ***кабельные органайзеры***, для упорядочивания подходящих и отходящих к устройству кабелей.

Коммутационные панели могут отличаться:
а). По составу разъемов
б). По количеству портов
в). По экранированию
г). По способу крепления
д). По способу представления портов

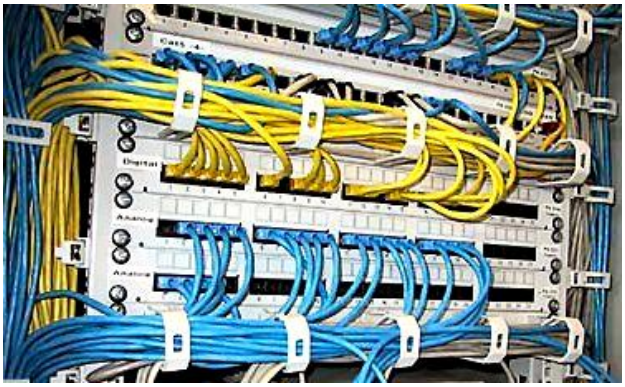


Рис. 79. Пример монтажа кросс-панели

Коммутационный шнур, коммутационный кабель или патч-корд (от англ. patching cord— соединительный шнур)— одна из составных частей структурированной кабельной системы. Представляет собой электрический кабель для подключения одного электрического устройства к другому. Может быть любых типов и размеров, на одном или обоих концах кабеля обязательно присутствуют соответствующие соединяемым устройствам коннекторы.

Главное отличие ***коммутационного шнура*** от ***кабеля внутренней прокладки***— использование многожильного провода, вместо цельного. Это снижает передаточные характеристики кабеля, но повышает гибкость и уменьшает минимальный радиус безопасного изгиба шнура.

Коммутационный шнур применяемый в ВОЛС носит название ***пигтейл,*** и представляет собой отрезок кабеля, оконеченный с одной стороны коннектором определенного типа. Соединение оптического пигтейла с волокном кабеля осуществляется с помощью сварки или механических неразъемных соединений.

Организация СКС

В общем виде всю конструкцию можно представить таким образом: на одном из этажей здания, содержащем рабочее место с офисной техникой, вдоль стены от подключенных устройств и от вспомогательных технических средств (датчиков пожарной сигнализации, систем видео наблюдения и др.) проводятся горизонтальные кабельные проводки. Они сходятся в единый коммутационный узел этажа (аналогичным образом проходят проводки и на остальных этажах, подключенных к СКС). От него идет вертикальная кабельная проводка, соединяющая последовательно все этажи. Затем вся система кабелей интегрируется в общий коммутационный центр, который может размещаться в специальном техническом помещении.

Все компоненты СКС логически связаны друг с другом и располагаются таким образом, что можно наращивать всю систему и расширять ее охват не

только внутри многоэтажных зданий, сооружений, но и между недвижимыми объектами на определенном расстоянии друг от друга.

Кабельная система предприятия может быть выполнена различными способами: по технологии скрытой проводки, в накладных каналах, в пространстве под фальшполом или над навесным потолком и т. п.

Часто в условиях предприятия экономят на кабелях, при помощи которых осуществляется подключение компьютера в розетку кабельной сети. Следует отметить, что эти патч-корды, часто являются причиной снижения скорости передачи данных. Они подвергаются наибольшему механическому воздействию, в то время как бывают изготовлены специалистом недостаточной квалификации. С течением времени их параметры ухудшаются, что приводит к ошибкам передачи данных, появление которых достаточно трудно заметить.

> Обратите внимание, что, по данным одного из производителей патч-кордов, две трети их не проходят тестирования. Трудно ожидать стабильности характеристик от изделий, изготовленных в кустарных условиях, поэтому стоит комплектовать рабочие места только профессионально выполненными патч-кордами.

Каждое рабочее место пользователя должно быть оборудовано розеткой электропитания с заземлением и информационными розетками. В небольших организациях обычно используют розетки существующей электропроводки. При этом следует учитывать, что расстояние между силовой и информационными розетками одного рабочего места по стандарту не должно превышать 1 м. Кроме того при необходимости пересечения кабеля электропитания, необходимо это выполнять под прямым углом. Часто чтобы минимизировать влияние силового кабеля, используют специальные кабели с экранированием.

Одним из мощных источников электро помех являются люминесцентные лампы. При прокладке информационных кабелей часто не обращают внимания на их близость к таким лампам, например, при монтаже новых трасс над фальш-потолком. Для снижения влияния данного источника помех не следует допускать прокладку информационного кабеля ближе 15 см от люминесцентной лампы.

При размещении большого числа пользователей в помещении, не оборудованном достаточным количеством силовых розеток, часто осуществляется проводка силовых и информационных кабелей до рабочего места в одном канале. Согласно стандарту, если оба кабеля прокладываются в общем канале, то должна быть предусмотрена сплошная перегородка между силовыми и информационным отсеками.

Современное оборудование, подключаемое к компьютерным сетям, часто потребляет совсем немного энергии. Учитывая, что в стандартах передачи дан-

ных 10/100 Мбит/сек используются только две пары проводников витой пары из четырех имеющихся, часто можно существенно сэкономить на прокладке кабелей, если применить технологию питания оборудования по кабелю Ethernet ***(Power over Ethernet, PoE).***

Существует несколько вариантов обеспечения PoE.

Первый состоит в использовании специальных коммутаторов либо уже имеющих функцию PoE, либо поддерживающих ее (коммутаторы допускают установку дополнительного блока питания, после чего обеспечивается предоставление услуги PoE). Данный способ применяется при наличии значительного числа портов с функцией PoE, например, при эксплуатации в организации IP-телефонов. В качестве примера - 8-портовый настольный коммутатор DES-1008P D-Link с 4 портами PoE.

Рис. 80. DES-1008P

Второй способ подачи питания через сеть Ethernet заключается в приобретении специальных блоков питания, включаемых в «разрыв» сетевого кабеля (для подачи напряжения 48 В используется коричневая пара проводников). Такое решение оправдано при подключении единичных устройств.

Рис. 81. DWL-P200

DWL-P200 передает данные, и электрические сигналы на устройства Ethernet по одному кабелю Ethernet.

В PoE-коммутаторах применяется специальная технология для проверки порта. Перед подачей питания на порт производится специальное тестирование, замеряются параметры подключенного оборудования и, если оно соответствует требованиям технологии PoE, коммутатор включает питание. Таким образом, в

порты PoE можно безопасно включать обычные устройства. При использовании же «врезных» блоков питания, особенно самых дешевых их вариантов, следует исключить возможность случайного подключения другого оборудования.

В соответствии со стандартом IEEE 802.3af максимальная мощность, которая может быть получена устройством с PoE-порта, составляет 12,95 Вт (при этом порт должен обеспечить мощность до 15,4 Вт). Подключаемые устройства часто потребляют меньшую мощность, например, типовая точка беспроводного доступа потребляет около 11 Вт, IP-телефоны — от 2 до 14 Вт в зависимости от модели. В целях экономии на некоторых моделях коммутаторов суммарно допустимая мощность питания по портам Ethernet меньше величины 15,4х<количество портов> Вт. В случае превышения допустимого значения потребляемой мощности коммутатор начинает отключать питание отдельных портов, учитывая приоритеты портов для PoE, которые администратору необходимо назначить вручную в соответствии с предназначением подключенного оборудования.

Требования пожарной безопасности

Основные требования пожарной безопасности при прокладке кабелей в офисе заключаются в следующем:

кабели, каналы, розетки и т. п. должны соответствовать определенной категории пожароустойчивости; обычно это выполняется при помощи современных элементов СКС;

силовые и информационные кабели при прокладке в одном канале должны быть разделены сплошной перегородкой. Минимальное расстояние от силовых кабелей до информационных определяется по специальным нормативам в зависимости от нагрузки, но обычно не должно быть менее 12—15 см;

отверстия, выполненные для прокладки кабелей между помещениями, должны быть закрыты легко удаляемым негорючим материалом, например, цементом или гипсом низкой прочности, минеральной ватой и т. п.;

при прокладке кабелей в пространстве над навесным потолком недопустимо использовать горючие материалы.

Достоинства СКС

Первое – это универсальность СКС, которая заключается в том, что данные системы с успехом могут применяться для построения компьютерных сетей, телефонных линий, охранной, пожарной систем, а также для видео наблюдения и "прослушки" ряда помещений.

Второе – как уже коснулись выше – способность легко расширяться, что имеет большое значение при стремительном научно-техническом прорыве вперед. Благодаря этой возможности отпадает проблема в глобальной перестройке установленных ранее СКС в течение 25 лет при подсоединении новых, более совершенных устройств.

Третье – надежность всей конструкции при условии, что все компоненты выполнены одним и тем же изготовителем, что в корне исключает возможные помехи, и сбои в отлаженной работе подсоединенного оборудования.

Данная технология постепенно вытесняет традиционную кабельную систему, и уже в недалеком будущем мы сможем наблюдать полный переход предприятий и организаций различного уровня на современную СКС.

Необходимость в диагностике СКС

Совершенно ясно, что любая организация заинтересована в бесперебойной работе своих сотрудников на предприятии. И понятно, что простой работы по вине некачественного монтажа, а также не проверенных на соответствие международным стандартам структурированных кабельных систем оборачивается гораздо большими потерями как временного, так и финансового характера, нежели затраты на их диагностику. Очень досадно бывает узнать, что невозможность работать с информацией в офисе связана всего лишь с мелким обрывом кабеля или с дефектом какого-то разъема.

И чтобы не оказаться в неприятной ситуации, нужно проводить диагностику СКС на физическом уровне. Другой причиной необходимости исследования физических параметров сети является влияние этих параметров на результаты тестирования более высоких уровней.

Сейчас на рынке предлагается достаточно моделей приборов для решения подобных задач. Мы рассмотрим два вида приборов: кабельные тестеры и анализаторы СКС.

Кабельные тестеры

Данные приборы являются самыми простейшими и сравнительно недорогими. Они часто используются для проведения монтажа кабелей и оценки качества построенных линий СКС. Внешне представляют собой небольшие коробочные устройства, с возможностями выявления обрывов, коротких замыканий жил в паре и между жилами разных пар, ошибочной полярности пары, когда случайно путают жилы между собой и с соседними участками.

В некоторых моделях тестеров есть возможность задания разводки, а также установления соответствия между розетками коммутационной панели и рабочих мест, в последнем случае проверяются все розетки, подключенные на горизонтальной линии проводки при помощи пронумерованных заглушек. При под-

ключении тестера к одной стороне кабеля его индикатор высвечивает номер заглушки. Другие тестеры могут посылать тональный сигнал на жилу кабеля для его идентификации и трассировки.

Анализаторы СКС

В отличие от вышеупомянутых кабельных тестеров, данные приборы имеют более широкий набор функций и призваны определять не только простейшие дефекты, вызванные отсутствием контакта в кабеле.

Анализаторы СКС способны выявить более сложные неисправности, возникшие вследствие неправильного монтажа, когда не соблюдены правила соединений кабелей в линию (чрезмерное растяжение кабеля, малый радиус изгиба и др.). От некачественного монтажа страдает производительность СКС и ухудшаются их электрические характеристики.

Применяя в диагностике эти приборы, можно определить целостность цепи, характеристический импеданс, погонное и переходное затухание, задержку распространения сигнала, длину линии, сопротивление линии по постоянному току, емкость линии, а также электрическую симметричность и наличие шумов. Столь широкие возможности диагностики обуславливают дороговизну этих приборов, поэтому их может приобрести далеко не каждый, кто имеет дело с монтажом и диагностикой СКС.

Физическая структура ЛВС

Типовая структура сети предприятия

Длина кабеля от одного элемента активного оборудования до другого, например от компьютера до коммутатора, в сети Ethernet согласно стандарта IEEE 802.3 не должна превышать 100 м. На практике максимальную длину самого кабеля определяют 90 м, а 10 м отводится на соединительные кабели.

На практике существует два подхода к построению линий передачи данных. В первом случае развитие начинается от комнаты системного администратора, в которой устанавливается коммутирующее оборудование, становящееся центром сети. В дальнейшем, по мере увеличения числа рабочих мест, к сети подключаются новые коммутаторы, и структура сети принимает достаточно хаотичный вид. Подобная сеть, хотя и обеспечивает текущее функционирование сетевых приложений, не является отказоустойчивой и часто не позволяет внедрить современные решения, критичные к параметрам инфраструктуры.

Если предприятие въезжает в новый офис, то, как правило, структура сети проектируется «с нуля». Принято выделять несколько уровней структуры.

Современная сеть создается на основе трех уровней:

- ядра (Core),
- распределения (Distribution)
- доступа (Access),

На ***уровне доступа*** обеспечивается подключение конечных рабочих станций. На ***уровне распределения*** реализуется маршрутизация пакетов и их фильтрация (на основе списков доступа и т. п.). Задача оборудования ***уровня ядра*** — максимально быстро передать трафик между оборудованием уровня распределения.

Если рассматривать типовую сеть небольшой организации, занимающей несколько этажей одного здания, то уровень распределения будет соответствовать оборудованию, объединяющим коммутаторы каждого этажа, а уровень ядра — активному оборудованию, размещаемому обычно в главной серверной.

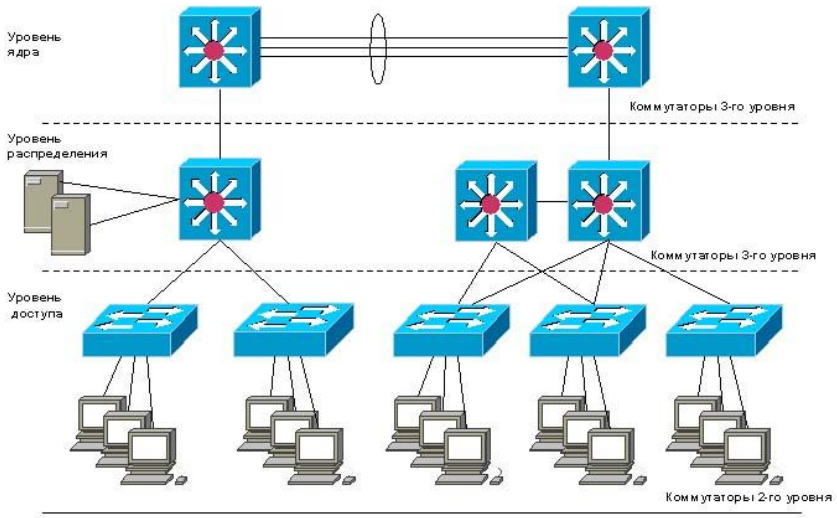


Рис. 82. Трёхуровневая сеть предприятия

Это классическая схема иерархической структуры, которая на практике часто модифицируется с учетом специфики организации, оборудования и т. д. Так, в зависимости от размеров предприятия, может отсутствовать какой-либо уровень, и структура сети станет двухуровневой. Маршрутизацию данных

можно реализовать на уровне ядра, а оборудование уровня распределения будет только пересылать данные внутри сегмента сети. Все зависит от решаемых задач, распределения потоков информации и предъявляемых к информационной системе требований.

Часто в схеме сети выделяют ***серверную ферму***. Принципиально серверная ферма представляет собой обычный узел распределения, но реализованный на быстродействующем оборудовании и, как правило, со 100%-ным резервированным решением.

В малых организациях часто практикуется подключение серверов непосредственно к ядру сети передачи данных., так как трехуровневая схема больше свойственна крупным сетям. Для средних и небольших предприятий чаще всего создается двухуровневая схема: существует один, обычно самый мощный коммутатор, к которому подключаются как серверы, так и рабочие станции. К этому коммутатору подключены коммутаторы второго уровня, распределяющие данные на остальные рабочие станции.

На практике структуру сети администраторам обычно приходится «примерять» на уже существующие линии связи, ограничиваться возможностями по созданию новых соединений (учитывая, по какой трассе можно проложить линию связи собственными силами) и т. д. Поэтому одной из основных рекомендаций при изменении топологии сети должна быть минимизация количества коммутаторов между любыми двумя точками подключения компьютеров.

Топология каналов сети распределенного предприятия

Если при построении сети внутри здания обычно удается придерживаться иерархии связей «здание — этаж — рабочее место», то в случае размещения предприятия в нескольких зданиях структура сети в значительной степени определяется возможностями прокладки внешних кабелей. Наличие кабельной канализации, воздушных линий связи, кабельных эстакад и т. п. достаточно жестко определяют возможные направления каналов передачи данных. Поскольку стоимость прокладки кабелей между зданиями достаточно высока, обычно прокладывается лишь минимум связей, которые обеспечат отказоустойчивость сетевой структуры. При этом весьма часто используется кольцевая структура, иногда снабжаемая «перемычкой» для снижения числа промежуточных узлов между двумя узлами распределения.

Документирование структуры линий и каналов связи

Традиционной проблемой большинства организаций является документирование своей кабельной подсистемы. Специализированные программные продукты, позволяющие поддерживать схемы сети с учетом вносимых в нее изме-

нений в актуальном состоянии, стоят весьма дорого, а исходная документация быстро становится неактуальной после нескольких перемещений сотрудников и прокладки дополнительных каналов связи. Существует много программ, которые позволяют контролировать трафик и автоматически воспроизвести структуру сети.

Задачу контроля и анализа сетевого трафика успешно решают так называемые программы ***«снифферы».***

> ***Анализатор трафика, или сниффер (от англ. to sniff, нюхать)*** - сетевой анализатор трафика, программа или программно-аппаратное устройство, предназначенное для перехвата и последующего анализа, либо только анализа сетевого трафика, предназначенного для других узлов.

Одна из таких программ - ***Wireshark (ранее Ethereal)*** - программа для анализа пакетов Ethernet и некоторых других сетей ***(сниффер).*** Имеет графический пользовательский интерфейс. Программа позволяет использовать сетевую карту в ***«режим прослушивания» (Promiscuous mode***) и даёт возможность пользователю просматривать весь проходящий по сети трафик в режиме реального времени.

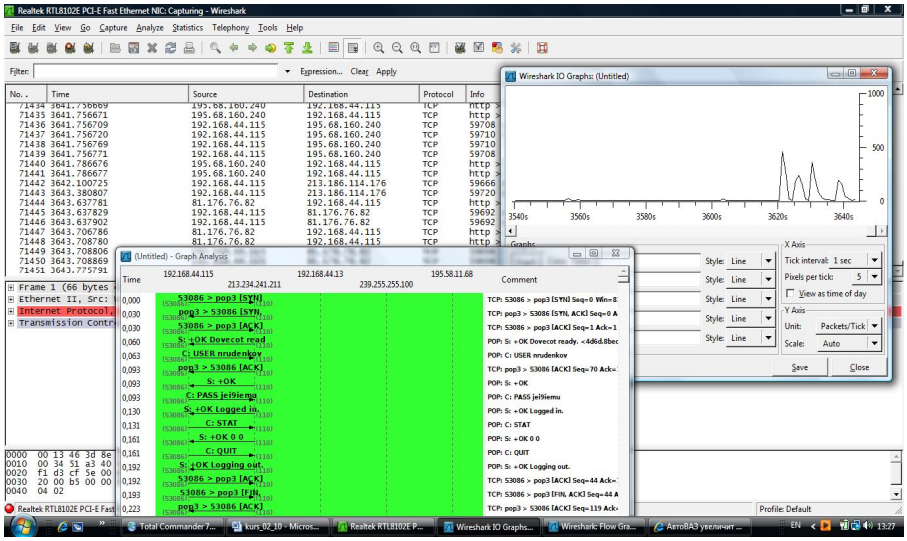


Рис. 83. Скриншот программы Wireshark

Более полную картину о состоянии сети в целом, и отдельных её узлов, предоставляют программные (аппаратно-программные) комплексы SNMP-управления.

D-View 6.0 –современная многофункциональная платформа для SNMP-управления. D-View 6.0 поставляется в двух версиях: стандартная (DV-600S) и профессиональная (DV-600P). Стандартная версия поддерживает управление до 1000 IP-узлами и предназначена для использования на предприятиях сектора SMB. Профессиональная версия поддерживает управление более 1000 IP-узлами и рекомендована для использования на крупных предприятиях.

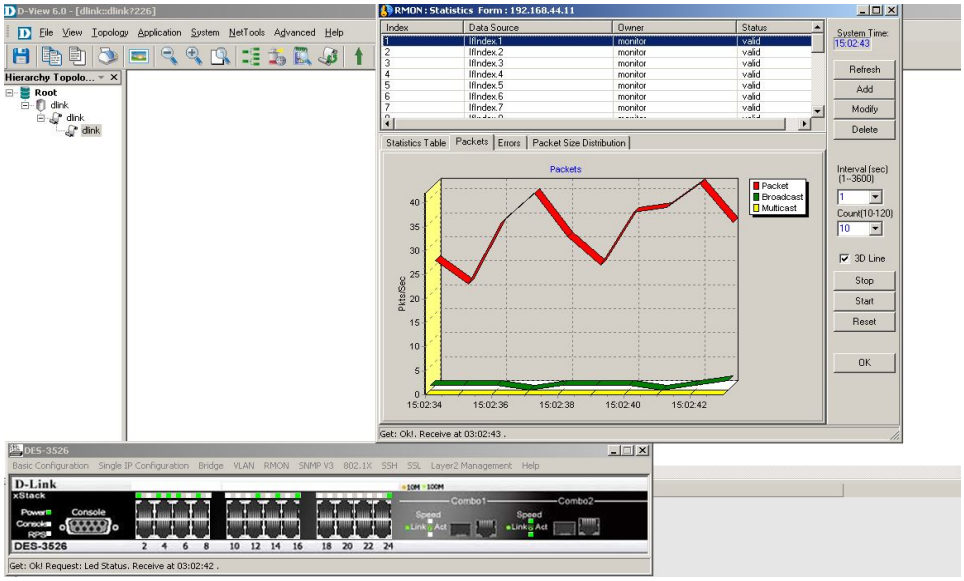


Рис. 84. Скриншот программы D-View 6.0

D-View 6.0 позволяет визуально отобразить схему подключения и поддерживает групповую конфигурацию устройств, что дает возможность выполнить резервную копию конфигурации, обновление программного обеспечения и другие аналогичные действия сразу для всех устройств в группе. Также в D-View 6.0 реализованы другие важные функции системы сетевого управления, включая MIB-браузер и MIB-компилятор, мониторинг производительности и рассылку уведомляющих сообщений.

Надежность сетевой инфраструктуры

Необходимым условием надежной работы информационной системы является безотказное функционирование каналов связи. Данная задача решается путем дублирования как собственно каналов связи, так и активного оборудования

(коммутаторов). Понятно, что на практике отказоустойчивая конфигурация сети создается только в тех случаях, когда простои в работе информационной системы недопустимы и могут привести к существенным экономическим потерям.

Дублирование каналов связи и оборудования производят как в ядре сети (обязательно), так и на уровне распределения (рекомендуется). Подключение оконечных устройств (рабочих станций пользователей) не дублируется.

Отказоустойчивая топология сети передачи данных

На предыдущих рисунках показаны варианты отказоустойчивой схемы сети передачи данных. Связи между коммутаторами уровня распределения и ядра дублированы, коммутаторы также дублированы. Серверы предприятия отказоустойчивым образом подключены к коммутаторам ядра (один сетевой интерфейс сервера подключен к одному коммутатору, второй — к другому).

Отказоустойчивые схемы, несмотря на кажущуюся простоту, требуют тщательной настройки коммутаторов. При этом в зависимости от выбранного варианта конфигурации может потребоваться использование протоколов, которые не поддерживаются относительно дешевыми моделями оборудования.

Простое соединение двух коммутаторов двумя кабелями создаст кольцо, которое недопустимо в сети Ethernet. Результатом станет широковещательный шторм и практическая не работоспособность сегмента сети. Поэтому создание отказоустойчивых решений требует первоначальной настройки активного оборудования.

Отказоустойчивая конфигурация, построенная с использованием протоколов второго уровня, обеспечивает самое быстрое восстановление в случае аварии. Сеть может восстановиться за считанные секунды или даже еще быстрее, в случае использования ***проприетарных*** протоколов.

> ***Проприетарным*** называют протокол, не описываемый открытым стандартом, а являющийся уникальной технологией определенного вендора. Хотя использование проприетарных решений позволяет получить лучшие показатели по сравнению с открытыми стандартами, но такой выбор связан с ориентацией на использование оборудования только одного вендора и с вытекающими из этого рисками.

1.18. Базовые технологии канального уровня вычислительных систем

Структура стандартов Ethernet. Понятие MAC адреса

В 80-е годы, как уже отмечалось ранее, произошёл бурный рост компьютерных технологий, связанный с появлением новой элементной базы, и новым витком развития сетевых решений.

Были приняты основные стандарты на коммуникационные технологии для локальных сетей: в 1980 году — Ethernet, в 1985 — Token Ring, в конце 80-х — FDDI. Это позволило обеспечить совместимость сетевых операционных систем на нижних уровнях, а также стандартизировать интерфейс ОС с драйверами сетевых адаптеров.

В 1980 году в результате работы **«комитета 802»**, организации ***Institute of Electrical and Electronics Engineers, IEEE,*** было принято семейство стандартов **IEEE 802-x**, которые содержат рекомендации по проектированию нижних уровней локальных сетей. Позже результаты работы этого комитета легли в основу комплекса международных стандартов ***ISO 8802-1...5.***

Стандарты семейства **IEEE 802.x** охватывают два нижних уровня модели ISO/OSI - физический и канальный, потому что именно эти уровни в наибольшей степени отражают специфику локальных сетей

Функции канального уровня подразделяются на два подуровня:

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

Подуровень MAC определяет такие элементы канального уровня, как логическая топология сети, метод доступа к среде передачи информации и правила физической адресации между сетевыми объектами. Аббревиатура ***MAC*** используется также при определении физического адреса сетевого устройства: физический адрес устройства (который определяется внутри сетевого устройства или сетевой карты на этапе производства) часто ***называют MAC-адресом этого устройства.*** Существует возможность программно изменить MAC-адрес большого количества сетевых устройств, особенно сетевых карт. При этом необходимо помнить, что канальный уровень модели ISO/OSI накладывает ограничения на использование MAC-адресов: в одной физической сети не может быть двух или более устройств, использующих одинаковый MAC-адрес.

Для определения физического адреса сетевого объекта может быть использовано понятие ***«адрес узла».*** Адрес узла чаще всего совпадает с MAC-адресом или определяется логически при программном переназначении адреса.

Подуровень LLC определяет правила синхронизации передачи и сервиса соединений. Этот подуровень канального уровня тесно взаимодействует с сетевым уровнем модели ISO/OSI и отвечает за надежность физических (с использованием MAC-адресов) соединений.

Канальный уровень обеспечивает сервис соединений.

Существует три типа сервиса соединений:

- ***сервис без подтверждения и без установления соединений (unacknowledged connectionless)*** - посылает и получает фреймы без управления потоком и без контроля ошибок или последовательности пакетов;
- ***сервис, ориентированный на соединение (connection-oriented),*** - обеспечивает управление потоком, контроль ошибок и последовательности пакетов посредством выдачи квитанций (подтверждений);
- ***сервис с подтверждением без установления соединения (acknowledged connectionless)*** - использует квитанции для управления потоком и контроля ошибок при передачах между двумя узлами сети.

Сервис соединений использует ***подтверждения, или квитанции***, представляющие собой специальные сообщения, которые подтверждают факт приема фрейма или пакета данных. Подтверждения используются для управления потоком данных LLC-уровня и для контроля ошибок.

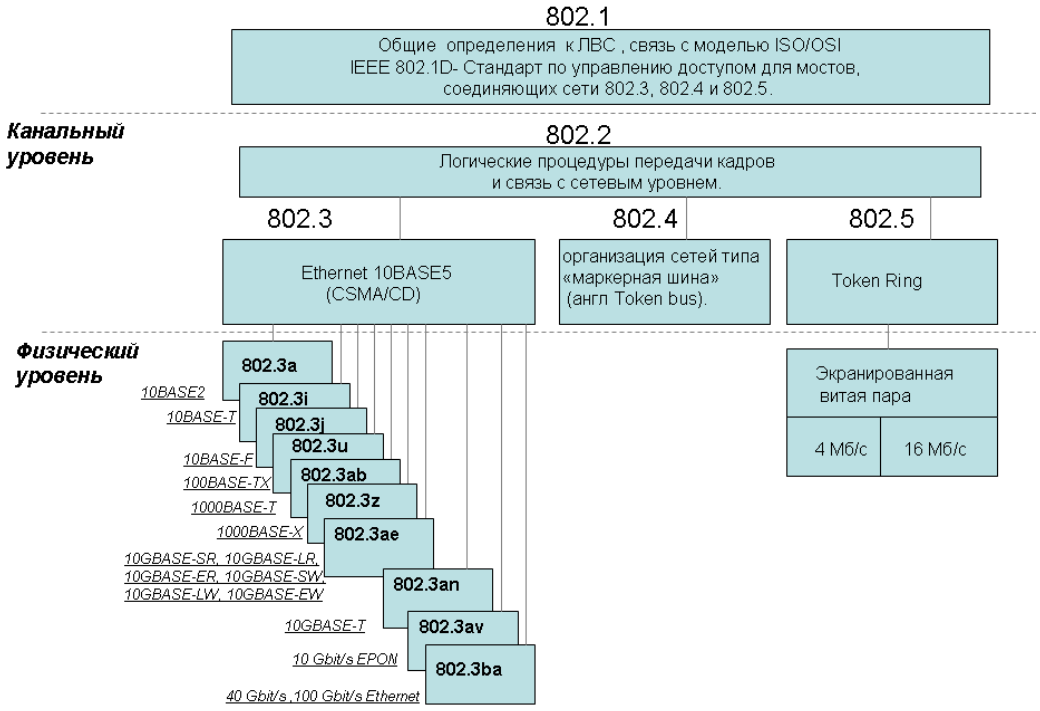


Рис. 85. Структура стандартов IEEE802.x

. Помимо IEEE в работе по стандартизации протоколов локальных сетей принимали участие и другие организации. Так, для сетей, работающих на оптоволокне, американским институтом по стандартизации ***ANSI*** был разработан стандарт ***FDDI***, обеспечивающий скорость передачи данных 100 Мб/с. Работы по стандартизации протоколов ведутся также ассоциацией ***ECMA***, которой приняты стандарты ***ECMA-80, 81, 82*** для локальной сети типа ***Ethernet*** и впоследствии стандарты ***ECMA-89,90*** по методу передачи маркера.

Технология Ethernet была разработана вместе со многими первыми проектами корпорации Xerox PARC. Общепринято считать, что Ethernet был изобретён 22 мая 1973 года, когда Роберт Меткалф составил докладную записку для главы PARC о потенциале ***технологии Ethernet***. Но законное право на технологию Меткалф получил через несколько лет. В 1976 году он и его ассистент Дэвид Боггс издали брошюру под названием ***«Ethernet: Distributed Packet-Switching For Local Computer Networks».*** Меткалф ушёл из Xerox в 1979 году и основал компанию 3Com для продвижения компьютеров и локальных вычислительных сетей. Ему удалось убедить DEC, Intel и Xerox работать совместно и разработать стандарт ***Ethernet (DIX).*** Впервые этот стандарт был опубликован 30 сентября 1980 года. Он начал соперничество с двумя крупными запатенто-

ванными технологиями: ***Token Ring и ARCNET***,— которые вскоре уступили свои места под накатывающимися волнами продукции ***Ethernet.***

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

Причинами перехода на витую пару были:

- возможность работы в дуплексном режиме;
- низкая стоимость кабеля «витой пары»;
- более высокая надёжность сетей при неисправности в кабеле;
- большая помехозащищенность при использовании дифференциального сигнала;
- возможность питания по кабелю маломощных узлов, например IP-телефонов (стандарт Power over Ethernet, POE);
- отсутствие гальванической связи (прохождения тока) между узлами сети.

При использовании коаксиального кабеля в российских условиях, где, как правило, отсутствует заземление компьютеров, применение коаксиального кабеля часто сопровождалось пробоем сетевых карт, и иногда даже полным «выгоранием» системного блока.

Причиной перехода на оптический кабель была необходимость увеличить длину сегмента без повторителей, и возможность увеличения скорости передачи данных.

Форматы кадров технологии Ethernet

В сетях Ethernet существует 4 типа фреймов: кадр 802.3/LLC (или кадр Novell 802.2), кадр Raw 802.3 (или кадр Novell 802.3), кадр Ethernet DIX (или кадр Ethernet II), кадр Ethernet SNAP.

Большинство устройств Ethernet умеет работать со всеми вышеупомянутыми форматами фреймов. Чаще всего используется фрейм Ethernet II. Стандарт технологии Ethernet, описанный в документе IEEE 802.3, дает описание единственного формата кадра уровня MAC. Так как в кадр уровня MAC должен вкладываться кадр уровня LLC, описанный в документе IEEE 802.2, то по стандартам IEEE в сети Ethernet может использоваться только единственный вариант кадра канального уровня, заголовок которого является комбинацией заголовков MAC и LLC подуровней.

Ethernet Version 2 или Ethernet-кадр II, ещё называемый ***DIX*** — наиболее распространена и используется по сей день.

Часто используется непосредственно протоколом интернет.

Рис. 86. Кадр Ethernet II (64-1518 byte)

Logical Link Control (общепринятое сокращение — LLC) — подуровень управления логической связью. По стандарту IEEE 802 — верхний подуровень канального уровня модели ISO/OSI, осуществляет:

- управление передачей данных;
- обеспечивает проверку и правильность передачи информации по соединению.

По своему назначению все кадры уровня LLC (называемые в стандарте IEEE 802.2 блоками данных — Protocol Data Unit, PDU) подразделяются на три типа — **информационные, управляющие и ненумерованные:**

Информационные кадры предназначены для передачи информации в процедурах с установлением логического соединения и должны обязательно содержать поле информации. В процессе передачи информационных блоков осуществляется их нумерация в режиме скользящего окна.

Тег (иногда тэг, англ. tag— «ярлык, этикетка, бирка; метить»)— метка как ключевое слово, в более узком применении идентификатор для категоризации, описания, поиска данных и задания внутренней структуры. Метка-идентификатор, добавляемая к Ethernet-пакетам, используемая при выделении разных виртуальных каналов данных в одном физическом канале. Определяется в стандарте IEEE 802.1Q.;

Управляющие кадры предназначены для передачи команд и ответов в процедурах с установлением логического соединения, в том числе запросов на повторную передачу искаженных информационных блоков.

Ненумерованные кадры предназначены для передачи ненумерованных команд и ответов, выполняющих в процедурах без установления логического соединения передачу информации, идентификацию и тестирование LLC-

уровня, а в процедурах с установлением логического соединения — установление и разъединение логического соединения, а также информирование об ошибках.

Все типы кадров уровня LLC имеют единый формат. Они содержат четыре поля:

- адрес точки входа сервиса назначения (Destination Service Access Point, DSAP),
- адрес точки входа сервиса источника (Source Service Access Point, SSAP),
- управляющее поле (Control)
- поле данных (Data)

Флаг	DSAP	SSAP	Control	Data	Флаг
01111110	Адрес точки входа сервиса назначения	Адрес точки входа сервиса источника	Управляющее поле	Данные	01111110

Рис. 87. Формат кадра LLC.

Кадр LLC обрамляется двумя однобайтовыми полями «Флаг», имеющими значение 01111110. Флаги используются на MAC-уровне для определения границ блока. Заголовок кадра 802.3/LLC является результатом объединения полей заголовков кадров, определенных в стандартах IEEE 802.3 и 802.2.

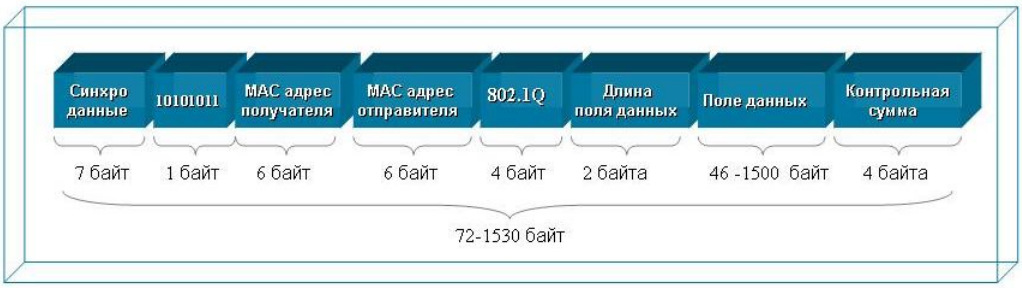


Рис. 88. формат кадра Ethernet IEEE 802.3

Стандарт IEEE 802.3 определяет восемь полей заголовка:

Поле преамбулы состоит из семи байтов синхронизирующих данных. Каждый байт содержит одну и ту же последовательность битов - 10101010. При манчестерском кодировании эта комбинация представляется в физической среде периодическим волновым сигналом. Преамбула используется для того, чтобы дать время и возможность схемам приемопередатчиков прийти в устойчивый синхронизм с принимаемыми тактовыми сигналами.

Начальный ограничитель кадра состоит из одного байта с набором битов 10101011. Появление этой комбинации является указанием на предстоящий прием кадра.

Адрес получателя - может быть длиной 2 или 6 байтов (MAC-адрес получателя). Первый бит адреса получателя - это признак того, является адрес индивидуальным или групповым: если 0, то адрес указывает на определенную станцию, если 1, то это групповой адрес нескольких (возможно всех) станций сети. При широковещательной адресации все биты поля адреса устанавливаются в 1. Общепринятым является использование 6-байтовых адресов.

Адрес отправителя - 2-х или 6-ти байтовое поле, содержащее адрес станции отправителя. Первый бит - всегда имеет значение 0.

Поле TAG включает в себя данные QoS и номер VLAN , все пакеты, содержащие информацию о качестве обслуживания, являются тегированными.

Поле данных может содержать от 0 до 1500 байт. Но если длина поля меньше 46 байт, то используется следующее поле - поле заполнения, чтобы дополнить кадр до минимально допустимой длины.

Поле заполнения состоит из такого количества байтов заполнителей, которое обеспечивает определенную минимальную длину поля данных (46 байт). Это обеспечивает корректную работу механизма обнаружения коллизий. Если длина поля данных достаточна, то поле заполнения в кадре не появляется.

Поле контрольной суммы - 4 байта, содержащие значение, которое вычисляется по определенному алгоритму (CRC-32). После получения кадра рабочая станция выполняет собственное вычисление контрольной суммы для этого кадра, сравнивает полученное значение со значением поля контрольной суммы и, таким образом, определяет, не искажен ли полученный кадр.

Методы доступа к среде передачи данных

Представим себе сеть, в которой всем устройствам позволено функционировать безо всяких правил получения доступа к среде передачи. Если бы все устройства передавали сигналы по мере готовности данных, эти передачи иногда совпадали бы во времени. В результате наложения сигналы исказились бы и произошла бы потеря передаваемых данных (рис.90). Такая ситуация называет-

ся ***коллизией (collision***). Коллизии не позволяют организовать надежную и эффективную передачу информации между сетевыми объектами

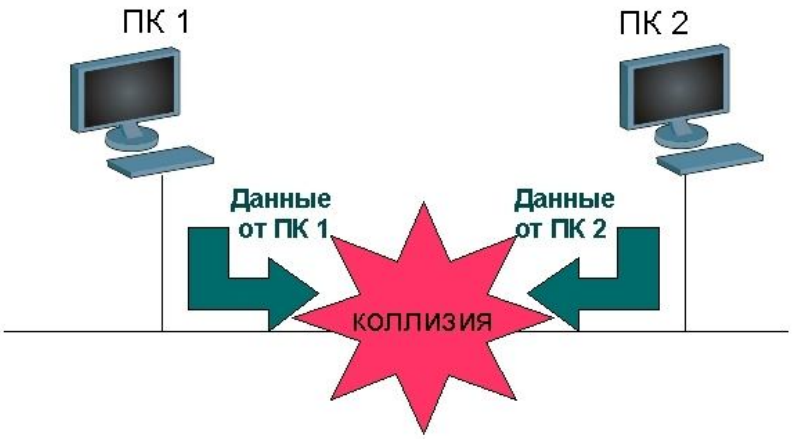


Рис. 89. Возникновение коллизии.

Коллизии распространяются на физические сегменты сети, к которым подключаются сетевые устройства. Такие соединения образуют единое пространство(домен) коллизий (collision domain), в котором влияние коллизий распространяется на всех ее участников. Для уменьшения размеров пространств коллизий путем ***сегментации*** физической сети можно использовать мосты и другие сетевые устройства, обладающие функциями фильтрации трафика на канальном уровне. Сеть не может нормально работать до тех пор, пока все ее объекты не смогут контролировать коллизии, управлять ими, устранять или хотя бы ослаблять их влияние. Логические топологии используют специальные правила, управляющие разрешением на передачу сигналов данных другим сетевым объектам. Процесс управления называется ***доступом к среде передачи данных.***

Снижать число коллизий или интерференции (наложения) одновременных сигналов можно различными методами. Существуют стандартные методы доступа к среде передачи, описывающие правила, в соответствии с которыми осуществляется управление разрешением на передачу информации для сетевых устройств: ***состязание, передача маркера и опрос.***

Состязание. Системы на основе состязания (конкуренции) предполагают, что доступ к среде передачи реализуется на основе принципа «первым пришел – первым обслужен». Другими словами, каждое сетевое устройство борется за контроль над средой передачи. Системы, использующие метод состязания, разработаны таким образом, чтобы все устройства в сети могли передавать данные только по мере надобности. Эта практика, в конечном счете, приводит к час-

тичной или полной потере данных, потому что в действительности коллизии все же происходят.

Системы с передачей маркера. В таких системах (token passing) небольшой фрейм (маркер) передается в определенном порядке от одного устройства к другому. Маркер - это специальное сообщение, которое передает временное управление средой передачи устройству, владеющему маркером. Передача маркера распределяет управление доступом между устройствами сети. В основном этот метод получил развитие в сетях Token Ring, и FDDI.

Опрос (polling) - это метод доступа, при котором специально выделенное устройство (называемое контроллером, первичным или мастер устройством) служит арбитром доступа к среде. Это устройство опрашивает остальные устройства (вторичные) в некотором предопределенном порядке, чтобы узнать, есть ли у них информация для передачи. Чтобы получить данные, первичное устройство направляет вторичному соответствующий запрос, а полученные данные направляет устройству-получателю. Затем первичное устройство запрашивает другое вторичное устройство и принимает данные от него и т. д. Протокол ограничивает количество данных, которое может передать после запроса каждое вторичное устройство.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD). Принято говорить, что кабель, к которому подключены все узлы, работает в режиме коллективного доступа (multiply-access, MA). Все данные, передаваемые по сети, помещаются в кадры определенной структуры и снабжаются уникальным адресом узла назначения. Затем кадр передается по кабелю. Все узлы, подключенные к кабелю, могут распознать факт передачи кадра, и тот узел, который узнает собственный адрес в заголовках кадра, записывает его содержимое в свой внутренний буфер, обрабатывает полученные данные и посылает по кабелю кадр-ответ. Адрес узла-источника также включен в исходный кадр, поэтому получатель знает, кому нужно послать ответ.

При описанном подходе возможна ситуация, когда два узла одновременно пытаются передать кадр данных по общему кабелю. Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающий узел слушает кабель (то есть принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции. Если опознается несущая (carrier-sense, CS), то узел откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать. Но даже при таком алгоритме два узла одновременно могут решить, что по шине в данный момент времени нет передачи, и начать одновременно передавать свои кадры. Говорят, что при этом происходит коллизия, так как содержимое обоих кадров сталкивается на общем кабеле, что приводит к искажению информации.

Чтобы корректно обработать коллизию, все узлы одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется обнаружение коллизии (collision detection, CD). Для увеличения вероятности немедленного обнаружения коллизии всеми узлами сети, ситуация коллизии усиливается посылкой в сеть узлами, начавшими передачу своих кадров, специальной последовательности битов, называемой ***jam-последовательностью***.

После обнаружения коллизии передающий узел обязан прекратить передачу и ожидать в течение короткого случайного интервала времени, а затем может снова сделать попытку передачи кадра. Каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности передачи кадров. При разработке этого метода предполагалось, что скорость передачи данных в 10 Мб/с очень высока по сравнению с потребностями компьютеров во взаимном обмене данными, поэтому загрузка сети будет всегда небольшой. Это предположение остается часто справедливым и по сей день, однако уже появились приложения, работающие в реальном масштабе времени с мультимедийной информацией, для которых требуются гораздо более высокие скорости передачи данных. Поэтому наряду с классическим Ethernet растет потребность и в новых высокоскоростных технологиях.

Кроме метода доступа к среде передачи данных, называемым методом множественного доступа с опознаванием несущей и обнаружением коллизий (CSMA/CD, Carrier Sense Multiple Access With Collision Detection), существует метод множественного доступа с прослушиванием несущей и избеганием коллизий (CSMA/CA, Carrier Sense Multiple Access With Collision Avoidance).

Протоколы CSMA/CA используют такие схемы, как доступ с квантованием времени (time slicing) или посылка запроса на получение доступа к среде.

При использовании квантования времени каждая станция может передавать информацию только в строго определенные для этой станции моменты времени. При этом в сети должен реализовываться механизм управления квантами времени. Каждая новая станция, подключаемая к сети, оповещает о своем появлении, тем самым, инициируя процесс перераспределения квантов времени для передачи информации.

В случае использования централизованного управления доступом к среде передачи каждая станция формирует специальный запрос на передачу, который

адресуется управляющей станции. Центральная станция регулирует доступ к среде передачи для всех сетевых объектов. Примером CSMA/CA является протокол LocalTalk фирмы Apple Computer.

Четкое распознавание коллизий всеми станциями сети является необходимым условием корректной работы сети Ethernet. Если какая-либо передающая станция не распознает коллизию и решит, что кадр данных ею передан верно, то этот кадр данных будет утерян, так как информация кадра исказится из-за наложения сигналов при коллизии, он будет отбракован принимающей станцией (скорее всего из-за несовпадения контрольной суммы). Скорее всего, искаженная информация будет повторно передана каким-либо протоколом верхнего уровня, например, транспортным или прикладным, работающим с установлением соединения и нумерацией своих сообщений. Но повторная передача сообщения протоколами верхних уровней произойдет через гораздо более длительный интервал времени (десятки секунд) по сравнению с микросекундными интервалами, которыми оперирует протокол Ethernet. Поэтому, если коллизии не будут надежно распознаваться узлами сети Ethernet, то это приведет к заметному снижению полезной пропускной способности данной сети.

Передача кадра Ethernet

Уточним основные параметры операций передачи и приема кадров Ethernet. Станция, которая хочет передать кадр, должна сначала с помощью MAC-узла упаковать данные в кадр соответствующего формата. Затем для предотвращения смешения сигналов с сигналами другой передающей станции, MAC-узел должен прослушивать электрические сигналы на кабеле и в случае обнаружения несущей частоты 10 МГц отложить передачу своего кадра. После окончания передачи по кабелю станция должна выждать небольшую дополнительную паузу, называемую межкадровым интервалом (interframe gap), что позволяет узлу назначения принять и обработать передаваемый кадр, и после этого начать передачу своего кадра. Одновременно с передачей битов кадра приемно-передающее устройство узла следит за принимаемыми по общему кабелю битами, чтобы вовремя обнаружить коллизию. Если коллизия не обнаружена, то передается весь кадр, поле чего MAC-уровень узла готов принять кадр из сети либо от LLC-уровня.

Если же фиксируется коллизия, то MAC-узел прекращает передачу кадра и посылает jam-последовательность, усиливающую состояние коллизии. После посылки в сеть ***jam-последовательности*** MAC-узел делает случайную паузу и повторно пытается передать свой кадр.

В случае повторных коллизий существует максимально возможное число попыток повторной передачи кадра, которое равно 16. При достижении этого предела фиксируется ошибка передачи кадра, сообщение о которой передается протоколу верхнего уровня.

Для того чтобы уменьшить интенсивность коллизий, каждый MAC-узел с каждой новой попыткой случайным образом увеличивает длительность паузы между попытками. Временное расписание длительности паузы определяется на основе усеченного двоичного экспоненциального алгоритма отсрочки. Пауза всегда составляет целое число так называемых интервалов отсрочки. Это время тесно связано с другим важным временным параметром сети - ***окном коллизий.*** Интервал отсрочки выбирается равным величине окна коллизий плюс некоторая дополнительная величина задержки для гарантии:

интервал отсрочки = окно коллизий + дополнительная задержка

В стандартах IEEE 802.3 большинство временных интервалов измеряется в количестве межбитовых интервалов, величина которых для битовой скорости 10 Мб/с составляет 0.1 мкс и равна времени передачи одного бита.

Величина интервала отсрочки в стандарте IEEE 802.3 определена равной 512 битовым интервалам, и эта величина рассчитана для максимальной длины коаксиального кабеля в 2.5 км. Величина 512 определяет и минимальную длину кадра в 64 байта, так как при кадрах меньшей длины станция может передать кадр и не успеть заметить факт возникновения коллизии из-за того, что искаженные коллизией сигналы дойдут до станции в наихудшем случае после завершения передачи. Такой кадр будет просто потерян. Время паузы после N-ой коллизии полагается равным L интервалам отсрочки, где L - случайное целое число, равномерно распределенное в диапазоне [0, 2N]. Величина диапазона растет только до 10 попытки (напомним, что их не может быть больше 16), а далее диапазон остается равным [0, 210], то есть [0, 1024].

Интервал отсрочки (slot time) - это время, в течение которого станция гарантированно может узнать, что в сети нет коллизии.
Окно коллизий (collision window) -равно времени двукратного прохождения сигнала между самыми удаленными узлами сети - наихудшему случаю задержки, при которой станция еще может обнаружить, что произошла коллизия.

Значения основных параметров процедуры передачи кадра стандарта IEEE 802.3 приведено в таблице.

Таблица 6. основные параметры кадра 802.3

Битовая скорость	10 Мб/с

Интервал отсрочки	512 битовых интервалов
Межкадровый интервал	9.6 мкс
Максимальное число попыток передачи	16
Максимальное число возрастания диапазона паузы	10
Длина jam-последовательности	32 бита
Максимальная длина кадра (без преамбулы)	1518 байтов
Минимальная длина кадра (без преамбулы)	64 байта (512 бит)
Длина преамбулы	64 бита

Учитывая приведенные параметры, нетрудно рассчитать максимальную производительность сегмента Ethernet в таких единицах, как число переданных пакетов минимальной длины в секунду (packets-per-second, pps). Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мостов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому интересно знать чистую максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

Так как размер пакета минимальной длины вместе с преамбулой составляет 64+8 = 72 байта или 576 битов, то на его передачу затрачивается 57.6 мкс. Прибавив межкадровый интервал в 9.6 мкс, получаем, что период следования минимальных пакетов равен 67.2 мкс. Это соответствует максимально возможной пропускной способности сегмента Ethernet в 14880 пакет(кадр)/с.

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

В зависимости от скорости передачи данных и передающей среды были разработаны несколько вариантов технологии.

10BASE5, IEEE 802.3— первоначальная разработка технологии со скоростью передачи данных 10 Мбит/с. Следуя раннему стандарту IEEE использует коаксиальный кабель с волновым сопротивлением 50 Ом (RG-8), с максимальной длиной сегмента 500 метров.

10BASE2, IEEE 802.3a используется кабель RG-58, с максимальной длиной сегмента 200 метров, компьютеры присоединялись один к другому, для подключения кабеля к сетевой карте нужен Т-коннектор, а на кабеле должен

быть BNC-коннектор. Требуется наличие терминаторов на каждом конце. Многие годы этот стандарт был основным для технологии Ethernet.

StarLAN 10— Первая разработка, использующая витую пару для передачи данных на скорости 10 Мбит/с. В дальнейшем эволюционировал в стандарт 10BASE-T.

Несмотря на то, что теоретически возможно подключение к одному кабелю (сегменту) витой пары более чем двух устройств, работающих в симплексном режиме, такая схема никогда не применяется для Ethernet, в отличие от работы с коаксиальным кабелем. Поэтому, все сети на витой паре используют топологию «звезда», в то время как, сети на коаксиальном кабеле построены на топологии «шина».

10BASE-T, IEEE 802.3i— для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории-3 или категории-5. Максимальная длина сегмента 100 метров.

FOIRL— (акроним от англ. Fiber-optic inter-repeater link). Базовый стандарт для технологии Ethernet, использующий для передачи данных оптический кабель. Максимальное расстояние передачи данных без повторителя 1 км.

10BASE-F, IEEE 802.3j— Основной термин для обозначения семейства 10 Мбит/с ethernet-стандартов, использующих оптоволоконный кабель на расстоянии до 2 километров: ***10BASE-FL, 10BASE-FB и 10BASE-FP***. Из перечисленного только ***10BASE-FL*** получил широкое распространение.

10BASE-FL (Fiber Link)— Улучшенная версия стандарта ***FOIRL***. Улучшение коснулось увеличения длины сегмента до 2 км.

10BASE-FB (Fiber Backbone)— Сейчас не используемый стандарт, предназначался для объединения повторителей в магистраль.

10BASE-FP (Fiber Passive)- Топология «пассивная звезда», в которой не нужны повторители— никогда не применялся.

Технология Fast Ethernet

Физический уровень Fast Ethernet

Для технологии Fast Ethernet разработаны различные варианты физического уровня, отличающиеся не только типом кабеля и электрическими параметрами импульсов, как это сделано в технологии 10 Мб/с Ethernet, но и способом кодирования сигналов, и количеством используемых в кабеле проводников. Поэтому физический уровень Fast Ethernet имеет более сложную структуру, чем классический Ethernet. Эта структура представлена на рисунке 11.

Устройство физического уровня (PHY) обеспечивает кодирование данных, поступающих от MAC-подуровня для передачи их по кабелю определенного типа, синхронизацию передаваемых по кабелю данных, а также прием и декодирование данных в узле-приемнике.

Интерфейс MII поддерживает независимый от используемой физической среды способ обмена данными между MAC-подуровнем и подуровнем PHY. Этот интерфейс аналогичен по назначению интерфейсу ***AUI*** классического Ethernet за исключением того, что интерфейс AUI располагался между подуровнем физического кодирования сигнала (для любых вариантов кабеля использовался одинаковый метод физического кодирования - манчестерский код) и подуровнем физического присоединения к среде, а интерфейс MII располагается между MAC-подуровнем и подуровнями кодирования сигнала, которых в стандарте ***Fast Ethernet*** три - ***FX, TX и T4***.

Подуровень согласования нужен для того, чтобы согласовать работу подуровня MAC с интерфейсом MII.

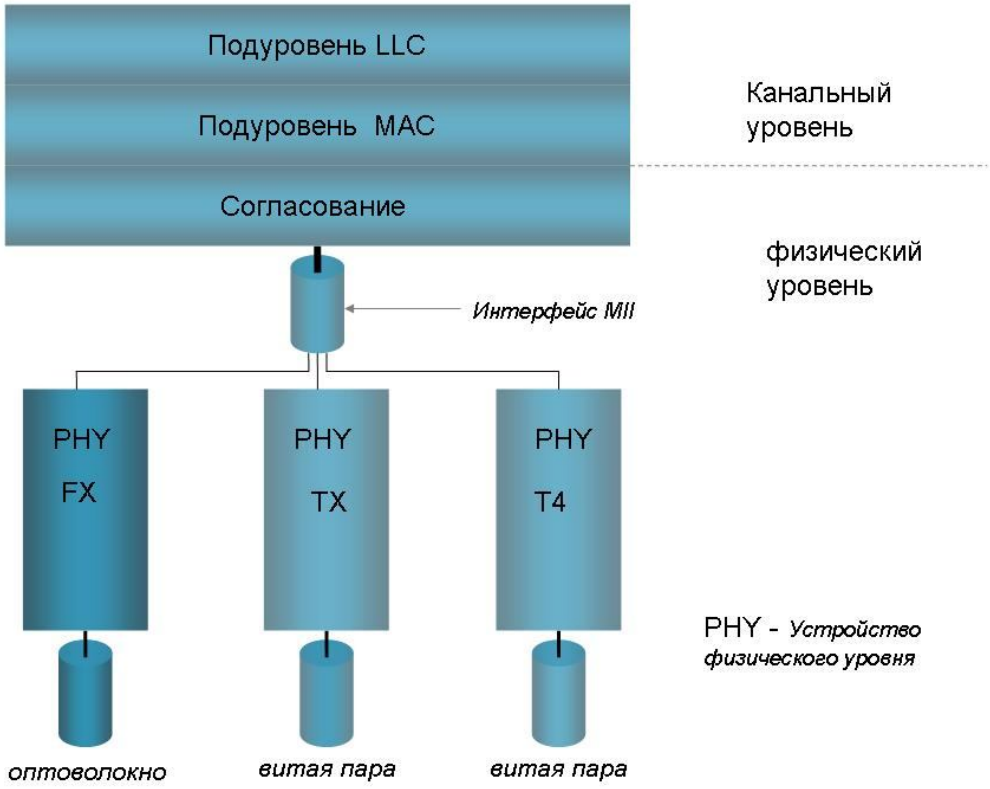


Рис. 90. Структура физического уровня Fast Ethernet

Физический уровень состоит из трех подуровней:

- Уровень согласования (reconciliation sublayer);
- Независимый от среды интерфейс (Media Independent Interface, MII);
- Устройство физического уровня (Physical layer device, PHY).

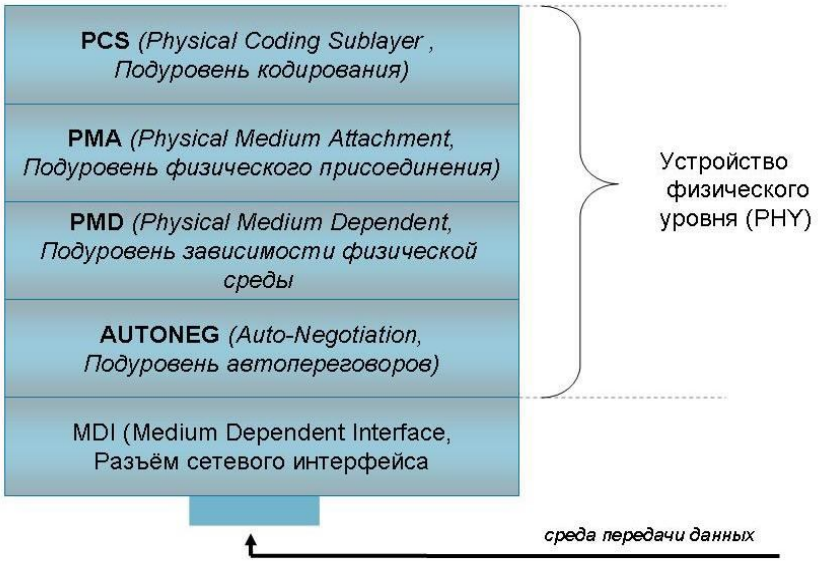


Рис. 91. Структура Устройства физического уровня (PHY).

Интерфейс MII (Media Independent Interface - независящий от среды передачи интерфейс) представляет собой стандартизованный интерфейс для подключения MAC-блока сети FastEthernet к блоку PHY. Интерфейс MII может быть выведен на разъём для подключения внешнего приемопередатчика или может просто соединять две микросхемы на одной печатной плате. Независимость от среды передачи означает, что существует возможность использования любых PHY-устройств без необходимости смены или переработки аппаратуры MAC-блока.

Интерфейс MII

Существует два варианта реализации интерфейса MII: внутренний и внешний.

При внутреннем варианте микросхема, реализующая подуровни MAC и согласования, с помощью интерфейса MII соединяется с микросхемой трансивера внутри одного и того же конструктива, например, платы сетевого адаптера или модуля маршрутизатора. Микросхема трансивера реализует все функции устройства PHY.

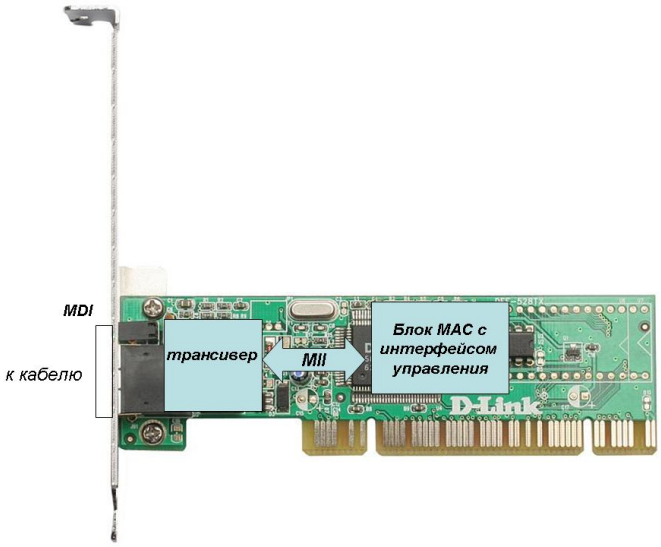


Рис. 92. Сетевой адаптер с внутренним интерфейсом MII

Внешний вариант соответствует случаю, когда трансивер вынесен в отдельное устройство и соединен кабелем MII через разъем MII с микросхемой MAC-подуровня. Разъем MII в отличие от разъема AUI имеет 40 контактов, максимальная длина кабеля MII составляет 1 метр. Сигналы, передаваемые по интерфейсу MII, имеют амплитуду 5 В.

Интерфейс MII может использоваться не только для связи PHY с MAC, но и для соединения устройств PHY с микросхемой повторения сигналов в многопортовом повторителе-концентраторе

MII использует 4-битные порции данных для параллельной передачи их между MAC и PHY. Канал передачи данных от MAC к PHY образован 4-битной шиной данных, которая синхронизируется тактовым сигналом, генерируемым PHY, а также сигналом «Передача», генерируемым MAC-подуровнем. Аналогично, канал передачи данных от PHY к MAC образован другой 4-битной шиной данных, которая синхронизируется тактовым сигналом и сигналом «Прием», которые генерируются PHY.

Если устройство PHY обнаружило ошибку в состоянии физической среды, то оно может передать сообщение об этом на подуровень MAC в виде сигнала «Ошибка приема» (receive error). MAC-подуровень (или повторитель) сообщают об ошибке устройству PHY с помощью сигнала «Ошибка передачи» (transmit error). Обычно, повторитель, получив от PHY какого-либо порта сиг-

нал «Ошибка приема», передает на все устройства PHY остальных портов сигнал «Ошибка передачи».

В MII определена двухпроводная шина для обмена между MAC и PHY управляющей информацией. MAC-подуровень использует эту шину для передачи PHY данных о режиме его работы. PHY передает по этой шине информацию по запросу о статусе порта и линии. Данные о конфигурации, а также о состоянии порта и линии хранятся соответственно в двух регистрах: ***регистре управления и регистре статуса.***

Регистр управления используется для установки скорости работы порта, для указания, будет ли порт принимать участие в процессе автопереговоров о скорости линии, для задания режима работы порта - полудуплексный или полнодуплексный, и т.п. Функция автопереговоров (Auto-negotiation) позволяет двум устройствам, соединенным одной линией связи, автоматически, без вмешательства оператора, выбрать наиболее высокоскоростной режим работы, который будет, поддерживается обоими устройствами.

Регистр статуса содержит информацию о действительном текущем режиме работы порта, в том числе и в том случае, когда режим выбран в результате проведения автопереговоров.

Регистр статуса может содержать данные об одном из следующих режимов:

- 100Base-T4;
- 100Base-TX полный дуплекс;
- 100Base-TX полудуплекс;
- 10 Мбит/с полный дуплекс;
- 10Мбит/с полудуплекс;
- ошибка на дальнем конце линии.

Авто согласование

Структура физического уровня спецификации ***PHY TX*** представлена на рисунке 14. В данной спецификации используется метод кодирования MLT-3 для передачи сигналов 5-битовых порций ***кода 4B/5B*** по витой паре, а также наличие функции автопереговоров (Auto-negotiation) для выбора режима работы порта.

Кроме использования метода MLT-3, в спецификации ***PHY TX*** используется пара шифратор-дешифратор (scrambler/descrambler), как это определено в спецификации ANSI TP-PMD. Шифратор принимает 5-битовые порции данных от подуровня PCS (подуровень физического кодирования), выполняющего кодирование NRZI (4B/5B), и зашифровывает сигналы перед передачей на подуровень MLT-3 таким образом, чтобы равномерно распределить энергию сигнала по всему частотному спектру - это уменьшает электромагнитное излучение кабеля.

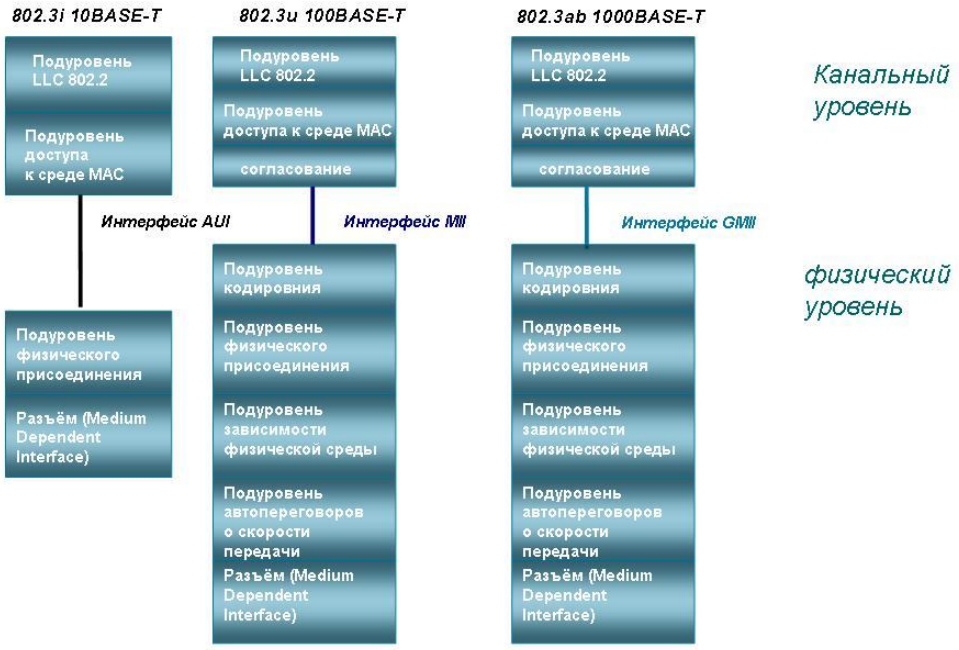


Рис. 93. Структура физического уровня IEEE 802

Спецификация PHY TX поддерживает функцию ***Auto-negotiation (авто согласование)***, с помощью которой два взаимодействующих устройства PHY могут автоматически выбрать наиболее эффективный режим работы.

Режим 10Base-T имеет самый низкий приоритет при переговорном процессе, а режим 100Base-TX - самый высокий. Переговорный процесс происходит при включении питания устройства, а также может быть инициирован и в любой момент модулем управления.

Для организации переговорного процесса используются служебные сигналы проверки целостности линии технологии 10Base-T - ***link test pulses***, если узел-партнер поддерживает только стандарт 10Base-T. Узлы, поддерживающие функцию ***авто согласования***, также используют существующую технологию сигналов проверки целостности линии, при этом они посылают пачки таких импульсов, ***инкапсулирующие*** информацию переговорного процесса ***авто согласования***. Такие пачки носят название ***Fast Link Pulse burst (FLP).*** Устройство, начавшее процесс ***авто согласования***, посылает своему партнеру пачку импульсов FLP, в котором содержится 8-битное слово, кодирующее предлагаемый режим взаимодействия, начиная с самого приоритетного, поддерживаемого данным узлом.

Инкапсуляция - это механизм, который объединяет данные и методы, манипулирующие этими данными, и защищает и то и другое от внешнего вмешательства или неправильного использования. Когда методы и данные объединяются таким способом, создается объект.

Можно сказать, что инкапсуляция подразумевает под собой скрытие данных, что позволяет защитить эти данные

Если узел-партнер поддерживает функцию авто согласования и также может поддерживать предложенный режим, то 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, каждые 16 миллисекунд посылает импульсы для проверки целостности линии, связывающей его с соседним узлом. Такой узел не понимает запрос FLP, который делает ему узел с функцией авто согласования, и продолжает посылать свои импульсы. Узел, получивший в ответ на запрос FLP только импульсы проверки целостности линии, понимает, что его партнер может работать только по стандарту 10Base-T и устанавливает этот режим работы и для себя.

Узлы, поддерживающие спецификации ***PHY FX (оптоволокно)*** *и* ***PHY TX***, могут работать в полнодуплексном режиме. В этом режиме не используется метод доступа к среде CSMA/CD и отсутствует понятие коллизий - каждый узел одновременно передает и принимает кадры данных по каналам Tx и Rx.

При полнодуплексной работе стандарты 100Base-TX и 100Base-FX обеспечивают скорость обмена данными между узлами 200 Мб/с.

Ниже, приведён набор стандартов передачи данных в компьютерных сетях, со скоростью до 100 Мбит/с

100BASE-T - общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару. Длина сегмента до 100 метров. Включает в себя стандарты ***100BASE-TX, 100BASE-T4 и 100BASE-T2***.

100BASE-TX, IEEE 802.3u— развитие стандарта 10BASE-T для использования в сетях топологии «звезда». Задействована витая пара категории 5, фактически используются только две неэкранированные пары проводников, поддерживается дуплексная передача данных, расстояние до 100 м.

100BASE-T4 - стандарт, использующий витую пару категории 3. Задействованы все четыре пары проводников, передача данных идёт в полудуплексе. Практически не используется.

100BASE-T2 - стандарт, использующий витую пару категории 3. Задействованы только две пары проводников. Поддерживается полный дуплекс, когда сигналы распространяются в противоположных направления по каждой паре.

Скорость передачи в одном направлении— 50 Мбит/с. Практически не используется.

100BASE-SX - стандарт, использующий многомодовое оптоволокно. Максимальная длина сегмента 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе.

100BASE-FX - стандарт, использующий одномодовое оптоволокно. Максимальная длина ограничена только величиной затухания в оптоволоконном кабеле и мощностью передатчиков.

100BASE-FX WDM - стандарт, использующий одномодовое оптоволокно. Максимальная длина ограничена только величиной затухания в оптоволоконном кабеле и мощностью передатчиков. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются одной латинской буквой: T (передатчик 1550 нм, приемник 1310 нм) или R (передатчик 1310 нм, приемник 1550 нм). В паре могут работать только парные интерфейсы: с одной стороны передатчик на 1310 нм, а с другой — на 1550 нм.

Технология Gigabit Ethernet

Физический уровень 1000Base-T - четырехпарная витая пара

1000Base-T - это стандартный интерфейс Gigabit Ethernet передачи по неэкранированной витой паре категории 5 и выше на расстояния до 100 метров. Для передачи используются все четыре пары медного кабеля, скорость передачи по одной паре 250 Мбит/с. Стандарт обеспечивает дуплексную передачу, причем данные по каждой паре передаются одновременно сразу в двух направлениях - двойной дуплекс (dual duplex). Технически реализовать дуплексную передачу 1 Гбит/с по витой паре UTP cat.5 оказалось довольно сложно. Влияние ближних и дальних переходных помех от трех соседних витых пар на данную пару в четырёх парном кабеле требует разработки специальной скремблированной помехоустойчивой передачи, и интеллектуального узла распознавания и восстановления сигнала на приеме.

Как и в стандарте Fast Ethernet, в Gigabit Ethernet не существует универсальной схемы кодирования сигнала, которая была бы идеальной для всех физических интерфейсов - для стандартов 1000Base-LX/SX/CX используется кодирование 8B/10B, для стандарта 1000Base-T используется специальный расширенный линейный код TX/T2. Функцию кодирования выполняет подуровень кодирования PCS, размещенный ниже среданезависимого интерфейса GMII.

GMII интерфейс. Среданезависимый интерфейс ***GMII (gigabit media independent interface)*** обеспечивает взаимодействие между уровнем MAC и физическим уровнем. GMII интерфейс является расширением интерфейса MII и

может поддерживать скорости 10, 100 и 1000 Мбит/с. Он имеет отдельные 8 битные приемник и передатчик, и может поддерживать как полудуплексный, так и дуплексный режимы. Кроме этого, GMII интерфейс несет один сигнал, обеспечивающий синхронизацию (clock signal), и два сигнала состояния линии - первый (в состоянии ON) указывает наличие несущей, а второй (в состоянии ON) говорит об отсутствии коллизий - и еще несколько других сигнальных каналов и питание. Трансиверный модуль, охватывающий физический уровень и обеспечивающий один из физических средазависимых интерфейсов, может подключать например к коммутатору Gigabit Ethernet посредством GMII интерфейса.

Подуровень физического кодирования PCS. При подключении интерфейсов группы 1000Base-X, подуровень PCS использует блочное избыточное кодирование 8B/10B, так же подуровень PCS осуществляет специальное помехоустойчивое кодирование, для обеспечения передачи по витой паре UTP Cat.5 на расстояние до 100 метров - линейный код TX/T2, Два сигнала состояния линии - сигнал наличие несущей и сигнал отсутствие коллизий - генерируются этим подуровнем.

Физический уровень Gigabit Ethernet использует несколько интерфейсов, включая традиционную витую пару категории 5, а также многомодовое и одномодовое волокно. Подуровень PMA преобразует параллельный поток символов от PCS в последовательный поток, а также выполняет обратное преобразование (распараллеливание) входящего последовательного потока от PMD. Подуровень PMD определяет оптические/электрические характеристики физических сигналов для разных сред. Всего определяются 4 различный типа физических интерфейса среды, которые отражены в стандартах IEEE 802.3z (1000Base-X) и 802.3ab (1000Base-T)

Физический уровень 1000Base-X

Интерфейс 1000Base-X основывается на стандарте физического уровня Fibre Channel. Fibre Channel - это технология взаимодействия рабочих станций, суперкомпьютеров, устройств хранения и периферийных узлов.

Блочный код 8B/10B аналогичен коду 4B/5B, принятому в стандарте FDDI. Однако код 4B/5B был отвергнут в Fibre Channel, потому что этот код не обеспечивает баланса по постоянному току. Отсутствие баланса потенциально может привести к зависящему от передаваемых данных нагреванию лазерных диодов, поскольку передатчик может передавать больше битов "1" (излучение есть), чем "0" (излучения нет), что может быть причиной дополнительных ошибок при высоких скоростях передачи.

1000Base-X подразделяется на три физических интерфейса, основные характеристики которых приведены ниже:

1. 1000Base-CX экранированная витая пара (STP "twinax") на короткие расстояния.

2. Интерфейс 1000Base-SX определяет лазеры с допустимой длиной излучения в пределах диапазона 770-860 нм, мощность излучения передатчика в пределах от -10 до 0 дБм, при отношении ON/OFF (сигнал / нет сигнала) не меньше 9 дБ. Чувствительность приемника -17 дБм, насыщение приемника 0 дБм;

Рис. 94. DEM-310GM2

Рис. 95. DEM-312GT2

3. Интерфейс 1000Base-LX определяет лазеры с допустимой длиной излучения в пределах диапазона 1270-1355 нм, мощность излучения передатчика в пределах от -13,5 до -3 дБм, при отношении ON/OFF (есть сигнал / нет сигнала) не меньше 9 дБ. Чувствительность приемника -19 дБм, насыщение приемника -3 дБм;

Рис. 96. DEM-331T

Рис. 97. DGS-703

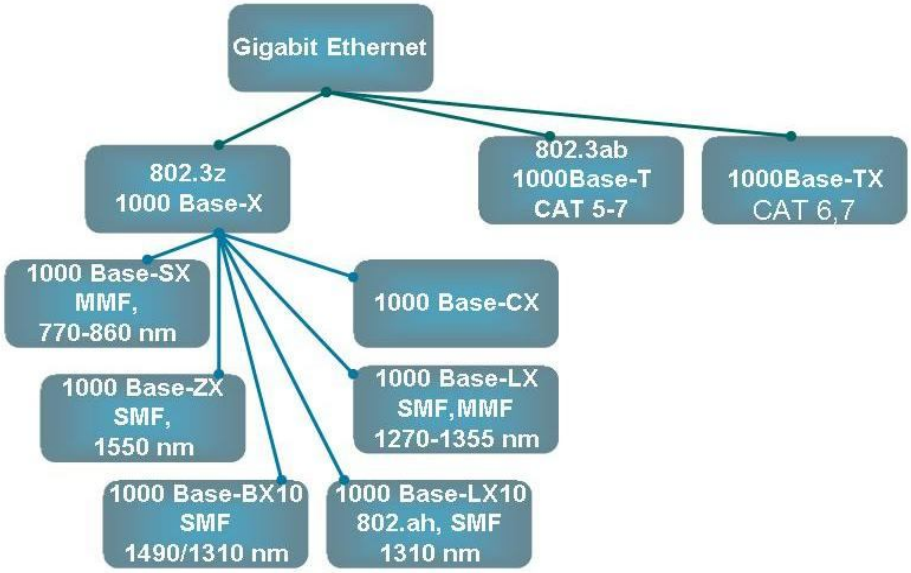


Рис. 98. Физические интерфейсы Gigabit Ethernet

1000BASE-T, IEEE 802.3ab - стандарт, использующий витую пару категорий 5e. В передаче данных участвуют 4 пары. Скорость передачи данных— 250Мбит/с по одной паре. Используется метод кодирования PAM5, частота основной гармоники 62,5 МГц.

1000BASE-TX был создан Ассоциацией Телекоммуникационной Промышленности (англ. Telecommunications Industry Association, TIA). Стандарт, использует раздельную приёмо-передачу (2 пары на передачу, 2 пары на приём, по каждой паре данные передаются со скоростью 500 Мбит/с), что существенно упрощает конструкцию приёмопередающих устройств. Но, как следствие, для стабильной работы по такой технологии требуется кабельная система высокого качества, поэтому 1000BASE-TX может использовать только кабель 6 категории. Ещё одним существенным отличием 1000BASE-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, в результате чего сложность, уровень энергопотребления и цена процессоров становится ниже, чем у процессоров стандарта 1000BASE-T. На основе данного стандарта практически не было создано продуктов, хотя 1000BASE-TX использует более простой протокол, чем стандарт 1000BASE-T, и поэтому может использовать более простую электронику.

1000BASE-X - общий термин для обозначения стандартов со сменными приёмопередатчиками GBIC или SFP.

1000BASE-SX, IEEE 802.3z - стандарт, использующий многомодовое оптоволокно. Дальность прохождения сигнала без повторителя до 550 метров.

1000BASE-LX, IEEE 802.3z - стандарт, использующий одномодовое оптоволокно. Дальность прохождения сигнала без повторителя до 5 километров.

1000BASE-LX10, IEEE 802.3ah - стандарт, использующий одномодовое оптоволокно. Дальность прохождения сигнала без повторителя до 10 километров.

1000BASE-CX — стандарт для коротких расстояний (до 25 метров), использующий твинаксиальный кабель с волновым сопротивлением 150 Ом. Заменён стандартом 1000BASE-T и сейчас не используется.

1000BASE-LH (Long Haul) - расширение стандарта LX, использует одномодовое оптоволокно. Дальность прохождения сигнала без повторителя до 50 километров.

1000BASE-LX WDM - расширение стандарта LX, позволяющее по одному оптическому волокну одномодового кабеля передавать сигнал до 40 км. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются одной латинской буквой T (передатчик 1550 нм, приемник 1310 нм) или R (передатчик 1310 нм, приемник 1550 нм).

1000BASE-ZX не стандартизированный, однако использующееся расширение стандарта LX. Позволяет передавать сигнал на расстояние до 80 км по одномодовому оптоволокну.

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

Технология 10 Gigabit Ethernet

Физический уровень 10GBase-SR, 10GBase-LR, 10GBase-ER

Строение физического интерфейса вполне типично, он состоит из трех уровней: PCS (Physical Coding Sublayer), отвечающий за управление передаваемыми битовыми последовательностями, PMA (Physical Medium Attachment) - преобразование группы кодов в последовательный поток бит и обратно, плюс синхронизация, и PMD (Physical Media Dependent), преобразующий биты в оптические сигналы. Традиционно, они выполнены логически независимыми друг от друга частями.

На каждую из длин волн принят свой PMD - 10GBASE-S для 850нм (от short), 10GBASE-L для 1310нм (long) и 10GBASE-E для 1550нм (extra long).

10GBASE-SR - Технология 10 Гигабит Ethernet для коротких расстояний (до 300 метров), используется многомодовое оптоволокно.

10GBASE-LR и 10GBASE-ER - эти стандарты поддерживают расстояния до 10 и 40 (80) километров соответственно. 10GBASE-LR использует лазеры 1310 нм, а 10GBASE-ER лазеры 1550 нм.

10GBASE-LX4 - использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому оптоволокну, IEEE 802.3 Clause 48 PCS и технологию «грубый» WDM. Данная спецификация позволяет поддерживать два типа оптоволокна. При использовании многомодового оптоволокна длина участка может достигать до 300 м, при скорости 10 Гбит/с, а при использовании одномодового оптоволокна расстояние увеличивается до 10 километров. Это достигается использованием 4-х лазерных источников, работающих на уникальных длинах волн в диапазоне 1300 нм.

10GBASE-LRM (Long Reach Multimode) также известный как IEEE ***802.3aq***, использует IEEE 802.3 Clause 49 64B/66B PCS и 1310 нм лазерные излучатели. Это обеспечивает передачу данных, используя многомодовый оптический кабель, со скоростью 10.3125 Гбит/с. 10GBASE-LRM поддерживает расстояния в 220 метров, при использовании многомодового оптического кабеля

10GBASE-ZR. Некоторые производители создали сменные интерфейсные устройства, для работы на расстоянии до 80 км. Так как эти устройства не определены стандартом IEEE 802.3ae,, изготовители создали свою спецификацию 10GBASE-ZR, описанную в спецификации OC-192/STM-64 SDH/SONET.

Модуль XFP, разрабатывался как универсальный модуль с оптическим интерфейсом. Основными достоинствами данного решения считаются большой список поддерживаемых скоростей (практически все возможные "около" 10 гигабит), и миниатюрные размеры.

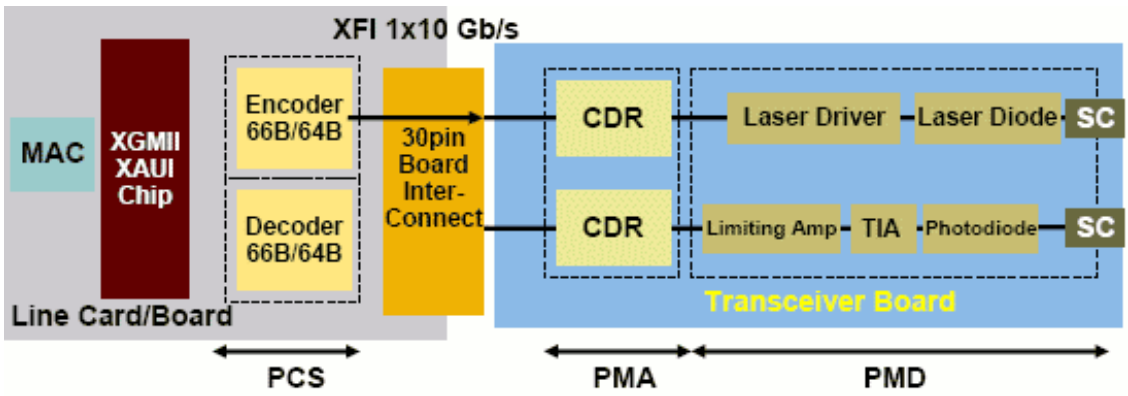


Рис. 99. Схема XFP 10G

Кодирование битовой последовательности (PCS) вынесено из модуля на основное устройство, и сам XFP является по сути универсальным последова-

тельным преобразователем, которому все равно, что передавать в линию .Внешний вид модуля показан на рис. 101.

Рис. 100. DEM-422XT

Технические особенности:

- интерфейс XFI 1*10G;
- размер устройства - 78*18*10 мм;
- не поддерживает стандарт 10GBASE-LX4;
- потребление электроэнергии - 3,5 Вт;
- коннектор 30 pin;
- оптический разъем LC;
- реализован в устройствах D-Link : DEM-421XT, DEM-422XT, DEM-423XT
- поддерживает скорости, отличные от 10GB (10.3 Гбит/с), - OC-192/STM-64 9,95 Gb/c, 10G FC 10,5 Gb/c, G.709 10,709 Gb/c.

Физический уровень 10GBase-CX4

10GBASE-CX4— Технология 10 Гигабит Ethernet для коротких расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand. Этот стандарт был первым опубликованным «медным» 10 Гигабитным стандартом как IEEE 802.3ak-2004. Он использует 4-х линейный интерфейс XAUI, подуровень физического кодирования PCS (Clause 48) и прокладку медного кабеля аналогично использовавшемуся в InfiniBand. Длина участка 15 м, скорость в каждой паре 3.125 Гбит/с. Ориентирован этот вид на внутриузловые соединения.

> ***Infiniband*** — высокоскоростная коммутируемая последовательная шина, применяющаяся как для внутренних (внутрисистемных), так и для межсистемных соединений

Хотя этот вариант 10-ти гигабитного Ethernet не является оптическим, он так же далеко от витой пары, как и от "стекла". Частотные возможности твинаксиального кабеля близки к оптическому, соответственно, используются похожие технические решения.

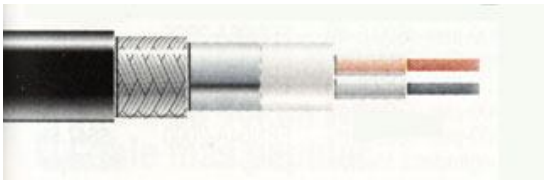


Рис. 101. Твинаксиальный кабель.

Разработчики пошли примерно по тому же пути, как в вышеописанном 10GBASE-LX4. А именно, применили четырех дифференциальных передатчика и приемника на каждую линию. В каждом канале скорость 2,5 Гбит/с, тактовая частота 3,125 ГГц и кодированием по стандарту 8B/10B (т.е. тому же, что и в LX4). Для этого требуются четыре дифференциальные пары, работающие в каждом направлении, и, соответственно, общее число твинаксиальных каналов в соединительном кабеле равно восьми.

Рис. 102. DEM-412CX

Рис. 103. D-Link DEM-CB300CX. Кабель 10GE-CX4, 3 м

Модули D-Link с портом CX4 предоставляют предприятиям доступное по цене, высокопроизводительное сетевое подключение со скоростью 10 GE по коаксиальному медному кабелю. Этот медный кабель значительно дешевле оптоволоконного и позволяет передавать информацию на расстояния от 15 до 20 метров в зависимости от сортамента проводов. Модули не требуют установки дорогостоящих трансиверов, исключая необходимость в их приобретении.

Модули с портом CX4 устанавливаются в открытые слоты гигабитных коммутаторов D-Link DGS-34xx. При работе в режиме полного дуплекса порт обеспечивает полосу пропускания до 20 Гбит/с. Модули можно использовать для высокоскоростного стекирования коммутаторов или их подключения к корневому коммутатору на основе шасси. Также они могут применяться при подключении серверов или сетевых устройств хранения информации с поддержкой CX4.

Модули с портом CX4 - это идеальное решение для организации высокоскоростного сетевого подключения внутри высокопроизводительных вычислительных кластеров и серверных комнат.

10GBASE-T, IEEE 802.3an. Использует экранированную витую пару. Расстояние до 100 метров.

10GBASE-KX4, 10GBASE-KR. Backplane Ethernet — направление деятельности рабочей группы 802.3ap — использование объединительных плат для «блэйд-серверов» (blade servers) и маршрутизаторов/коммутаторов с расширительными сетевыми картами. Стандарт IEEE 802.3ap реализован на участке медного кабеля на расстояниях до 1 метра, со скоростью 10 Гбит/с. В 10Gbase-KX4 используется подуровень физического кодирования IEEE 802.3 Clause 48, а в 10GBASE-KR используется подуровень физического кодирования IEEE 802.3 Clause 49.

В настоящее время в сфере Ethernet приоритет отдан разработке стандартов 40/100 Гбит/с.

Перспективные темы группы IEEE 802.3

802.3av, 10GEPON (10 Гигабит EPON). Потребность в увеличении пропускной способности существует и на уровне доступа. Это объясняется тем, что в будущем одной семье могут понадобиться, к примеру, четыре канала телевидения высокой четкости ***(High Definition Television, HDTV)*** или широкоэкранное цифровое изображение ***(Large Scale Digital Imagery, LSDI).*** 10GEPON представляет собой расширение стандарта IEEE ***802.3ah, EFM***. Ратифицированный в 2004 г. стандарт определяет технологию Gigabit EPON, которая, как ожидается, будет расширена до 10 Гбит/с. Между коммутационным узлом и домашней сетью развертывается распределительная сеть, по которой через оптическое волокно подается 10 Гбит/с для 32 домохозяйств.

802.3at, DTE Power Enhancements. Стандарт IEEE 802.3af, DTE Power, был принят в 2003 г. Предусмотренных в нем 15 Вт сегодня недостаточно. Новый стандарт IEEE ***802.3at, PoE Plus***, совместим с существующим, и обеспечивать мощность 30 Вт.

802.3az, энергоэффективные сети Ethernet (Energy Efficient Ethernet). Рабочая группа 802.3az занялась актуальными вопросами экономии электроэнергии. Ее деятельность началась в марте 2007 г., и уже в ноябре того же года группа получила задание PAR. Лавинообразно растущий сетевой сегмент может внести значительный вклад в экономию энергии. Суть идеи заключается в переводе соединений в режим низкого энергопотребления (Low Power), когда передавать данные не требуется. Режим Low Power реализуется путем уменьшения скорости передачи вплоть до нуля.

802.3ba, 40/100 Gigabit Ethernet: для того чтобы удовлетворить потребность в еще большей пропускной способности, в ноябре 2006 г. проектная группа IEEE P802 учредила «группу исследования высоких скоростей» (High Speed Study Group), которая в декабре 2007 г. под эгидой рабочей группы IEEE 802.3ba получила «запрос на авторизацию проекта» (Project Authorization Request, PAR) о разработке стандарта Ethernet на 40/100 Гбит/с со следующими задачами:

- поддержка исключительно полнодуплексного режима;
- поддержка обоих форматов кадров (CSMA/CD и Ethernet V2.0);
- сохранение минимальной и максимальной длины кадров;
- поддержка оптических транспортных сетей (Optical Transport Network, OTN);
- скорость передачи данных 40 и 100 Гбит/с.

«На выходе» ожидается технология с поддержкой оптического волокна, меди и объединительных плат ***(Backplane).*** Эти расширения Ethernet касаются только физического уровня модели OSI. Подуровень MAC остается без изменений. Аналогично обстоит дело с MAC Control и Logical Link Control (LLC). Стандарт ратифицирован в 2010 году, и вскоре должно появится оборудование с его поддержкой.

Беспроводные технологии

Кроме стандартов для проводных линий и каналов, информационных сетей, разработаны стандарты для беспроводных соединений.

IEEE 802.11 (Wi-Fi)

IEEE 802.11 — набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц. Пользователям

более известен по названию ***Wi-Fi,*** фактически являющийся брендом, предложенным и продвигаемым организацией ***Wi-Fi Alliance*****. «Wi-Fi»** — торговая марка **«Wi-Fi Alliance».** Технологию назвали **Wireless-Fidelity (дословно «беспроводная точность»)** по аналогии с Hi-Fi.

Изначально стандарт ***IEEE 802.11*** предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей, ***IEEE 802.11a,*** определяет скорость передачи уже до 54 Мбит/с. Рабочий диапазон стандарта 5 ГГц. + использование ***OFDM.***

OFDM (англ. Orthogonal frequency-division multiplexing) является цифровой схемой модуляции, которая использует большое количество близко расположенных ортогональных поднесущих. Каждая поднесущая модулируется по обычной схеме модуляции (например, квадратурная амплитудная модуляция) на низкой символьной скорости, сохраняя общую скорость передачи данных, как и у обычных схем модуляции одной несущей в той же полосе пропускания. На практике сигналы OFDM получаются путем использования БПФ (Быстрое преобразование Фурье).

Вопреки своему названию, принятый в 1999 году стандарт ***IEEE 802.11b*** не является продолжением стандарта IEEE 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в IEEE 802.11b против OFDM в IEEE 802.11a. Стандарт предусматривает использование диапазона частот 2,4 ГГц. Скорость передачи до 11 Мбит/с. Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией ***Wireless Ethernet Compatibility Alliance (WECA),*** которая в настоящее время больше известна под названием ***Wi-Fi Alliance***.

Проект стандарта ***IEEE 802.11g*** был утверждён в 2003г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость передачи 54 Мбит/с и превосходя, таким образом, стандарт IEEE 802.11b (который обеспечивает скорость передачи 11 Мбит/с). Кроме того, он гарантирует обратную совместимость со стандартом IEEE 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость передачи будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость составляет 54 Мбит/с.

Производители всегда стремятся представить быстрые беспроводные продукты. Например, стандарт IEEE 802.11g неофициально преодолел лимит 54 Мбит/с с помощью технологий объединения каналов ***Super G, AirPlusXtremeG, MIMO, Turbo*** и получил поддержку пропускной способности 108 и даже 150 Мбит/с.

Рис. 104 Беспроводной маршрутизатор DIR-300/NRU Wireless 150

IEEE 802.11y-2008 дополненный стандарт IEEE 802.11-2007 предусматривает использование оборудования Wi-Fi с рабочими частотами 3650 - 3700 МГц на территории США Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.

IEEE 802.11n — новейшая версия стандарта IEEE 802.11 для сетей Wi-Fi. Стандарт IEEE 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандарта IEEE 802.11g, при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически IEEE 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с. Устройства 802.11n работают в диапазонах 2,4 — 2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

- наследуемом (Legacy), в котором обеспечивается поддержка устройств 802.11b/g и 802.11a
- смешанном (Mixed), в котором поддерживаются устройства 802.11b/g, 802.11a и 802.11n
- «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом IEEE 802.11n).

Основные направления деятельности IEEE по темам беспроводной передачи данных

802.11, беспроводные локальные сети с наиболее важными на данный момент группами:

Группа High-Throughput Study Group (HTSG);

802.11ac, Very High Throughput, работает над гигабитной технологией;

802.15, беспроводные персональные сети (Wireless Personal Area Network, Wireless PAN), технологию Bluetooth планируется дополнить следующими функциями: TG3c, mmWave PHY - 1-2 Гбит/с для применения внутри помеще-

ний; ячеистые сети TG5 (Mesh Networking); «телесные сети» TG6 BAN (Body Area Networks), а также TG7 (Visual Light Communication) - связь при помощи видимого света;

802.16, широкополосный беспроводной доступ (Broadband Wireless Access). Этой темой занимаются три группы: 802.16h, 802.16j, мобильная многоузловая трансляция (Mobile Multihop Relay); 802.16m, усовершенствованный воздушный интерфейс (Advanced Air Interface), разрабатывающая гигабитную технологию.

Исследователи уже смотрят в сторону гигабитных беспроводных сетей. Группа ***High-Throughput Study Group (HTSG),*** которая ранее ставила задачу добиться утверждения 802.11n, разделилась на два новых образования, которые работают над будущими стандартами с частотами до ***6 ГГц (IEEE 802.11ac) и 60 ГГц (IEEE 802.11ad).*** Эти беспроводные технологии потенциально могут удвоить пропускную способность 802.11n.

Организация ***IEEE (Institute of Electrical and Electronics Engineers - Институт инженеров по электротехнике и радиоэлектронике)*** объявила о планах по разработке стандарта IEEE ***802.11ac*** для Wi-Fi, который обещает стать одним из ключевых нововведений в сфере беспроводной передачи данных в ближайшие два года. Ожидается, что в новый стандарт, построенный на базе IEEE 802.11a, будет использовать каналы шириной 80 МГц или даже 160 МГц. В перспективе разработка сможет обеспечить пропускную способность эквивалентную Gigabit Ethernet: 1 Гбит/с, что более чем в три раза превышает характеристики недавно утвержденного стандарта IEEE 802.11n (600 Мбит/с). На данный момент проект находится на стадии обсуждения. Предположительно испытания начнутся в конце 2011 года, а окончательное утверждение стандарта произойдет в декабре 2012.

Вместе с тем пока Wi-Fi только планирует подобраться к отметке 1 Гбит/с, организация ***Wireless Gigabit Alliance***, ответственная за продвижение беспроводной 60-ГГц технологии, уже заявила о завершении работ над первой версией спецификации ***WiGig (IEEE 802.11ad).***. Новый стандарт предусматривает более чем в десять раз большую пропускную способность по сравнению с самыми быстрыми современными сетями Wi-Fi. При этом, что немаловажно, сохранена обратная совместимость с существующими на рынке Wi-Fi устройствами.

Несмотря на высокую производительность технологии ***WiGig***, она уступает современному Wi-Fi по дальности действия. Если Wi-Fi в помещениях позволяет связывать устройства на расстоянии в несколько десятков метров, то ***WiGig*** гарантирует качественное соединение на расстоянии всего 10 метров. Впрочем, во многих случаях этого может оказаться вполне достаточно для организации домашней беспроводной сети. Напомним, недавно представленный стандарт ***WHDI 1.0*** имеет дальность связи в тридцать метров, но его максимальная скорость передачи данных не превышает 3 Гбит/с.

Новый стандарт ***Wireless Home Digital Interface (WHDI)*** предусматривает передачу высококачественного несжатого видео 1080p/60 Гц на расстояние до тридцати метров, при этом стены – не помеха. WHDI позволяет пользователям строить беспроводные HD-сети у себя дома и наслаждаться новейшими интерактивными сервисами. Источниками видео высокого разрешения, которое передается на телевизоры (а их в квартире может быть несколько), могут выступать самые разнообразные устройства, включая настольные персональные компьютеры, ноутбуки и нетбуки, смартфоны, карманные плееры. Подключение устройств с логотипом WHDI удобное и простое, и не требует прокладки кабелей.

Спецификацией предусмотрена пропускная способность сети до трёх гигабит в секунду в 40-МГц полосе 5-ГГц диапазона. Задержка сигнала составляет менее одной миллисекунды. Также в WHDI предусмотрена поддержка защиты контента HDCP 2.0.

Технология WiMax

WiMax (англ. Worldwide Interoperability for Microwave Access)— телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте ***IEEE 802.16***, который также называют Wireless MAN. Название «WiMax» было создано WiMax Forum — организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMax. Форум описывает WiMax как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL»

WiMax подходит для решения следующих задач:

Соединения точек доступа Wi-Fi друг с другом и другими сегментами Интернета.

Обеспечения беспроводного широкополосного доступа как альтернативы выделенным линиям и DSL.

Предоставления высокоскоростных сервисов передачи данных и телекоммуникационных услуг.

Создания точек доступа, не привязанных к географическому положению.

WiMax позволяет осуществлять доступ в Интернет на высоких скоростях, с гораздо большим покрытием, чем у Wi-Fi сетей. Это позволяет использовать технологию в качестве «магистральных каналов», продолжением которых выступают традиционные DSL- и выделенные линии, а также локальные сети. В результате подобный подход позволяет создавать масштабируемые высокоскоростные сети в масштабах целых городов.

IEEE 802.16-2004 (известен также как IEEE 802.16d и фиксированный WiMax). Спецификация утверждена в 2004 году. Используется ортогональное

частотное мультиплексирование (OFDM), поддерживается фиксированный доступ в зонах с наличием либо отсутствием прямой видимости. Пользовательские устройства представляют собой стационарные модемы для установки вне и внутри помещений, а также PCMCIA-карты для ноутбуков. В большинстве стран под эту технологию отведены диапазоны 3,5 и 5 ГГц. По сведениям WiMax Forum, насчитывается уже порядка 175 внедрений фиксированной версии. Многие аналитики видят в ней конкурирующую или взаимодополняющую технологию проводного широкополосного доступа DSL.

IEEE 802.16-2005 (известен также как IEEE 802.16e и мобильный WiMax). Спецификация утверждена в 2005 году. Это — новый виток развития технологии фиксированного доступа (IEEE 802.16d). Оптимизированная для поддержки мобильных пользователей версия поддерживает ряд специфических функций, таких как хэндовер (англ.), idle mode и роуминг. Применяется масштабируемый OFDM-доступ (SOFDMA), возможна работа при наличии либо отсутствии прямой видимости. Планируемые частотные диапазоны для сетей Mobile WiMax таковы: 2,3–2,5; 2,5–2,7; 3,4–3,8 ГГц. Конкурентами IEEE 802.16e являются все мобильные технологии третьего поколения (например, EV-DO, HSDPA).

Основное различие двух технологий состоит в том, что фиксированный WiMax позволяет обслуживать только «статичных» абонентов, а мобильный ориентирован на работу с пользователями, передвигающимися со скоростью до 120 км/ч. Мобильность означает наличие функций роуминга и «бесшовного» переключения между базовыми станциями при передвижении абонента (как происходит в сетях сотовой связи). В частном случае, мобильный WiMax может применяться и для обслуживания фиксированных пользователей.

Таблица 7.Сравнительная таблица стандартов беспроводной связи

Технология	Стандарт IEEE	Использование	Пропускная способность	Радиус действия	Частоты
UWB	802.15.3a	WPAN	110–480 Мбит/с	до 10 метров	7,5 ГГц
Wi-Fi	802.11a	WLAN	до 54 Мбит/с	до 100 метров	5,0 ГГц
Wi-Fi	802.11b	WLAN	до 11 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11g	WLAN	до 108 Мбит/с	до 100 метров	2,4 ГГц
Wi-Fi	802.11n	WLAN	до 300 Мбит/с (в перспективе до 450, а за-	до 100 метров	2,4 — 2,5 или 5,0 ГГц

			тем до 600 Мбит/с)		
WiMax	802.16d	WMAN	до 75 Мбит/с	6–10 км	1,5–11 ГГц
WiMax	802.16e	Mobile WMAN	до 30 Мбит/с	1–5 км	2–6 ГГц
WiMax	802.16m	WMAN, Mobile WMAN	до 1 Гбит/с (WMAN), до 100 Мбит/с (Mobile WMAN)	н/д (стандарт в разработке)	н/д (стандарт в разработке)

WiMax это система дальнего действия, покрывающая километры пространства, которая обычно использует лицензированные спектры частот (хотя возможно и использование нелицензированных частот) для предоставления соединения с интернетом типа точка-точка провайдером конечному пользователю. Разные стандарты семейства IEEE 802.16 обеспечивают разные виды доступа, от мобильного (схож с передачей данных с мобильных телефонов) до фиксированного (альтернатива проводному доступу, при котором беспроводное оборудование пользователя привязано к местоположению).

Wi-Fi это система более короткого действия, обычно покрывающая сотни метров, которая использует нелицензированные диапазоны частот для обеспечения доступа к сети. Обычно Wi-Fi используется пользователями для доступа к их собственной локальной сети, которая может быть и не подключена к Интернету. Если WiMax можно сравнить с мобильной связью, то Wi-Fi скорее похож на стационарный беспроводной телефон.

WiMax и Wi-Fi имеют совершенно разный механизм Quality of Service (QoS). WiMax использует механизм, основанный на установлении соединения между базовой станцией и устройством пользователя. Каждое соединение основано на специальном алгоритме планирования, который может гарантировать параметр QoS для каждого соединения. Wi-Fi, в свою очередь, использует механизм QoS подобный тому, что используется в Ethernet, при котором пакеты получают различный приоритет. Такой подход не гарантирует одинаковый QoS для каждого соединения.

Из-за дешевизны и простоты установки, Wi-Fi часто используется для предоставления клиентам быстрого доступа в Интернет различными организациями. Например, в некоторых кафе, отелях, вокзалах и аэропортах можно обнаружить бесплатную точку доступа Wi-Fi.

Ведущие разработчики, поставщики элементной базы и производители оборудования WiMax выдвинули инициативу, направленную на ускорение внедрения нового поколения технологии WiMax, известного под обозначением WiMax 2.

Технология WiMax 2 будет построена на стандарте IEEE 802.16m, представляющем собой стандарт IEEE 802.16e, дополненный новыми возможностями, но сохранивший обратную совместимость. Стандарт соответствует требованиям International Telecommunications Union для 4G (или IMT-Advanced) по части производительности — пиковое значение скорости передачи превышает 300 Мбит/с, задержки уменьшены, а «вместимость» с точки зрения приложений VoIP увеличена. Эти изменения помогут операторам WiMax соответствовать взрывному росту потребностей широкополосного доступа, вызванному распространением мультимедийных мобильных приложений.

Технология 3G

3G (от англ. third generation— «третье поколение»), технологии мобильной связи 3 поколения— набор услуг, который объединяет как высокоскоростной мобильный доступ с услугами сети Интернет, так и технологию радиосвязи, которая создаёт канал передачи данных.

Стандарт 3G был разработан Международным союзом электросвязи (International Telecommunication Union, ITU) и носит название IMT-2000 (International Mobile Telecommunications 2000). Основная цель — гармонизация систем третьего поколения для обеспечения глобального роуминга — в настоящее время труднодостижима, так как многие из них работают в разных стандартах: под аббревиатурой IMT-2000, объединены 5 стандартов, а именно:

- W-CDMA
- CDMA2000
- TD-CDMA/TD-SCDMA
- DECT
- UWC-136

Из этих пяти только три первых — ***W-CDMA, CDMA2000 и TD-CDMA/TD-SCDMA*** обеспечивают полное покрытие в макро-, микро- и пикосотах, и поэтому фактически только они могут рассматриваться в качестве полноценных 3G-решений. В числе остальных стандартов, ***DECT*** используется, в частности, в беспроводных телефонах домашнего и офисного назначения. Кроме того, он может применяться для организации 3G хот-спотов с небольшой зоной обслуживания (с этой точки зрения его можно рассматривать в качестве подмножества "большой" 3G-сети). И, наконец, ***UWC-136*** — это просто другое название технологии ***EDGE***, которую обычно относят к ***2,5G***. В 2007 году к этому стандарту причислили и WiMax.

Наибольшее распространение в мире получили два стандарта: UMTS (или W-CDMA) и CDMA2000 (IMT-MC), в основе которых лежит одна и та же технология— CDMA (Code Division Multiple Access— множественный доступ с кодовым разделением каналов). Также возможно использование стандарта CDMA450.

Технология CDMA2000 обеспечивает эволюционный переход от узкополосных систем с кодовым разделением каналов IS-95 (американский стандарт цифровой сотовой связи второго поколения) к системам CDMA «третьего поколения» и получила наибольшее распространение на североамериканском континенте, а также в странах Азиатско-Тихоокеанского региона.

Технология UMTS (Universal Mobile Telecommunications Service— универсальная система мобильной электросвязи) разработана для модернизации сетей GSM (европейского стандарта сотовой связи второго поколения), и получила широкое распространение не только в Европе, но и во многих других регионах мира.

Работа по стандартизации UMTS координируется международной группой 3GPP (Third Generation Partnership Project), а по стандартизации CDMA2000— международной ***группой 3GPP2 (Third Generation Partnership Project 2),*** созданными и сосуществующими в рамках ITU.

В сетях 3G обеспечивается предоставление двух базовых услуг: передача данных и передача голоса. Согласно регламентам ITU (International Telecommunications Union)— Международный Союз Электросвязи) сети 3G должны поддерживать следующие скорости передачи данных:

- для абонентов с высокой мобильностью (до 120 км/ч)— не менее 144 кбит/с;
- для абонентов с низкой мобильностью (до 3 км/ч)— 384 кбит/с;
- для неподвижных объектов— 2,048 кбит/с.

Технология HSDPA

HSDPA (англ. High-Speed Downlink Packet Access — высокоскоростная пакетная передача данных от базовой станции к мобильному телефону) — стандарт мобильной связи, рассматривается специалистами как один из переходных этапов миграции к технологиям мобильной связи четвёртого поколения (4G). Максимальная теоретическая скорость передачи данных по стандарту составляет 14,4 Мбит/сек, практически же достижимая скорость в существующих сетях обычно не превышает 4 Мбит/сек.

Технология 4G

4G— перспективное (четвёртое) поколение мобильной связи, характеризующееся высокой скоростью передачи данных и повышенным качеством голосовой связи. К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с.

В отличие от 3G, стандартизованного Международным союзом электросвязи как IMT-2000, общепринятого определения для 4G по состоянию на 2009

г. не существует. Сторонники технологии WiMax иногда утверждают, что WiMax относится к четвёртому поколению мобильной связи, однако такой взгляд не является общепринятым, так как стандарт не обладает функционалом телефонной связи, а является одной из многочисленных технологий беспроводного широкополосной передачи данных.

В конце января 2008 г. спецификация сети LTE-TRAN (LTE Terrestrial Radio Access Network) была одобрена организацией 3GPP (3rd Generation Partnership Project) и стала частью спецификаций 3GPP Release 8. Фактически, эта технология базируется на радиоинтерфейсе OFDMA (Orthogonal Frequency Division Multiple Access) и технологии MIMO (Multiple Input Multiple Output). Кроме того, протокол LTE уже поддерживают решения таких компаний, как Alcatel-Lucent, Broadcom, Ericsson, Hewlett-Packard, LSI Logic, Motorola, Nokia-Siemens Networks, Panasonic, Qualcomm, Telcordia и т.д.

Long Term Evolution (LTE) – стандарт сотовой связи, позволяющий передавать и принимать информацию на скорости 100-326 Мбит/с. Для сетей LTE используются диапазоны 760-870 МГц и 2000 МГц. Технология LTE должна прийти на смену сетям сотовой связи третьего поколения (3G). Технология Long Term Evolution, как ожидается, приведет к появлению качественно новых мобильных сервисов: пользователи смогут здесь и сейчас получать высококачественное видео, работать с интерактивными службами.

На сегодняшний день, провайдер мобильной связи ***TeliaSonera*** сообщает, что его усилиями введены в эксплуатацию первые в мире коммерческие сети 4G, работающие по протоколу LTE. Протестировать их работу смогут жители центральных частей Стокгольма, Швеция и Осло, Норвегия.

1.19. Адресация

Типы адресов стека TCP/IP

Распознаются объекты компьютерной сети с помощью адресации. Канальный уровень имеет дело только с физическими адресами устройств (иногда называются также MAC-адресами). Физические адреса устройств — это уникальные адреса оборудования. Чаще всего они назначаются производителями оборудования, которые используют адреса, закрепленные за ними стандартизирующей организацией. Формат адреса зависит от используемого метода доступа к среде передачи.

Хотя сетевые компьютеры могут быть идентифицированы по их физическим адресам, фактическая доставка данных в локальной сети обычно осуществляется передачей фрейма всем сетевым устройствам. Каждое устройство читает физический адрес фрейма, и если его физический адрес соответствует адресу во фрейме, забирает данные. Все другие устройства игнорируют остальную часть фрейма. Физические адреса устройств используются мостами (маршрутизаторами) для выборочного повтора сигналов данных на раздельных сегментах

среды передачи. Кроме того в любых сетях, в том числе и в TCP/IP, необходимо идентифицировать отдельные, взаимодействующие между собой устройства и программы.

В стеке TCP/IP используется три типа адресов:

1. ***Локальный (физический, аппаратный адрес, MAC-адрес***) – тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, которая является элементом составной интерсети. Адрес имеет формат 6 байт и назначается производителем оборудования и является уникальным.

2. ***IP-адрес (читается как айпи-адрес)*** – представляет собой основной тип адресов, на основании которых сетевой уровень передаёт пакеты между сетями. ***IP*** - это основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. ***IP версии 4 (IPv4)*** занимает 4 байта, например, 192.168.17.25. Если IPX/IPX использует MAC-адреса канального уровня, то IP-адресация - это самостоятельная, независимая от технологий канального уровня, система адресации. Это было сделано преднамеренно, так как TCP/IP предназначался изначально для объединения локальных сетей, использующих разнообразные технологии передачи данных, и, следовательно, нужна была самостоятельная система адресации, позволяющая уникально идентифицировать любой компьютер в глобальном масштабе. IP-адреса назначаются администратором во время конфигурирования компьютеров и маршрутизатора в ручную или с помощью протокола ***DHCP.***

3. ***Символьно-доменное имя*** (expertise.dlink.com.tw). Символьные имена разделяются точками.

В терминологии TCP/IP под ***локальным адресом*** понимается такой тип адреса, который используется средствами базовой технологии для доставки данных в пределах подсети, являющейся элементом составной интерсети. В разных подсетях допустимы разные сетевые технологии, разные стеки протоколов, поэтому при создании стека TCP/IP предполагалось наличие разных типов локальных адресов. Если подсетью интерсети является локальная сеть, то локальный адрес - это MAC - адрес.

MAC - адрес назначается сетевым адаптерам и сетевым интерфейсам маршрутизаторов. MAC - адреса назначаются производителями оборудования и являются уникальными, так как управляются централизованно. Для всех существующих технологий локальных сетей MAC - адрес имеет формат 6 байт, например 00-1F-16-06-57-06. Однако протокол IP может работать и над протоко-

лами более высокого уровня, например над протоколом IPX или X.25. В этом случае локальными адресами для протокола IP соответственно будут адреса IPX и X.25. Следует учесть, что компьютер в локальной сети может иметь несколько локальных адресов даже при одном сетевом адаптере. Некоторые сетевые устройства не имеют локальных адресов. Например, к таким устройствам относятся глобальные порты маршрутизаторов, предназначенные для соединений типа «точка-точка».

IP –адресация

IP-адреса (Ipv4) представляют собой основной тип адресов, на основании которых сетевой уровень передает пакеты между сетями. Эти адреса состоят из 4 байт, например 109.26.17.100. IP-адрес назначается администратором во время конфигурирования компьютеров и маршрутизаторов. IP-адрес состоит из двух частей: номера сети и номера узла. Номер сети может быть выбран администратором произвольно, либо назначен по рекомендации специального подразделения Internet (Internet Network Information Center, InterNIC), если сеть должна работать как составная часть Internet. Обычно поставщики услуг Internet получают диапазоны адресов у подразделений InterNIC, а затем распределяют их между своими абонентами.

IP-адрес состоит из двух частей:

- ***Номер сети*** – выбирается администратором произвольно или назначается службой InterNic (Internet Network Information Center), если подсеть должна работать как составная часть Internet, Поставщики услуг Internet (или провайдеры) получают диапазоны IP-адресов, а затем распределяется между абонентами сети. IP — не зависит от локального адреса компьютера.
- ***Номер узла в сети*** – назначается независимо от локального адреса узла.

IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей.

Если адрес начинается с 0 (а мы помним, что 0=БИТ), то сеть относят к ***классу А*** и номер сети занимает 1 байт, номер узла 3 байта. Сети класса А имеют номера в диапазоне от 1 до 126. Таких сетей немного, зато количество узлов в них может достигать $2^{24.}$

Если первые два бита равны 10, то сеть относится к ***классу B***. Является сетью средних размеров, максимальное количество узлов в которой равняется 2^{16}.

Если адрес начинается последовательностью 110, то он относится к ***классу C***, количество узлов в котором равняется 2^8.

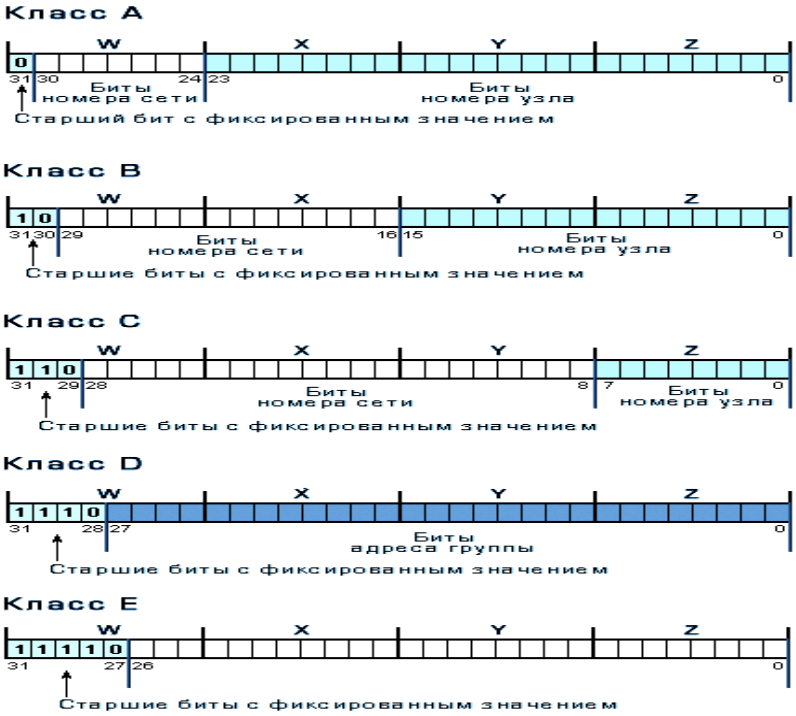


Рис. 105. Классификация IP-адресов

Если адрес начинается последовательностью 1110, то это сеть ***класса D***. Она означает групповой адрес—***Multicast.*** Технология IP Multicast использует адреса с 224.0.0.0 до 239.255.255.255. Поддерживается статическая и динамическая адресация. Примером статических адресов являются 224.0.0.1 — адрес группы, включающей в себя все узлы локальной сети, 224.0.0.2 — все маршрутизаторы локальной сети. Диапазон адресов с 224.0.0.0 по 224.0.0.255 зарезервирован для протоколов маршрутизации и других низкоуровневых протоколов поддержки групповой адресации. Остальные адреса динамически используются приложениями.

Если адрес начинается с 11110, то эта сеть относится к ***классу E***. Адреса этого класса зарезервированы для будущего применения.

Протокол IP предполагает наличие адресов, которые трактуются особым образом. К ним относятся следующие:

1. Адреса, значение первого октета которых равно 127. Пакеты, направленные по такому адресу, реально не передаются в сеть, а обрабатываются программным обеспечением узла-отправителя. Таким образом, узел может направить данные самому себе. Этот подход очень удобен для тестирования сетевого программного обеспечения

в условиях, когда нет возможности подключиться к сети. 127.0.0.1 – этот адрес имеет название ***loopback.***

2. Адрес 255.255.255.255. Пакет, в назначении которого стоит адрес 255.255.255.255, должен рассылаться всем узлам сети, в которой находится источник. Такой вид рассылки называется ограниченным широковещанием. В двоичной форме этот адрес имеет вид 11111111 11111111 11111111 11111111.
3. Адрес 0.0.0.0. Он используется в служебных целях и трактуется как адрес того узла, который сгенерировал пакет. Двоичное представление этого адреса 00000000 00000000 00000000 00000000

Дополнительно особым образом интерпретируются адреса:

- содержащие 0 во всех двоичных разрядах поля номера узла; такие IP-адреса используются для записи адресов сетей в целом;
- содержащие 1 во всех двоичных разрядах поля номера узла; такие IP-адреса являются широковещательными адресами для сетей, номера которых определяются этими адресами.

Таблица 8. Классы сетевых адресов

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.0.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.555.555	Зарезервирован

В локальных сетях, основанных на протоколе IP, могут использоваться специальные адреса, назначенные IANA (стандарты RFC 1918 и RFC 1597):

10.0.0.0—10.255.255.255;

172.16.0.0—172.31.255.255;

192.168.0.0—192.168.255.255.

Такие адреса называют ***локальными или «серыми»,*** эти адреса не маршрутизируются в Интернет. Необходимость использовать такие адреса возникла из-за того, что, когда разрабатывался протокол IP, не предусматривалось столь широкое его распространение, и постепенно адресов стало не хватать. Как вариант был придуман протокол IPv6. В различных непересекающихся LAN ад-

реса могут повторяться, и это не является проблемой, так как доступ в другие сети происходит с применением технологий, подменяющих или скрывающих адрес внутреннего узла сети за её пределами - NAT или proxy дают возможность подключить ЛВС к глобальной сети (WAN). Для обеспечения связи локальных сетей с глобальными применяются маршрутизаторы (в роли шлюзов и межсетевых экранов).

Конфликт адресов - распространённая ситуация в локальной сети, при которой в одной IP подсети оказываются два или более компьютеров с одинаковыми IP адресами. Для предотвращения таких ситуаций и облегчения работы сетевых администраторов применяется протокол DHCP, с помощью которого можно автоматически назначать адреса компьютерам.

NAT (от англ. Network Address Translation - «преобразование сетевых адресов») - это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation

.

Использование масок в IP-адресации.

Маска – четырех байтное число, которое используется в паре с IP адресом, двоичная запись маски содержит единицы в тех разделах, которые должны в IP адресе интерпретироваться как номер сети. Поскольку номер сети является цельной частью адреса, 1 в маске представляют непрерывную последовательность.

Для стандартных классов сетей маски имеют след. значения:
Класс А – 11111111.00000000.00000000.00000000 (255.0.0.0);
Класс В – 11111111.11111111.00000000.00000000 (255.255.0.0);
Класс В – 11111111.11111111.11111111.00000000 (255.255.255.0);

В терминологии сетей TCP/IP маской подсети или маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая— к адресу самого узла в этой сети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0/24 с длиной префикса 24 бита.

Другой вариант определения— это определение подсети IP-адресов. Например, с помощью маски подсети можно сказать, что один диапазон IP-адресов будет в одной подсети, а другой диапазон соответственно в другой подсети.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И). Например, в случае более сложной маски (битовые операции в IPv6 выглядят идентично):

IP-адрес: 11000000 10101000 00000001 00000010 (192.168.1.2)

Маска подсети: 11111111 11111111 11111111 00000000 (255.255.255.0)
Адрес сети: 11000000 10101000 00000001 00000000 (192.168.1.0)

Разбиение одной большой сети на несколько маленьких подсетей позволяет упростить маршрутизацию. Например, пусть таблица маршрутизации некоторого маршрутизатора содержит следующую запись:

Сеть назначения	Маска	Адрес шлюза
192.168.1.0	255.255.255.0	192.168.1.1

Пусть теперь маршрутизатор получает пакет данных с адресом назначения 192.168.1.2. Обрабатывая построчно таблицу маршрутизации, он обнаруживает, что при наложении маски 255.255.255.0 на адрес 192.168.1.2 получается адрес сети 192.168.1.0. В таблице маршрутизации этой сети соответствует шлюз 192.168.1.1, которому и отправляется пакет.

Маски подсети являются основой метода бесклассовой маршрутизации (CIDR). При этом подходе маску подсети записывают вместе с IP-адресом в формате «IP-адрес/количество единичных бит в маске». Число после слэша означает количество единичных разрядов в маске подсети.

Рассмотрим пример записи диапазона IP-адресов в виде 10.96.0.0/11. В этом случае маска подсети будет иметь двоичный вид 11111111 11100000 00000000 00000000, или то же самое в десятичном виде: 255.224.0.0. 11 разрядов IP-адреса отводятся под номер сети, а остальные 32-11 = 21 разряд полного адреса— под локальный адрес в этой сети. Итого, 10.96.0.0/11 означает диапазон адресов от 10.96.0.1 до 10.127.255.254.

Маска назначается по следующей схеме $2^8 - n$ (для сетей класса С), где n— количество компьютеров в подсети + 2, округленное до ближайшей большей степени двойки.(2 добавляется, чтобы учесть IP-адрес сети (первый в диапазоне) и широковещательный (последний в диапазоне, задаваемом маской)

Пример: В некой сети класса С есть 30 компьютеров, маска для такой сети вычисляется следующим образом:

2^8 - 32 = 224 (E0h) < = > 255.255.255.224 (0xFFFFFFE0)

Пользователи обычно предпочитают работать с символьными именами компьютеров, и операционные системы локальных сетей приучили их к этому удобному способу. Следовательно, в сетях TCP/IP должны существовать символьные имена хостов и механизм для установления соответствия между символьными именами и IP-адресами.

Как отмечалось ранее, диапазон IP- адресов в формате IPv4, по оценкам специалистов заканчивается в 2011 году. В конце 1992 года сообщество Интернет для решения проблем адресного пространства и ряда смежных задач разра-

ботало и приняло новый протокол **IPv6** с IP-адресами в 128 бит вместо 32 для IPv4.

IPv6 представляет собой новую версию протокола Интернет [RFC-1883], являющуюся преемницей версии 4 (IPv4; RFC-791). Изменения IPv6 по отношению к IPv4 можно поделить на следующие группы:

- *Расширение адресации*

В IPv6 длина адреса расширена до 128 бит (против 32 в IPv4), что позволяет обеспечить больше уровней иерархии адресации, увеличить число адресуемых узлов, упростить авто-конфигурацию. Для расширения возможности мультикастинг-маршрутизации в адресное поле введено субполе "scope" (группа адресов). Определен новый тип адреса "anycast address" (эникастный), который используется для посылки запросов клиента любой группе серверов. Эникаст адресация предназначена для использования с набором взаимодействующих серверов, чьи адреса не известны клиенту заранее.

- *Спецификация формата заголовков*

Некоторые поля заголовка IPv4 отбрасываются или делаются опционными, уменьшая издержки, связанные с обработкой заголовков пакетов с тем, чтобы уменьшить влияние расширения длины адресов в IPv6.

- Улучшенная поддержка расширений и опций

Изменение кодирования опций IP-заголовков позволяет облегчить переадресацию пакетов, ослабляет ограничения на длину опций, и делает более доступным введение дополнительных опций в будущем.

- *Возможность пометки потоков данных*

Введена возможность помечать пакеты, принадлежащие определенным транспортным потокам, для которых отправитель запросил определенную процедуру обработки, например, нестандартный тип TOS (вид услуг) или обработка данных в реальном масштабе времени.

- *Идентификация и защита частных обменов*

В IPv6 введена спецификация идентификации сетевых объектов или субъектов, для обеспечения целостности данных и при желании защиты частной информации.

Формат и семантика адресов IPv6 описаны в документе RFC-1884. Версия ICMP IPv6 рассмотрена в RFC-1885.

В протоколе IPv6 адреса имеют длину 128 битов (16-байт).

Рекомендованы три формы для текстового представления адресов.

1. **Форма шестнадцатеричных чисел и двоеточий.** Эта форма является предпочтительной и имеет вид n:n:n:n:n:n:n:n.

Каждый знак n соответствует 4-х значному шестнадцатеричному числу (всего 8 шестнадцатеричных чисел, для каждого числа отводится 16 бит).

Например: 3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562.

2. **Сжатая форма.** По причине большой длины адрес обычно содержит много нулей подряд. Для упрощения записи адресов используется сжатая форма, в которой смежные последовательности нулевых блоков заменяются парами символов двоеточий (::).Однако такой символ может встречаться в адресе только один раз.

Например, адрес групповой рассылки FFED:0:0:0:0:BA98:3210:4562 имеет сжатую форму FFED::BA98:3210:4562. Адрес одноадресной рассылки 3FFE:FFFF:0:0:8:800:20C4:0 в сжатой форме имеет вид: 3FFE:FFFF::8:800:20C4:0. Шлейфовый адрес 0:0:0:0:0:0:0:1 в сжатой форме выглядит так ::1. Неопределенный адрес 0:0:0:0:0:0:0:0 превращается в :: .

3. **Смешанная форма.** Эта форма представляет собой сочетание адресов протоколов IPv4 и IPv6. В этом случае адрес имеет формат n:n:n:n:n:n:d.d.d.d, где каждый символ n соответствует 4-х значному шестнадцатеричному числу (6 шестнадцатеричных чисел, для каждого числа отводится 16 бит), а d.d.d.d - часть адреса, записанная в формате IPv4 (32 бита).

IPv6 адреса всех типов ассоциируются с интерфейсами, а не узлами. Так как каждый интерфейс принадлежит только одному узлу, уникастный адрес интерфейса может идентифицировать узел. Одному интерфейсу могут соответствовать много IPv6 адресов различного типа (уникастные, эникастные и мультикстные). Существует два исключения из этого правила:

1. Одиночный адрес может приписываться нескольким физическим интерфейсам, если приложение рассматривает эти несколько интерфейсов как единое целое при представлении его на уровне Интернет.
2. Маршрутизаторы могут иметь ненумерованные интерфейсы (например, интерфейсу не присваивается никакого IPv6 адреса) для соединений точка-точка, чтобы исключить необходимость вручную конфигурировать и объявлять (афишировать) эти адреса. Адреса не нужны для соединений точка-точка маршрутизаторов, если эти интерфейсы не используются в качестве точки отправления или назначения при посылке IPv6 дейтограмм. Маршрутизация здесь осуществляется по схеме близкой к используемой протоколом CIDR в IPv4.

IPv6 соответствует модели IPv4, где субсеть ассоциируется с каналом. Одному каналу могут соответствовать несколько субсетей.

Протокол IPv6 определяет следующие типы адресов.

1. **Адрес одноадресной рассылки (unicast).** Идентификатор в адресе определяет один интерфейс. Пакет, посланный на этот адрес, доставляется по указанному адресу. Адреса одноадресной рассылки отличаются от адресов групповой рассылки значением старшего октета. Старший октет адресов групповой рассылки имеет шестнадцатеричное значение FF. Все остальные значения этого октета определяют адрес одноадресной рассылки.

Рассмотрим различные типы адресов одноадресной рассылки.
Адреса локальной связи. Эти адреса используются для одной линии связи и имеют формат: FE80::InterfaceID, (Рис.

n бит	80-n бит	48 бит
Префикс подписчика	ID-субсети	Интерфейс ID

В этом случае 48-битовый идентификатор интерфейса представляет собой IEEE-802 MAC адрес. Использование IEEE 802 mac адресов в качестве идентификаторов интерфейсов будет стандартным в среде, где узлы имеют IEEE 802 MAC адреса. В других средах, где IEEE 802 MAC адреса не доступны, могут использоваться другие типы адресов связного уровня, такие как E.164 адреса, в качестве идентификаторов интерфейсов.

Включение уникального глобального идентификатора интерфейса, такого как IEEE MAC адрес, делает возможным очень простую форму автоконфигурации адресов. Узел может узнать идентификатор субсети, получая информацию от маршрутизатора в виде сообщений оповещения, которые маршрутизатор посылает связанным с ним партнерам, и затем сформировать IPv6 адрес для себя, используя IEEE MAC адрес в качестве идентификатора интерфейса для данной субсети.

Кроме того, существуют ещё два типа уникастных адресов локального использования. Различаются локальные адреса сети и канала. Локальный адрес канала предназначен для работы с одним каналом, а локальный адрес сети - с одной локальной сетью (site). Локальный IPv6 уникаст-адрес канала имеет формат, отображенный ниже на рис.:

10 бит	n бит	118-n бит
1111111010	0	ID интерфейса

Рис. Локальный адрес канала

Локальные адреса канала предназначены для обращения через определенный канал, например, для целей авто-конфигурации адресов, поиска соседей или в случае отсутствия маршрутизатора. Локальный адрес сети имеет формат, показанный на рис.:

Рис.. Локальный адрес сети

Локальные адреса сети могут использоваться для локальных сетей или организаций, которые (пока еще) не подключены к глобальному Интернет. Им не нужно запрашивать или “присваивать” префикс адреса из глобального адресного пространства Интернет. Вместо этого можно использовать локальный адрес сети IPv6. Когда организация соединяется с глобальным Интернет, она может сформировать глобальные адреса путем замещения локального префикса сети префиксом подписчика.

Маршрутизаторы не должны переадресовывать пакеты с локальными адресами сети отправителя.

Адреса локальных веб-узлов. Эти адреса используются на одном веб-узле и имеют следующий формат: FEC0::SubnetID:InterfaceID.

Адреса локальных веб-узлов используются для адресации внутри узла и не требуют глобального префикса, идентификатор субсети делится на идентификатор области и идентификатор субсети. Формат такого адреса имеет вид:

Рис.

Эта схема может быть развита с тем, чтобы позволить локальной сети или организации добавлять новые уровни внутренней иерархии. Возможно, предпочтительно использовать идентификатор интерфейса меньше чем 48-разрядный IEEE 802 MAC адрес, с тем, чтобы оставить больше места для полей, характеризующих уровни иерархии. Это могут быть идентификаторы интерфейсов, сформированные администрацией локальной сети или организации.

Глобальные адреса одноадресной рассылки протокола IPv6. Эти адреса могут использоваться для связи через Интернет и имеют следующий формат: 010 (FP, 3 бита) TLA ID (13 битов) Резерв (8 битов) NLA ID (24 бита) SLA ID (16 битов) InterfaceID (64 бита).

Глобальный IPv6 уникаст-адрес имеет формат, отображенный ниже на рис.:

Рис. Глобальный адрес провайдера

Старшая часть адреса предназначена для определения того, кто определяет часть адреса провайдера, подписчика и т.д.

Идентификатор регистрации определяет регистратора, который задает провайдерскую часть адреса. Термин "префикс регистрации" относится к старшей части адреса, включая поле идентификатор регистрации (ID).

Идентификатор провайдера задает специфического провайдера, который определяет часть адреса подписчика. Термин "префикс провайдера" относится к старшей части адреса включая идентификатора провайдера.

Идентификатор подписчика позволяет разделить подписчиков, подключенных к одному и тому же провайдеру. Термин "префикс подписчика" относится к старшей части адреса, включая идентификатор подписчика.

Часть адреса интра-подписчик определяется подписчиком и организована согласно местной топологии Интернет подписчика. Возможно, что несколько подписчиков пожелают использовать область адреса интра-подписчик для одной и той же субсети и интерфейса. В этом случае идентификатор субсети определяет специфический физический канал, а идентификатор интерфейса - определенный интерфейс субсети.

2. **Адрес групповой рассылки (multicast).** Идентификатор в адресе определяет набор интерфейсов (обычно принадлежащих различным узлам). Пакет, посланный на такой адрес, доставляется всем интерфейсам, идентифицирующимся этим адресом. Типы групповых адресов замещают широковещательные адреса протокола IPv4. Мультикастинг-адрес IPv6 является идентификатором для группы узлов. Узел может принадлежать к любому числу мультикастинг групп. Мультикастинг-адреса имеют следующий формат (рис.):

Рис.

11111111 в начале адреса идентифицирует адрес, как мультикатинг-адрес.

Рис.

Старшие 3 флага зарезервированы и должны быть обнулены.

t = 0 указывает на то, что адрес является стандартным ("well-known") мультикастным, официально выделенным для глобального использования в Интернет.

T = 1 указывает, что данный мультикастинг-адрес присвоен временно ("transient").

Поле scope представляет собой 4-битовый код мультикастинга, предназначенный для определения предельной области действия мультикастинг-группы.

Допустимые значения:

- 0 зарезервировано
- 1 Область действия ограничена локальным узлом
- 2 Область действия ограничена локальным каналом
- 3 (не определено)
- 4 (не определено)
- 5 Область действия ограничена локальной сетью
- 6 (не определено)
- 7 (не определено)
- 8 Область действия ограничена локальной организацией
- 9 (не определено)
- A (не определено)
- B (не определено)
- C (не определено)
- D (не определено)
- E глобальные пределы (global scope)
- F зарезервировано

Идентификатор группы идентифицирует мультикастинг-группы, постоянной или переходной (transient), в пределах заданных ограничений (scope). Значение постоянно присвоенного мультикастинг-адреса не зависит от значения поля scope. Например, если "NTP servers group" присвоен постоянный мультикастинг адрес с идентификатором группы 43 (hex), тогда:

- FF01:0:0:0:0:0:0:43 означает, что все ntp серверы одного и того же узла рассматриваются как отправители.
- FF02:0:0:0:0:0:0:43 означает, что все NTP серверы работают с тем же каналом, что и отправитель.

- FF05:0:0:0:0:0:0:43 означает, что все NTP серверы принадлежат той же сети, что и отправитель.
- FF0E:0:0:0:0:0:0:43 означает, что все NTP серверы находятся в Интернет.

Непостоянно выделенные мультикаст-адреса имеют значение только в пределах данного ограничения (scope). Например, группа, определенная непостоянным локальным мультикаст-адресом FF15:0:0:0:0:0:0:43, не имеет никакого смысла для другой локальной сети или непостоянной группы, использующей тот же групповой идентификатор с другим scope, или для постоянной группы с тем же групповым ID.

Мультикастинг адреса не должны использоваться в качестве адреса отправителя в IPv6 дейтограммах или встречаться в любых заголовках маршрутизации.

3. **Адрес для всех типов рассылок (anycast)**. Идентификатор в адресе определяет набор интерфейсов (обычно принадлежащих различным узлам). Пакет, посланный на такой адрес, доставляется только одному интерфейсу из идентифицирующихся данным адресом. Этот интерфейс является ближайшим из идентифицируемых метрикой маршрутизации.

Эникастные адреса выделяются из уникастного адресного пространства, и используют один из известных уникастных форматов. Таким образом эникастные адреса синтаксически неотличимы от уникастных адресов. Когда уникастный адрес приписан более чем одному интерфейсу, он превращается в эникастный адрес и узлы, которым он приписан, должны быть сконфигурированы так, чтобы распознавать этот адрес.

Одним из применений эникастных адресов является идентификация набора маршрутизаторов, принадлежащих Интернет сервис провайдеру. Такие адреса в маршрутном заголовке IPv6 могут использоваться в качестве промежуточных, чтобы обеспечить доставку пакета через определенного провайдера или последовательность провайдеров.

Другим возможным приложением таких адресов может стать идентификация набора маршрутизаторов, связанных с определенной субсетью, или набора маршрутизаторов, обеспечивающих доступ в определенный домен.

Имеются следующие ограничения при использовании эникастных IPv6 адресов:

- Эникастный адрес не может использоваться в качестве адреса отправителя в ipv6 пакете.

- Эникастный адрес не может быть приписан персональному компьютеру или устройству в локальной сети IPv6, таким образом, он может принадлежать только маршрутизатору.

Как правило, узел всегда имеет адрес локальной связи. Также у него могут быть адрес локального веб-узла и один или несколько глобальных адресов.

Конкретный тип адреса протокола IPv6 определяют его начальные биты. Поле, содержащее эти биты, называется префиксом формата (FP) или адресным префиксом и имеет переменную длину.

Адрес одноадресной рассылки в протоколе IPv6 разделяется на две части. Первая часть содержит адресный префикс, а вторая – идентификатор интерфейса.

Краткий способ представления адреса выглядит следующим образом:

ipv6-адрес/длина префикса.

Пример адреса с 64-битным префиксом.
3FFF:FFFF:0:CD30:0:0:0:0/64 .
Префиксом в этом примере является 3FFE:FFFF:0:CD30.

В IPv6 отсутствует такое понятия, как маска подсети. IPv6-адрес делится на три части:

- Глобальный префикс (Global Routing Prefix) – аналогичен идентификатору сети (Network ID) в IPv4 и присваивается провайдерам. Определяется он тремя первыми блоками.
- Идентификатор подсети (Subnet ID) – представлен четвертым блоком и, по сути, очень похож на идентификатор подсети (Subnet ID) в IPv4.
- Идентификатор интерфейса (Interface ID) – аналог Host ID в IPv4, определяет уникальный адрес хоста вашей сети.

Существует несколько способов получения уникального 64-битного идентификатора интерфейса: он может быть настроен вручную, определен DCHP-сервером или получен путем преобразования MAC-адреса сетевой карты. Вместо маски в IPv6 указывается префикс – это количество бит, которые определяют часть блоков, отвечающих за Global Routing Prefix. Пишется префикс через косую черту после самого адреса.

Возьмем для примера IPv6-адрес:
2001:0f68:0000:0000:0000:0000:1986:69af/48. Поскольку префикс (/48) указывает на первые 48 бит, можно сделать вид, что 2001:0f68:0000 будет являться ча-

стью Global Routing Prefix. Следующее поле, 0000, указывает на идентификатор подсети. Оставшиеся блоки 0000:0000:1986:69af – это идентификатор интерфейса.

В IPv6, опционная информация уровня Интернет записывается в отдельных заголовках, которые могут быть помещены между IPv6 заголовком и заголовком верхнего уровня пакета. Существует небольшое число таких заголовков, каждый задается определенным значением кода поля *следующий заголовок*. В настоящее время определены заголовки: маршрутизации, фрагментации, аутентификации, инкапсуляции, опций hop-by-hop, места назначения и отсутствия следующего заголовка. IPv6 пакет может нести один, или более заголовков расширения, а может и не иметь заголовка расширения, каждый задается предыдущим полем *следующий заголовок* (рис.):

Рис. . Структура вложения пакетов для IPv6

Заголовки расширения не рассматриваются и не обрабатываются узлами по пути доставки. Содержимое и семантика каждого заголовка расширения определяет, следует или нет обрабатывать *следующий заголовок*. Следовательно, заголовки расширения должны обрабатываться строго в порядке их выкладки в пакете. Получатель, например, не должен просматривать пакет, искать определенный тип заголовка расширения и обрабатывать его до обработки предыдущих заголовков.

Единственное исключение из этого правила касается заголовка опций hop-by-hop, несущего в себе информацию, которая должна быть рассмотрена и обработана каждым узлом по пути доставки, включая отправителя и получателя. Заголовок опций hop-by-hop, если он присутствует, должен следовать непосредственно сразу после IPv6-заголовка. Его присутствие отмечается записью нуля в поле *следующий заголовок* заголовка IPv6.

Если в результате обработки заголовка узлу необходимо перейти к следующему заголовку, а код поля *следующий заголовок* не распознается, необходимо игнорировать данный пакет и послать соответствующее сообщение ICMP (parameter problem message) отправителю пакета. Это сообщение должно со-

держать код ICMP = 2 ("unrecognized next header type encountered " - встретился нераспознаваемый тип *следующего заголовка*) и поле - указатель на не узнанное поле в пакете. Аналогичные действия следует предпринять, если узел встретил код следующего заголовка равный нулю в заголовке, отличном от IPv6-заголовка.

Каждый заголовок расширения имеет длину кратную 8 октетам. Многооктетные поля в заголовке расширения выравниваются в соответствии с их естественными границами, т.е., поля с шириной в n октетов помещаются в n октетов, начиная с начала заголовка, для n = 1, 2, 4 или 8.

IPv6 включает в себя следующие заголовки расширения:

- Опции hop-by-hop;
- Маршрутизация (routing;тип 0);
- Фрагмент;
- Опции места назначения ;
- Проверка прав доступа (authentication); [RFC-1826 и RFC-1827.]
- Поле безопасных вложений (encapsulating security payload), [RFC-1826 и RFC-1827.]

Адресное пространство IPv6 будет распределяться IANA(Internet Assigned Numbers Authority - комиссия по стандартным числам в Интернет [RFC-1881]). В качестве советников будут выступать IAB (internet architecture board - совет по архитектуре Интернет) и IESG (Internet Engineering Steering Group - инженерная группа управления Интернет). Внедрение этого нового протокола представляет отдельную серьезную проблему, так как этот процесс не предполагает замены всего программного обеспечения во всем мире одновременно.

1.20. Коммутаторы локальных сетей

Как отмечалось ранее, изначально коммутатор представлял собой многопортовый мост и также функционировал на канальном уровне модели OSI. Основное отличие коммутатора от моста заключалось в том, что он мог устанавливать одновременно несколько соединений между разными парами портов. При передаче пакета через коммутатор в нем создавался отдельный виртуальный (либо реальный, в зависимости от архитектуры) канал, по которому данные пересылались «напрямую» от порта-источника к порту-получателю с максимально возможной для используемой технологии скоростью. Такой принцип работы получил название микросегментация. Благодаря микросегментации, коммутаторы получили возможность функционировать в режиме полного дуп-

лекса (full duplex), что позволяло каждой рабочей станции одновременно передавать и принимать данные, используя всю полосу пропускания в обоих направлениях. Станции не приходилось конкурировать за полосу пропускания с другими устройствами, в результате чего не происходили коллизии, и повышалась производительность сети.

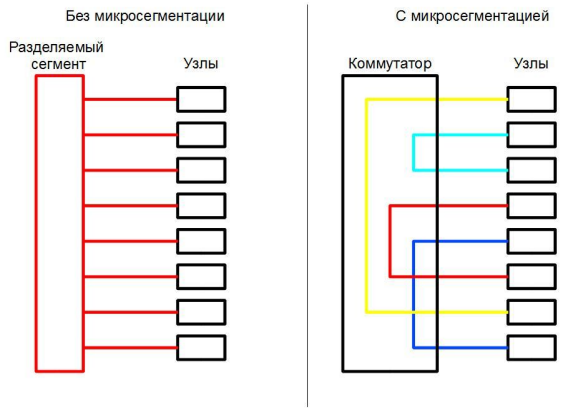


Рис. 106. Микросегментация.

В настоящее время коммутаторы являются основным строительным блоком для создания локальных сетей. Современные коммутаторы Ethernet превратились в интеллектуальные устройства со специализированными процессорами для обработки и перенаправления пакетов на высоких скоростях и реализации таких функций, как организация резервирования и повышения отказоустойчивости сети, агрегирование каналов, создание виртуальных локальных сетей (VLAN), маршрутизация, управление качеством обслуживания (Quality of Service, QoS), обеспечение безопасности и многих других. Также усовершенствовались функции управления коммутаторов, благодаря чему системные администраторы получили удобные средства настройки сетевых параметров, мониторинга и анализа трафика.

С появлением стандарта IEEE 802.3af-2003 PoE, описывающего технологию передачи питания по Ethernet (Power over Ethernet, PoE), разработчики начали встраивать его поддержку в коммутаторы, что позволило использовать их в качестве питающих устройств для IP-телефонов, Интернет-камер, беспроводных точек доступа и другого оборудования.

С ростом популярности технологий беспроводного доступа в корпоративных сетях производители оборудования выпустили на рынок унифицированные коммутаторы с поддержкой технологии PoE для питания подключаемых к их портам точек беспроводного доступа и централизованного управления как проводной, так и беспроводной сетью.

Повышение потребностей заказчиков и тенденции рынка стимулируют разработчиков коммутаторов более или менее регулярно расширять аппаратные

и функциональные возможности производимых устройств, позволяющие развертывать в локальных сетях новые услуги, повышать их надежность, управляемость и защищенность.

Коммутаторы локальной сети можно классифицировать по возможности управления. Существует три следующих категории, на которые можно разбить коммутаторы:

- Неуправляемые коммутаторы;
- Управляемые коммутаторы;
- Настраиваемые коммутаторы.

Неуправляемые коммутаторы не поддерживают возможности управления и обновления программного обеспечения.

Управляемые коммутаторы являются сложными устройствами, позволяющими выполнять расширенный набор функций 2 и 3 уровня модели OSI. Управление коммутаторами может осуществляться посредством Web-интерфейса, командной строки (CLI), протокола SNMP, Telnet и т.д.

Настраиваемые коммутаторы занимают промежуточную позицию между ними. Они предоставляют пользователям возможность настраивать определенные параметры сети с помощью интуитивно понятных средств управления, например Web-интерфейса.

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, поскольку пакет данных не претерпевает изменений. 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. Такие коммутаторы динамически решают, коммутировать (уровень 2) или маршрутизировать (уровень 3) входящий трафик. Коммутаторы 3-го уровня выполняет коммутацию в пределах рабочей группы и маршрутизацию между различными подсетями или виртуальными локальными сетями (VLAN).

Коммутаторы 3-го уровня функционально практически ничем не отличаются от традиционных маршрутизаторов и выполняют те же функции:

- определение оптимальных путей передачи данных на основе логических адресов (адресов сетевого уровня, традиционно IP-адресов);
- управление широковещательным и многоадресным трафиком;
- фильтрация трафика на основе информации 3-го уровня;
- IP- фрагментация.

Основное отличие между маршрутизаторами и коммутаторами 3-го уровня заключается в том, что в маршрутизаторах принятие решения о пересылке пакетов обычно выполняется программным образом, а в коммутаторах обрабатывается специализированными контроллерами ASIC. Это позволяет коммутаторам выполнять маршрутизацию пакетов на скорости канала связи.

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*).

Изначально таблица коммутации пуста. При включении питания, одновременно с передачей данных, коммутатор начинает изучать расположение подключенных к нему сетевых устройств путем анализа MAC-адресов источников получаемых кадров. Например, если на порт 1 коммутатора, показанного на рисунке 3, 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*. Это означает, что, как только 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 *временной штамп* (*aging*). Временной штамп позволяет коммутатору автоматически реагировать на перемещение, добавление или удаление сетевых устройств. Каждый раз, когда идет обращение по какому-либо MAC-адресу, соответствующая запись получает новый временной штамп. Записи, по которым не обращались долгое время, из таблицы удаляются. Это позволяет хранить записи в таблице коммутации в течение определенного времени и гарантирует, что она не будет использовать слишком много системной памяти.

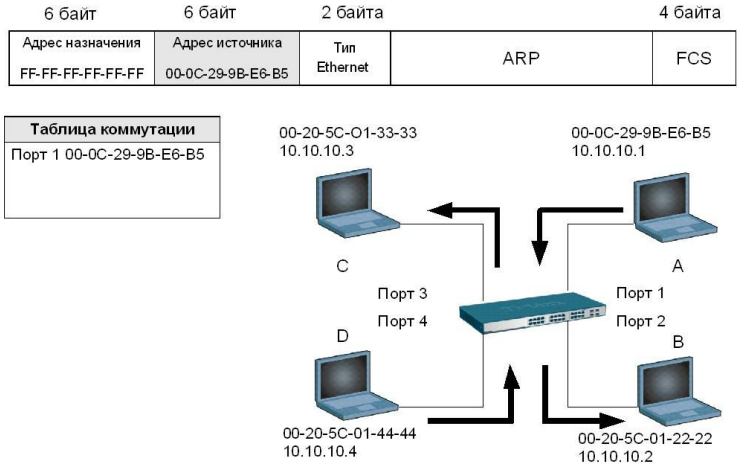


Рис. 107. Построение таблицы коммутации.

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 присваивается временной штамп, поэтому время их жизни не ограничено. При создании статической таблицы коммутации администратору сети необходимо отключить автоизучение MAC-адресов на портах коммутатора.

Статическую таблицу коммутации удобно использовать с целью повышения сетевой безопасности, когда необходимо гарантировать, что только устройства с определенными MAC- адресами могут подключаться к сети.

Внимание: как правило, размер статической таблицы коммутации меньше размера динамической таблицы коммутации. Размеры обоих таблиц также зависят от модели коммутатора. Обычно производители указывают размеры таблиц коммутации в спецификациях на устройства.

Как только в таблице коммутации появляется хотя бы одна запись, коммутатор начинает использовать ее для пересылки кадров. Рассмотрим пример, показанный на рисунке 107, описывающий процесс пересылки кадров между портами коммутатора.

Когда коммутатор получает кадр, отправленный компьютером А компьютеру В, он извлекает из него MAC-адрес приемника и ищет этот MAC-адрес в своей таблице коммутации. Как только в таблице коммутации будет найдена запись, ассоциирующая MAC-адрес приемника (компьютера В) с одним из портов коммутатора, за исключением порта-источника, кадр будет передан через соответствующий выходной порт (в приведенном примере - порт 2). Этот процесс называется *продвижение (forwarding)* кадра.

Если бы оказалось, что выходной порт и порт-источник совпадают, то передаваемый кадр был бы коммутатором отброшен. Этот процесс называется *фильтрацией (filtering)*.

В том случае, если MAC-адрес приемника 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 маршрутизацией (flooding)*. Несмотря на то, что процесс лавинной маршрутизации занимает полосу пропускания, он позволяет коммутатору избежать потери кадров, когда MAC-адрес приемника неизвестен, и осуществлять процесс самообучения.

Помимо лавинной маршрутизации одноадресных кадров, коммутаторы также выполняют лавинную маршрутизацию многоадресных и широковещательных кадров, которые генерируют сетевые мультимедийные приложения.

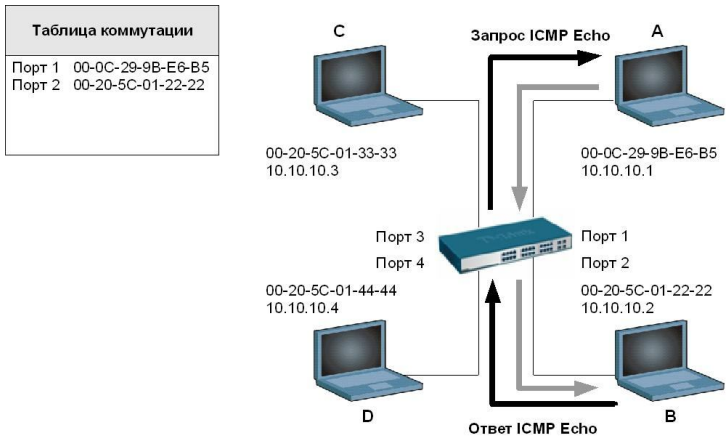


Рис. 108. Передача кадра с порта на порт коммутатора.

Более подробно изучить функциональные возможности коммутаторов и применяемые в коммутируемых сетях технологии, можно ознакомившись с учебным курсом компании D-Link «Коммутаторы локальных сетей D-Link. Базовый курс».

1.21. Протоколы сетевого уровня

Протоколы сетевого уровня - предназначается для определения пути передачи данных. Отвечают за трансляцию логических адресов и имён в физические, определение кратчайших маршрутов, коммутацию и маршрутизацию, отслеживание неполадок и заторов в сети. На этом уровне работает такое сетевое устройство, как маршрутизатор.

На сетевом уровне определяются два вида протоколов. Первый вид - сетевые протоколы - реализуют продвижение пакетов через сеть. Именно эти протоколы обычно имеют в виду, когда говорят о протоколах сетевого уровня. Од-

нако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто протоколами маршрутизации. С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

На сетевом уровне работают протоколы еще одного типа, которые отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Такие протоколы часто называют протоколами разрешения адресов - Address Resolution Protocol, ARP. Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути. Примером протоколов сетевого уровня являются протокол межсетевого взаимодействия IP стека TCP/IP.

Устройства сетевого уровня

Маршрутизаторы

Основная задача маршрутизатора - выбор наилучшего маршрута в сети - часто является достаточно сложной с математической точки зрения. Особенно интенсивных вычислений требуют протоколы, основанные на алгоритме состояния связей, вычисляющие оптимальный путь - OSPF, BGP. Кроме этой основной функции в круг ответственности маршрутизатора входят и другие задачи, такие как буферизация, фильтрация и фрагментация перемещаемых пакетов. При этом очень важна производительность, с которой маршрутизатор выполняет эти задачи.

Поэтому типичный маршрутизатор является мощным вычислительным устройством с одним или даже несколькими процессорами, часто специализированными или построенными на RISC-архитектуре, со сложным программным обеспечением. То есть сегодняшний маршрутизатор - это специализированный компьютер, имеющий скоростную внутреннюю шину или шины (с пропускной способностью 600-2000 Мбит/с), часто использующий симметричное или асимметричное мультипроцессирование и работающий под управлением специализированной операционной системы, относящейся к классу систем реального времени. Многие разработчики маршрутизаторов построили в свое время такие операционные системы на базе операционной системы Unix, естественно, значительно ее переработав.

Маршрутизаторы могут поддерживать как один протокол сетевого уровня (например, IP, IPX или DECnet), так и множество таких протоколов. В последнем случае они называются ***многопротокольными маршрутизаторами***. Чем больше протоколов сетевого уровня поддерживает маршрутизатор, тем лучше он подходит для корпоративной сети.

Большая вычислительная мощность позволяет маршрутизаторам наряду с основной работой по выбору оптимального маршрута выполнять и ряд вспомогательных высокоуровневых функций.

Классификация маршрутизаторов по областям применения

По областям применения маршрутизаторы делятся на несколько классов.

Магистральные маршрутизаторы (backbone routers) - предназначены для построения центральной сети корпорации. Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем.

Магистральные маршрутизаторы - это наиболее мощные устройства, способные обрабатывать несколько сотен тысяч или даже несколько миллионов пакетов в секунду, имеющие большое количество интерфейсов локальных и глобальных сетей. Чаще всего магистральный маршрутизатор конструктивно выполнен по модульной схеме на основе шасси с большим количеством слотов - до 10 (например, ***DES-7210***). Большое внимание уделяется в магистральных моделях надежности и отказоустойчивости маршрутизатора, которая достигается за счет системы терморегуляции, избыточных источников питания, заменяемых «на ходу» (hot swap) модулей, а также симметричного мультипроцессирования.

Маршрутизаторы региональных отделений - соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, так же как и центральная сеть, может состоять из нескольких локальных сетей. Такой маршрутизатор обычно представляет собой некоторую упрощенную версию магистрального маршрутизатора. Возможен также конструктив с фиксированным количеством портов. Поддерживаемые интерфейсы локальных и глобальных сетей менее скоростные. Примерами маршрутизаторов региональных отделений могут служить модульные коммутаторы ***DES-7200*** и коммутаторы серии ***DGS-3610***. Это наиболее обширный класс выпускаемых коммутаторов, характеристики которых могут приближаться к характеристикам магистральных маршрутизаторов, а могут и опускаться до характеристик маршрутизаторов удаленных офисов.

Маршрутизаторы удаленных офисов - соединяют, как правило, единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения по глобальной связи. Такие маршрутизаторы могут поддерживать и два интерфейса локальных сетей. Маршрутизатор удаленного офиса может поддерживать работу по коммутируемой телефонной линии в качестве резервной связи для выделенного канала (пример ***DI-804HV***). Существует очень большое количество типов маршрутизаторов удаленных офисов. Это объясняется как массовостью потенциальных потребителей, так и специализацией такого типа устройств, проявляющейся в поддержке одного конкретного типа глобальной связи. Например, существуют маршрутизаторы, работающие

только по сети ISDN, существуют модели только для аналоговых выделенных линий и т. п.

Примерами маршрутизаторов удалённых офисов могут служить ***DFL-800, DIR-100, DIR-300, DIR-320, DIR-628, DIR-685.***

Маршрутизаторы локальных сетей (коммутаторы 3-го уровня) - предназначены для разделения крупных локальных сетей на подсети. Основное требование, предъявляемое к ним, - высокая скорость маршрутизации. Все порты имеют скорость по крайней мере 10 Мбит/с, а многие работают на скорости 100 Мбит/с и выше, поэтому всю обработку трафика можно осуществлять аппаратно и с высокой скоростью. Примерами коммутаторов 3-го уровня служат коммутаторы ***DES-3828, DES-3852, DGS-3610-26, DGS-3612, DGS-3650, DES-7206.***

В зависимости от области применения, маршрутизаторы обладают различными основными и дополнительными техническими характеристиками.

Основные технические характеристики маршрутизатора

Основные технические характеристики маршрутизатора связаны с тем, как он решает свою главную задачу - маршрутизацию пакетов в составной сети. Именно эти характеристики прежде всего определяют возможности и сферу применения того или иного маршрутизатора.

Перечень поддерживаемых сетевых протоколов. Магистральный маршрутизатор должен поддерживать большое количество сетевых протоколов и протоколов маршрутизации, чтобы обеспечивать трафик всех существующих на предприятии вычислительных систем (в том числе и устаревших, но все еще успешно эксплуатирующихся, так называемых унаследованных - legacy), а также систем, которые могут появиться на предприятии в ближайшем будущем. Программное обеспечение магистральных маршрутизаторов обычно строится по модульному принципу, поэтому при возникновении потребности можно докупать и добавлять программные модули, реализующие недостающие протоколы.

Перечень поддерживаемых сетевых протоколов обычно включает протоколы IP, Frame Relay, ATM и Ethernet, MPLS.

Протокол маршрутизации — сетевой протокол, используемый маршрутизаторами для определения возможных маршрутов следования данных в составной компьютерной сети. Применение протокола маршрутизации позволяет избежать ручного ввода всех допустимых маршрутов, что, в свою очередь, снижает количество ошибок, обеспечивает согласованность действий всех маршрутизаторов в сети и облегчает труд администраторов.

Протоколы маршрутизации делятся на два вида, зависящие от типов алгоритмов, на которых они основаны:

- Дистанционно-векторные протоколы, основаны на Distance Vector Algorithm (DVA);
- Протоколы состояния каналов связи, основаны на Link State Algorithm (LSA).

Так же протоколы маршрутизации делятся на два вида в зависимости от сферы применения:

- Междоменной маршрутизации;
- Внутридоменной маршрутизации.

Перечень протоколов маршрутизации составляют протоколы RIP v1/v2, RIPng (IPv6),OSPF, BGP v4 (IPv6),

Перечень поддерживаемых интерфейсов локальных и глобальных сетей. Для локальных сетей - это интерфейсы, реализующие физические и канальные протоколы сетей Ethernet, Fast Ethernet, Gigabit Ethernet,10 Gigabit Ethernet.

Для глобальных связей - это интерфейсы физического уровня для связи с аппаратурой передачи данных, а также протоколы канального и сетевого уровней, необходимые для подключения к глобальным сетям с коммутацией каналов и пакетов.

Общая производительность маршрутизатора. Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как Frame Relay, Т3/Е3, SDH, ATM и MPLS. Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Общая производительность маршрутизаторов колеблется от нескольких десятков тысяч пакетов в секунду до нескольких миллионов пакетов в секунду. Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства - несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления таблицы маршрутизации, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

Дополнительные функциональные возможности маршрутизаторов

Наряду с функцией маршрутизации многие устройства обладают следующими важными дополнительными функциональными возможностями, которые значительно расширяют сферу применения этих устройств.

Поддержка одновременно нескольких протоколов маршрутизации. В протоколах маршрутизации обычно предполагается, что маршрутизатор строит свою таблицу на основе работы только этого одного протокола. Деление Internet на автономные системы также направлено на исключение использования в одной автономной системе нескольких протоколов маршрутизации. Тем не менее иногда в большой корпоративной сети приходится поддерживать одновременно несколько таких протоколов, чаще всего это складывается исторически. При этом таблица маршрутизации может получаться противоречивой -

разные протоколы маршрутизации могут выбрать разные следующие маршрутизаторы для какой-либо сети назначения. Большинство маршрутизаторов решает эту проблему за счет придания приоритетов решениям разных протоколов маршрутизации. Высший приоритет отдается статическим маршрутам (администратор всегда прав), следующий приоритет имеют маршруты, выбранные протоколами состояния связей, такими как OSPF, а низшим приоритетов обладают маршруты дистанционно-векторных протоколов, как самых несовершенных.

Приоритеты сетевых протоколов. Можно установить приоритет одного протокола сетевого уровня над другими. На выбор маршрутов эти приоритеты не оказывают никакого влияния, они влияют только на порядок, в котором многопротокольный маршрутизатор обслуживает пакеты разных сетевых протоколов. Это свойство бывает полезно в случае недостаточной полосы пропускания кабельной системы и существования трафика, чувствительного к временным задержкам, например голосового трафика, передаваемого одним из сетевых протоколов.

Поддержка политики маршрутных объявлений. В большинстве протоколов обмена маршрутной информации (например, RIP, OSPF) предполагается, что маршрутизатор объявляет в своих сообщениях обо всех сетях, которые ему известны. Аналогично предполагается, что маршрутизатор при построении своей таблицы учитывает все адреса сетей, которые поступают ему от других маршрутизаторов сети. Однако существуют ситуации, когда администратор хотел бы скрыть существование некоторых сетей в определенной части своей сети от других администраторов, например, по соображениям безопасности. Или же администратор хотел бы запретить некоторые маршруты, которые могли бы существовать в сети. При статическом построении таблиц маршрутизации решение таких проблем не составляет труда. Динамические же протоколы маршрутизации не позволяют стандартным способом реализовывать подобные ограничения. Существует только один широко используемый протокол динамической маршрутизации, в котором описана возможность существования правил, ограничивающих распространение некоторых адресов в объявлениях, - это протокол BGP. Необходимость поддержки таких правил в протоколе BGP понятна, так как это протокол обмена маршрутной информацией между автономными системами, где велика потребность в административном регулировании маршрутов (например, некоторый поставщик услуг Internet может не захотеть, чтобы через него транзитом проходил трафик другого поставщика услуг). Разработчики маршрутизаторов исправляют этот недостаток стандартов протоколов, вводя в маршрутизаторы поддержку правил передачи и использования маршрутной информации, подобных тем, которые рекомендует BGP.

Защита от широковещательных штормов (broadcast storm). Одна из характерных неисправностей сетевого программного обеспечения - самопроизвольная генерация с высокой интенсивностью широковещательных пакетов. Широковещательным штормом считается ситуация, в которой процент широковещательных пакетов превышает 20 % от общего количества пакетов в сети. Обычный коммутатор или мост слепо передает такие пакеты на все свои порты,

как того требует его логика работы, засоряя, таким образом, сеть. Борьба с широковещательным штормом в сети, соединенной коммутаторами, требует от администратора отключения портов, генерирующих широковещательные пакеты. Маршрутизатор не распространяет такие пакеты во все объединяемые им сети.

Поддержка не маршрутизируемых протоколов, таких как NetBIOS, NetBEUI или DEC LAT, которые не оперируют с таким понятием, как сеть. Маршрутизаторы могут обрабатывать пакеты таких протоколов двумя способами.

В первом случае они могут работать с пакетами этих протоколов как мосты, то есть передавать их на основании изучения MAC - адресов. Маршрутизатор необходимо сконфигурировать особым способом, чтобы по отношению к некоторым не маршрутизируемым протоколам на некоторых портах он выполнял функции моста, а по отношению к маршрутизируемым протоколам - функции маршрутизатора. Такой мост/маршрутизатор иногда называют brouter (bridge плюс router).

Другим способом передачи пакетов не маршрутизируемых протоколов является *инкапсуляция* этих пакетов в пакеты какого-либо сетевого протокола. Некоторые производители маршрутизаторов разработали собственные протоколы, специально предназначенные для инкапсуляции не маршрутизируемых пакетов. Кроме того, существуют стандарты для инкапсуляции некоторых протоколов в другие, в основном в IP. Примером такого стандарта является протокол DLSw, определяющий методы инкапсуляции пакетов SDLC и NetBIOS в IP-пакеты, а также протоколы PPTP и L2TP, инкапсулирующие кадры протокола PPP в IP-пакеты.

Разделение функций построения и использования таблицы маршрутизации. Основная вычислительная работа проводится маршрутизатором при составлении таблицы маршрутизации с маршрутами ко всем известным ему сетям. Эта работа состоит в обмене пакетами протоколов маршрутизации, такими как RIP или OSPF, и вычислении оптимального пути к каждой целевой сети по некоторому критерию. Для вычисления оптимального пути на графе, как того требуют протоколы состояния связей, необходимы значительные вычислительные мощности. После того как таблица маршрутизации составлена, функция продвижения пакетов происходит весьма просто - осуществляется просмотр таблицы и поиск совпадения полученного адреса с адресом целевой сети. Если совпадение есть, то пакет передается на соответствующий порт маршрутизатора. Некоторые маршрутизаторы поддерживают только функции продвижения пакетов по готовой таблице маршрутизации. Такие маршрутизаторы являются усеченными маршрутизаторами, так как для их полноценной работы требуется наличие полнофункционального маршрутизатора, у которого можно взять готовую таблицу маршрутизации. Этот маршрутизатор часто называется сервером маршрутов. Отказ от самостоятельного выполнения функций построения таблицы маршрутизации резко удешевляет маршрутизатор и повышает его производительность.

PPP (англ. Point-to-Point Protocol) — протокол точка-точка канального уровня (Data Link) сетевой модели OSI. Обычно используется для установления прямой связи между двумя узлами сети, причем он может обеспечить аутентификацию соединения, шифрование и сжатие данных. Используется на многих типах физических сетей: нуль-модемный кабель, телефонная линия, сотовая связь и т.д.

PPP представляет собой целое семейство протоколов: протокол управления линией связи (LCP), протокол управления сетью (NCP), протоколы аутентификации (PAP, CHAP), многоканальный протокол PPP (MLPPP).

PPTP (англ. Point-to-point tunneling protocol) — туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. PPTP может также использоваться для организации туннеля между двумя локальными сетями. PPTP использует дополнительное TCP-соединение для обслуживания туннеля.

L2TP (англ. *Layer 2 Tunneling Protocol*) — сетевой протокол туннелирова-

Корпоративные модульные коммутаторы

Компания D-Link, предлагает модульные коммутаторы в качестве «коммутационного центра» корпоративной сети.

Модульные корпоративные коммутаторы представляют собой многофункциональные устройства, которые могут включать несколько десятков модулей различного назначения: повторителей разных технологий, коммутаторов, удаленных мостов, маршрутизаторов и т. п., которые объединены в одном устройстве с модулями-агентами протокола SNMP, и, следовательно, позволяют централизованно объединять, управлять и обслуживать большое количество устройств и сегментов, что очень удобно в сетях большого размера.

Модульный коммутаторы масштаба предприятия обычно обладает внутренней шиной или набором шин очень высокой производительности - до нескольких десятков гигабит в секунду, что позволяет реализовать одновременные соединения между модулями с высокой скоростью, гораздо большей, чем скорость внешних интерфейсов модулей. Основная идея разработчиков таких устройств заключается в создании программно настраиваемой конфигурации связей в сети, причем сами связи между устройствами и сегментами могут также поддерживаться с помощью различных методов: побитовой передачи дан-

ных повторителями, передачи кадров коммутаторами и передачи пакетов сетевых протоколов маршрутизаторами. Примером такого решения может служить устройство серии DES-7200.

Рис. 109. DES-7200

Маршрутизирующие коммутаторы серии DES-7200 являются мультисервисными устройствами с высокой плотностью портов и поддержкой IPv6, предназначенными для установки на уровне ядра крупных корпоративных сетей, городских сетей или сетей операторов связи. Устройства обеспечивают высокую производительность обработки данных и возможность построение полностью защищенной сети. Помимо этого коммутаторы предоставляют распределенную платформу конвергенции сервисов и широкий выбор интерфейсов LAN и WAN, позволяя удовлетворить повышенные требованиям к безопасности и производительности сети, а также предоставляемым сервисам в будущем.

Коммутаторы серии DES-7200 используют маршрутизацию, основанную на стандартах, обеспечивая поддержку сетей на основе Windows, Unix и Интернет. Встроенная коммутационная фабрика осуществляет аппаратную фильтрацию/перенаправление пакетов на скорости канала связи.

Устанавливая в шасси модули расширения, пользователи могут получить до 384 гигабитных портов, до 32 10GE портов, до 192 портов MiniGBIC, или их комбинаций. Благодаря наличию до 8 слотов для установки дополнительных

модулей и их широкому выбору типов портов, пользователи могут легко добавлять или заменять модули в соответствии с их требованиями.

Коммутаторы серии DES-7200 обеспечивают расширенную поддержка VLAN, включая GARP/GVRP, 802.1Q VLAN для повышения производительности и безопасности. Для поддержки конвергированных приложений, включая VoIP, ERP, Интранет и видеоконференции, расширенный набор функций L2/L3/L4 QoS/CoS гарантирует доставку трафика критичных к задержкам приложений с надлежащим приоритетом.

Коммутаторы серии DES-7200 поддерживают IP-маршрутизацию (RIP, OSPF, BGP), IGMP и маршрутизацию многоадресных пакетов PIM-DM/SM, обеспечивая логическую сегментацию сети и управление трафиком. Для повышения отказоустойчивости на канальном уровне поддерживаются протоколы Spanning Tree Protocols (STP), Rapid Spanning Tree Protocol (RSTP) и Multiple Spanning Tree Protocol (MSTP).

Развитые функции управления. DES-7200 поддерживает разнообразные функции сетевого управления, включая CLI, Telnet, Web-интерфейс и SNMP-управление, мониторинг RMON и Single IP Management (SIM). Также доступны расширенные функции управления трафиком, включая управление полосой пропускания и широковещательным/многоадресным штормом.

Благодаря использованию Advanced Service Engine (ASE), DES-7200 поддерживает множество функций MPLS (Multi-protocol Label Switching), в том числе управление метками MPLS, LDP, MPLS L2*/L3 VPN и VPLS*, позволяя провайдерам и предприятиям создавать интеллектуальные сети нового поколения, обеспечивая предоставление всего многообразия расширенных и дополнительных сервисов поверх существующей инфраструктуры. Это решение хорошо совместимо с любой существующей инфраструктурой, в том числе IP, Frame Relay, ATM и Ethernet. Существует возможность объединить абонентов, использующих различные каналы доступа, в единую инфраструктуру MPLS, не требуя замены оборудования, поскольку технология MPLS не зависит от используемой технологии доступа.

Коммутаторы серии DES-7200 обеспечивают маршрутизацию IP-пакетов и функцию трансляции сетевых адресов (NAT) посредством ASE, одинаково полезную как при построении сети предприятия, так и в сетях провайдеров сервисов MAN Ethernet. Кроме того, коммутаторы DES-7200 поддерживают управление доступом 802.1x, периодический запрос ввода учетной записи, несколько учетных записей, вывод статистически, ограничение полосы пропускания. Все это позволяет предоставлять домашним пользователям комплексные услуги Интернет с использованием технологии Ethernet.

Коммутаторы серии DES-7200 поддерживают множество расширенных функций управления трафиком, включая управление полосой пропускания на основе потока и управление многоадресным / широковещательным штормом. Он обеспечивает управление полосой пропускания входящего трафика с шагом до 64Кбит/с. Сочетая в себе ограничение скорости, применяемое для определенных категорий абонентских CPE, и управление доступом на основе учетных

записей пользователей, DES-7200 обеспечивает все необходимые функции для предоставления услуг пользователям сети MAN Ethernet.

Более полную информацию о возможностях маршрутизаторов (коммутаторов L3) и методов их применения можно получить, изучив учебный курс компании D-Link посвящённый этой теме.

Протоколы ARP и RARP

Несмотря на то, что в TCP/IP не рассматриваются технологии канального и физического уровней, при реальной передаче данных все равно приходится отображать IP адрес на адрес канального уровня. Например, отображение на MAC-адреса ***осуществляет Address Resolution Protocol (ARP).***

ARP - очень распространённый и чрезвычайно важный протокол. Каждый узел сети имеет два адреса, физический адрес и логический адрес. В сети Ethernet для идентификации источника и получателя информации используются оба адреса. Информация, пересылаемая от одного компьютера другому по сети, содержит в себе физический адрес отправителя, IP-адрес отправителя, физический адрес получателя и IP-адрес получателя. ARP-протокол обеспечивает связь между этими двумя адресами.

DHCP (англ. Dynamic Host Configuration Protocol - протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к т.н. серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP.

Существует четыре типа ARP-сообщений:

- ARP-запрос (ARP request),
- ARP-ответ (ARP reply),
- RARP-запрос (RARP-request)
- RARP-ответ (RARP-reply).

Локальный хост при помощи ARP-запроса запрашивает физический адрес хоста-получателя. Ответ (физический адрес хоста-получателя) приходит в виде ARP-ответа. Хост-получатель, вместе с ответом, шлёт также RARP-запрос, адресованный отправителю, для того, чтобы проверить его IP-адрес. После проверки IP-адреса отправителя начинается передача пакетов данных.

Перед тем, как создать подключение к какому-либо устройству в сети, IP-протокол проверяет свой ARP-кэш, чтобы выяснить, не зарегистрирована ли в нём уже нужная для подключения информация о хосте-получателе. Если такой записи в ARP-кэше нет, то выполняется широковещательный ARP-запрос. Этот запрос для устройств в сети имеет следующий смысл: «Кто-нибудь знает физический адрес устройства, обладающего следующим IP-адресом?» Когда получатель примет этот пакет, то должен будет ответить: «Да, это мой IP-адрес. Мой физический адрес следующий: …» После этого отправитель обновит свой ARP-кэш, и будет способен передать информацию получателю.

Записи в ARP-кэше могут быть статическими и динамическими. Пример, данный выше, описывает динамическую запись кэша. Хост-отправитель автоматически послал запрос получателю, не уведомляя при этом пользователя. Записи в ARP-кэш можно добавлять вручную, создавая статические записи кэша. Это можно сделать при помощи команды (в MS Windows):

arp -s <IP адрес> <MAC адрес>

После того, как IP-адрес прошёл процедуру разрешения адреса, он остаётся в кэше в течение 2-х минут. Если в течение этих двух минут произошла повторная передача данных по этому адресу, то время хранения записи в кэше продлевается ещё на 2 минуты. Эта процедура может повторяться до тех пор, пока запись в кэше просуществует до 10 минут. После этого запись будет удалена из кэша и будет отправлен повторный ARP-запрос.

Существует также протокол, решающий обратную задачу – нахождение IP адреса по известному локальному адресу. Он называется реверсивный ARP (RARP).

Работа протокола ARP начинается с просмотра ARP-таблицы. Каждая строка таблицы устанавливает соответствие между IP адресом и локальным адресом. Для каждой сети, подключённой к сетевому адаптеру или к порту маршрутизатора, строится отдельная таблица.

ARP оповещение (ARP Announcement)— это пакет (обычно ARP запрос) содержащий корректный физический адрес отправителя (Sender hardware address, SHA) и логический адрес отправителя (Sender protocol address, SPA) хоста-отправителя, с логическим адресом получателя (Target protocol address, TPA) равной SPA. Это не разрешающий запрос, а запрос на обновление ARP-кэша других хостов, получающих пакет. Большинство операционных систем посылают такой пакет при включении хоста в сеть, это позволяет предотвратить ряд проблем. Например при смене сетевой карты (когда необходимо обновить связь между IP и MAC адресами), такой запрос исправит записи в ARP-кэше других хостов в сети.

RARP (англ. Reverse Address Resolution Protocol - Обратный протокол преобразования адресов) - протокол третьего (сетевого) уровня модели OSI, выполняет обратное отображение адресов, то есть преобразует аппаратный адрес в IP-адрес.

Кэш (англ. *cache*, от фр. *cacher* - прятать; произносится [kæʃ] - кэш) - проме-

Протоколы маршрутизации

Внутри сети доставка данных обеспечивается соответствующим канальным уровнем, а вот доставкой данных между сетями занимается сетевой уровень, который и поддерживает возможность правильного выбора маршрута передачи сообщения даже в том случае, когда структура связей между составляющими сетями имеет характер, отличный от принятого в протоколах канального уровня. Сети соединяются между собой специальными устройствами, называемыми маршрутизаторами.

Маршрутизатор - это устройство, которое собирает информацию о топологии межсетевых соединений и на ее основании пересылает пакеты сетевого

Чтобы передать сообщение от отправителя, находящегося в одной сети, получателю, находящемуся в другой сети, нужно совершить некоторое количество транзитных передач между сетями, или хопов (от hop - прыжок), каждый раз выбирая подходящий маршрут. Таким образом, маршрут представляет собой последовательность маршрутизаторов, через которые проходит пакет. На рис.110 показаны четыре сети, связанные тремя маршрутизаторами. Между узлами A и B данной сети пролегают два маршрута: первый через маршрутизаторы 1 и 3, а второй через маршрутизаторы 1, 2 и 3.

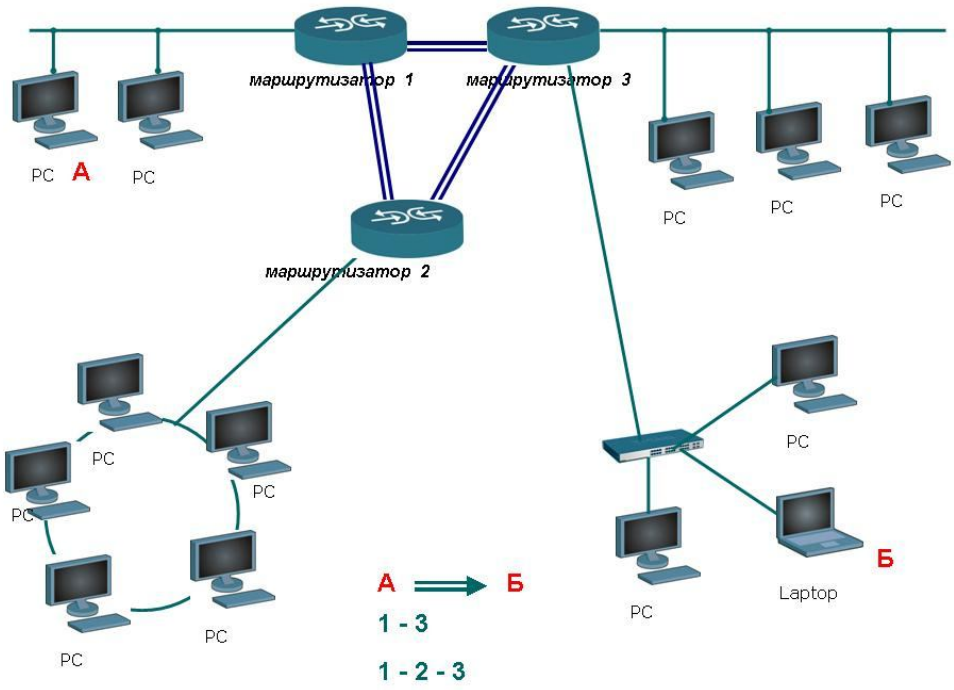


Рис. 110. Пример составной сети

Проблема выбора наилучшего пути называется маршрутизацией, и ее решение является одной из главных задач сетевого уровня. Эта проблема осложняется тем, что самый короткий путь не всегда самый лучший. Часто критерием при выборе маршрута является время передачи данных по этому маршруту; оно зависит от пропускной способности каналов связи и интенсивности трафика, которая может изменяться с течением времени. Некоторые алгоритмы маршрутизации пытаются приспособиться к изменению нагрузки, в то время как другие принимают решения на основе средних показателей за длительное время. Выбор маршрута может осуществляться и по другим критериям, например надежности передачи.

Однако часто к сетевому уровню относят и другой вид протоколов, называемых протоколами обмена маршрутной информацией или просто протоколами маршрутизации (routing protocols). С помощью этих протоколов маршрутизаторы собирают информацию о топологии межсетевых соединений. Протоколы сетевого уровня реализуются программными модулями операционной системы, а также программными и аппаратными средствами маршрутизаторов.

Внутренние и внешние протоколы маршрутизации

Большинство протоколов маршрутизации, применяемых в современных сетях с коммутацией пакетов, ведут свое происхождение от сети Internet и ее предшественницы - сети ARPANET. Для того чтобы понять их назначение и особенности, полезно сначала познакомиться со структурой сети Internet, которая наложила отпечаток на терминологию и типы протоколов.

Internet изначально строилась как сеть, объединяющая большое количество существующих систем. С самого начала в ее структуре выделяли магистральную сеть (core backbone network), а сети, присоединенные к магистрали, рассматривались как автономные системы (autonomous systems, AS). Магистральная сеть и каждая из автономных систем имели свое собственное административное управление и собственные протоколы маршрутизации. Необходимо подчеркнуть, что автономная система и домен имен Internet - это разные понятия, которые служат разным целям. Автономная система объединяет сети, в которых под общим административным руководством одной организации осуществляется маршрутизация, а домен объединяет компьютеры (возможно, принадлежащие разным сетям), в которых под общим административным руководством одной организации осуществляется назначение уникальных символьных имен. Естественно, области действия автономной системы и домена имен могут в частном случае совпадать, если одна организация выполняет обе указанные функции.

Маршрутизаторы/шлюзы, которые используются для образования сетей и подсетей внутри автономной системы, называются ***внутренними шлюзами (interior gateways)***, а шлюзы, с помощью которых автономные системы присоединяются к магистрали сети, называются ***внешними шлюзами (exterior gateways).*** Магистраль сети также является автономной системой. Все автономные системы имеют уникальный 16-разрядный номер, который выделяется организацией, учредившей новую автономную систему, InterNIC.

Соответственно протоколы маршрутизации внутри автономных систем называются ***протоколами внутренних шлюзов (interior gateway protocol, IGP),*** а протоколы, определяющие обмен маршрутной информацией между внешними шлюзами и шлюзами магистральной сети - ***протоколами внешних шлюзов (exterior gateway protocol, EGP)***. Внутри магистральной сети также допустим любой собственный внутренний протокол IGP.

Смысл разделения всей сети Internet на автономные системы - в ее многоуровневом модульном представлении, что необходимо для любой крупной системы, способной к расширению в больших масштабах. Изменение протоколов маршрутизации внутри какой-либо автономной системы никак не должно влиять на работу остальных автономных систем. Кроме того, деление Internet на автономные системы должно способствовать ***агрегированию*** информации в магистральных и внешних шлюзах.

Внутренние шлюзы могут использовать для внутренней маршрутизации достаточно подробные графы связей между собой, чтобы выбрать наиболее рациональный маршрут. Однако если информация такой степени детализации бу-

Бесклассовая адресация (англ. Classless InterDomain Routing, англ. CIDR) - метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать ограниченный ресурс IP-адресов, поскольку возможно применение различных масок подсетей к различным подсетям.

EGP (сокр. от англ. Exterior Gateway Protocol, протокол внешнего шлюза) - устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем. Разработан в 82-84 годах. Впоследствии был заменён на BGP.

BGP (англ. Border Gateway Protocol, протокол граничного шлюза) - основной протокол динамической маршрутизации в Интернете. ***BGP,*** в отличие от других протоколов динамической маршрутизации, предназначен для обмена информацией о маршрутах не между отдельными маршрутизаторами, а между целыми автономными системами, и поэтому, помимо информации о маршрутах в сети, переносит также информацию о маршрутах на автономные системы.

BGP не использует технические метрики, а осуществляет выбор наилучшего маршрута исходя из правил, принятых в сети. ***BGP*** поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации.

BGP является протоколом прикладного уровня и функционирует поверх протокола транспортного уровня TCP (порт 179). BGP, наряду с DNS, является одним из главных механизмов, обеспечивающих функционирование Internet.

дет храниться во всех маршрутизаторах сети, то топологические базы данных так разрастутся, что потребуют наличия памяти гигантских размеров, а время принятия решений о маршрутизации станет неприемлемо большим.

Поэтому детальная топологическая информация остается внутри автономной системы, а автономную систему как единое целое для остальной части Internet представляют внешние шлюзы, которые сообщают о внутреннем составе автономной системы минимально необходимые сведения - количество IP-сетей, их адреса и внутреннее расстояние до этих сетей от данного внешнего шлюза.

Техника бесклассовой маршрутизации ***CIDR*** может значительно сократить объемы маршрутной информации, передаваемой между автономными системами. Так, если все сети внутри некоторой автономной системы начинаются с общего префикса, например 194.27.0.0/16, то внешний шлюз этой автономной системы должен делать объявления только об этом адресе, не сообщая отдельно о существовании внутри данной автономной системы, например, сети 194.27.32.0/19 или 194.27.40.0/21, так как эти адреса агрегируются в адрес 194.27.0.0/16.

Приведенная выше структура Internet с единственной магистралью достаточно долго соответствовала действительности, поэтому специально для нее был разработан протокол обмена маршрутной информации между автономными системами, названный EGP. Однако по мере развития сетей поставщиков услуг структура Internet стала гораздо более сложной, с произвольным характером связей между автономными системами. Поэтому протокол EGP уступил место протоколу BGP, который позволяет распознать наличие петель между автономными системами и исключить их из межсистемных маршрутов. Протоколы EGP и BGP используются только во внешних шлюзах автономных систем, которые чаще всего организуются поставщиками услуг Internet. В маршрутизаторах корпоративных сетей работают внутренние протоколы маршрутизации, такие как RIP и OSPF.

Протокол RIP

Протокол RIP (Routing Information Protocol) является внутренним протоколом маршрутизации дистанционно-векторного типа, он представляет собой один из наиболее ранних протоколов обмена маршрутной информацией и до сих пор чрезвычайно распространен в вычислительных сетях ввиду простоты реализации. Кроме версии RIP для сетей TCP/IP существует также версия RIP для сетей IPX/SPX компании Novell.

Для IP имеются две версии протокола RIP: первая и вторая. Протокол RIPvl не поддерживает масок, то есть он распространяет между маршрутизаторами только информацию о номерах сетей и расстояниях до них, а информацию о масках этих сетей не распространяет, считая, что все адреса принадлежат к стандартными классам A, B или C. Протокол RIPv2 передает информацию о масках сетей, поэтому он в большей степени соответствует требованиям сегодняшнего дня. Так как при построении таблиц маршрутизации работа версии 2 принципиально не отличается от версии 1, то в дальнейшем для упрощения записей будет описываться работа первой версии.

В качестве расстояния до сети стандарты протокола RIP допускают различные виды метрик: хопы, метрики, учитывающие пропускную способность, вносимые задержки и надежность сетей (то есть соответствующие признакам D, T и R в поле «Качество сервиса» IP-пакета), а также любые комбинации этих метрик. Метрика должна обладать свойством аддитивности - метрика составного пути должна быть равна сумме метрик составляющих этого пути. В большинстве реализации RIP используется простейшая метрика - количество хопов, то есть количество промежуточных маршрутизаторов, которые нужно преодолеть пакету до сети назначения.

Рассмотрим процесс построения таблицы маршрутизации с помощью протокола RIP на примере составной сети, изображенной на рис. 111

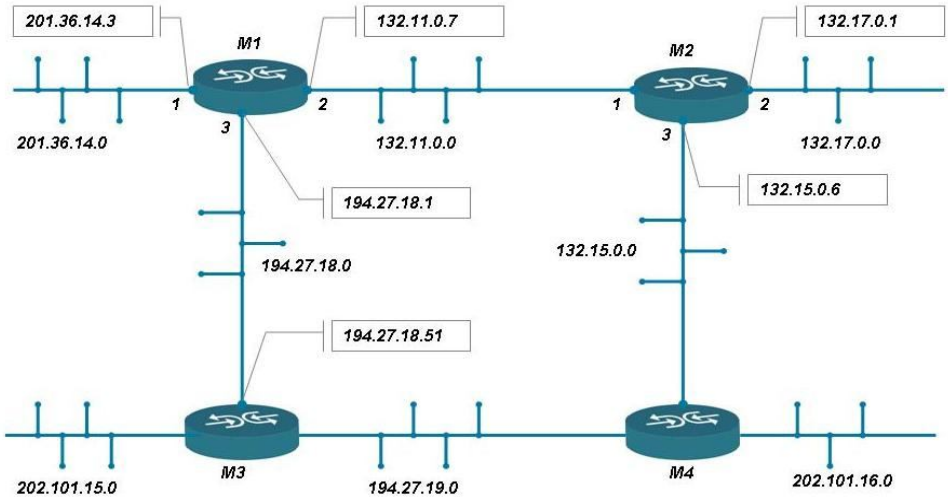


Рис. 111. Сеть, объединенная RIP-маршрутизаторами

Этап 1 - создание минимальных таблиц

В этой сети имеется восемь IP-сетей, связанных четырьмя маршрутизаторами с идентификаторами: Ml, М2, М3 и М4. Маршрутизаторы, работающие по протоколу RIP, могут иметь идентификаторы, однако для работы протокола они не являются необходимыми. В RIP-сообщениях эти идентификаторы не передаются.

В исходном состоянии в каждом маршрутизаторе программным обеспечением стека TCP/IP автоматически создается минимальная таблица маршрутизации, в которой учитываются только непосредственно подсоединенные сети.

Приведённая ниже таблица позволяет оценить примерный вид минимальной таблицы маршрутизации маршрутизатора Ml.

Номер сети	Адрес следующего маршрутизатора	Порт	расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1

Этап 2 - рассылка минимальных таблиц соседям

После инициализации каждого маршрутизатора он начинает посылать своим соседям сообщения протокола RIP, в которых содержится его минимальная таблица.

RIP-сообщения передаются в пакетах протокола UDP и включают два параметра для каждой сети: ее IP-адрес и расстояние до нее от передающего сообщение маршрутизатора.

Соседями являются те маршрутизаторы, которым данный маршрутизатор непосредственно может передать IP-пакет по какой-либо своей сети, не пользуясь услугами промежуточных маршрутизаторов. Например, для маршрутизатора Ml соседями являются маршрутизаторы М2 и М3, а для маршрутизатора М4 - маршрутизаторы М2 и М3.

Таким образом, маршрутизатор Ml передает маршрутизатору М2 и М3 следующее сообщение:

сеть 201.36.14.0, расстояние 1;

сеть 132.11.0.0, расстояние 1;

сеть 194.27.18.0, расстояние 1.

Этап 3 - получение RIP-сообщений от соседей и обработка полученной информации

После получения аналогичных сообщений от маршрутизаторов М2 и М3 маршрутизатор Ml наращивает каждое полученное поле метрики на единицу и запоминает, через какой порт и от какого маршрутизатора получена новая информация (адрес этого маршрутизатора будет адресом следующего маршрутизатора, если эта запись будет внесена в таблицу маршрутизации). Затем маршрутизатор начинает сравнивать новую информацию с той, которая хранится в его таблице маршрутизации.

Номер сети	Адрес следующего маршрутизатора	Порт	расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
194.27.19.0	194.27.18.51	3	2
202.101.15.0	194.27.18.51	3	2
132.11.0.0	132.11.0.101	2	2

194.27.18.0	194.27.18.51	3	2

Записи с четвертой по девятую получены от соседних маршрутизаторов, и они претендуют на помещение в таблицу. Однако только записи с четвертой по седьмую попадают в таблицу, а записи восьмая и девятая - нет. Это происходит потому, что они содержат данные об уже имеющихся в таблице Ml сетях, а расстояние до них хуже, чем в существующих записях.

Протокол RIP замещает запись о какой-либо сети только в том случае, если новая информация имеет лучшую метрику (расстояние в хопах меньше), чем имеющаяся. В результате в таблице маршрутизации о каждой сети остаётся только одна запись; если же имеется несколько равнозначных в отношении расстояния путей к одной и той же сети, то все равно в таблице остается одна запись, которая пришла в маршрутизатор первая по времени. Для этого правила существует исключение - если худшая информация о какой-либо сети пришла от того же маршрутизатора, на основании сообщения которого была создана данная запись, то худшая информация замещает лучшую.

Аналогичные операции с новой информацией выполняют и остальные маршрутизаторы сети.

Этап 4 - рассылка новой, уже не минимальной, таблицы соседям

Каждый маршрутизатор отсылает новое RIP-сообщение всем своим соседям. В этом сообщении он помещает данные о всех известных ему сетях - как непосредственно подключенных, так и удаленных, о которых маршрутизатор узнал из RIP-сообщений.

Этап 5 - получение RIP-сообщений от соседей и обработка полученной информации

Этап 5 повторяет этап 3 - маршрутизаторы принимают RIP-сообщения, обрабатывают содержащуюся в них информацию и на ее основании корректируют свои таблицы маршрутизации.

Посмотрим, как это делает маршрутизатор Ml

Номер сети	Адрес следующего маршрутизатора	Порт	расстояние
201.36.14.0	201.36.14.3	1	1
132.11.0.0	132.11.0.7	2	1
194.27.18.0	194.27.18.1	3	1
132.17.0.0	132.11.0.101	2	2
132.15.0.0	132.11.0.101	2	2
132.15.0.0	194.27.18.51	3	2
194.27.19.0	194.27.18.51	3	2

194.27.19.0	132.11.1.101	2	3
202.101.15.0	194.27.18.51	3	2
202.101.16.0	132.11.0.101	2	3
202.101.16.0	154.27.18.51	3	3

На этом этапе маршрутизатор Ml получил от маршрутизатора М3 информацию о сети 132.15.0.0, которую тот в свою очередь на предыдущем цикле работы получил от маршрутизатора М4. Маршрутизатор уже знает о сети 132.15.0.0, причем старая информация имеет лучшую метрику, чем новая, поэтому новая информация об этой сети отбрасывается.

О сети 202.101.16.0 маршрутизатор Ml узнает на этом этапе впервые, причем данные о ней приходят от двух соседей - от М3 и М4. Поскольку метрики в этих сообщениях указаны одинаковые, то в таблицу попадают данные, которые пришли первыми. В нашем примере считается, что маршрутизатор М2 опередил маршрутизатор М3 и первым переслал свое RIP-сообщение маршрутизатору Ml.

Если маршрутизаторы периодически повторяют этапы рассылки и обработки RIP-сообщений, то за конечное время в сети установится корректный режим маршрутизации. Под корректным режимом маршрутизации здесь понимается такое состояние таблиц маршрутизации, когда все сети будут достижимы из любой сети с помощью некоторого рационального маршрута. Пакеты будут доходить до адресатов и не зацикливаться в петлях, подобных той, которая образуется маршрутизаторами М1-М2-М3-М4.

Очевидно, если в сети все маршрутизаторы, их интерфейсы и соединяющие их каналы связи постоянно работоспособны, то объявления по протоколу RIP можно делать достаточно редко, например, один раз в день. Однако в сетях постоянно происходят изменения - изменяется как работоспособность маршрутизаторов и каналов, так и сами маршрутизаторы и каналы могут добавляться в существующую сеть или же выводиться из ее состава.

Для адаптации к изменениям в сети протокол RIP использует ряд механизмов.

Адаптация RIP-маршрутизаторов к изменениям состояния сети

К новым маршрутам RIP-маршрутизаторы приспосабливаются просто - они передают новую информацию в очередном сообщении своим соседям и постепенно эта информация становится известна всем маршрутизаторам сети. А вот к отрицательным изменениям, связанным с потерей какого-либо маршрута, RIP-маршрутизаторы приспосабливаются сложнее. Это связано с тем, что в формате сообщений протокола RIP нет поля, которое бы указывало на то, что путь к данной сети больше не существует.

Вместо этого используются два механизма уведомления о том, что некоторый маршрут более недействителен:

истечение времени жизни маршрута;

указание специального расстояния (бесконечности) до сети, ставшей недоступной.

Для отработки первого механизма каждая запись таблицы маршрутизации (как и записи таблицы продвижения моста/коммутатора), полученная по протоколу RIP, имеет время жизни (TTL). При поступлении очередного RIP-сообщения, которое подтверждает справедливость данной записи, таймер TTL устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм-аута не придет новое маршрутное сообщение об этом маршруте, то он помечается как недействительный.

Время тайм-аута связано с периодом рассылки векторов по сети. В RIP IP период рассылки выбран равным 30 секундам, а в качестве тайм-аута выбрано шестикратное значение периода рассылки, то есть 180 секунд. Выбор достаточно малого времени периода рассылки объясняется несколькими причинами, которые станут понятны из дальнейшего изложения. Шестикратный запас времени нужен для уверенности в том, что сеть действительно стала недоступна, а не просто произошли потери RIP-сообщений (а это возможно, так как RIP использует транспортный протокол UDP, который не обеспечивает надежной доставки сообщений).

Если какой-либо маршрутизатор отказывает и перестает слать своим соседям сообщения о сетях, которые можно достичь через него, то через 180 секунд все записи, которые породил этот маршрутизатор, станут недействительными у его ближайших соседей. После этого процесс повторится уже для соседей ближайших соседей - они вычеркнут подобные записи уже через 360 секунд, так как первые 180 секунд ближайшие соседи еще передавали сообщения об этих записях.

Как видно из объяснения, сведения о недоступных через отказавший маршрутизатор сетях распространяются по сети не очень быстро, время распространения кратно времени жизни записи, а коэффициент кратности равен количеству хопов между самыми дальними маршрутизаторами сети. В этом заключается одна из причин выбора в качестве периода рассылки небольшой величины в 30 секунд.

Если отказывает не маршрутизатор, а интерфейс или сеть, связывающие его с каким-либо соседом, то ситуация сводится к только что описанной - снова начинает работать механизм тайм-аута и ставшие недействительными маршруты постепенно будут вычеркнуты из таблиц всех маршрутизаторов сети.

Тайм-аут работает в тех случаях, когда маршрутизатор не может послать соседям сообщение об отказавшем маршруте, так как либо он сам неработоспособен, либо неработоспособна линия связи, по которой можно было бы передать сообщение.

Когда же сообщение послать можно, RIP-маршрутизаторы не используют специальный признак в сообщении, а указывают бесконечное расстояние до сети, причем в протоколе RIP оно выбрано равным 16 хопам (при другой метрике необходимо указать маршрутизатору ее значение, считающееся бесконечностью). Получив сообщение, в котором некоторая сеть сопровождается расстоянием 16 (или 15, что приводит к тому же результату, так как маршрутизатор наращивает полученное значение на 1), маршрутизатор должен проверить, исходит ли эта «плохая» информация о сети от того же маршрутизатора, сообщение которого послужило в свое время основанием для записи о данной сети в таблице маршрутизации. Если это тот же маршрутизатор, то информация считается достоверной и маршрут помечается как недоступный.

Такое небольшое значение «бесконечного» расстояния вызвано тем, что в некоторых случаях отказы связей в сети вызывают длительные периоды некорректной работы RIP-маршрутизаторов, выражающейся в зацикливании пакетов в петлях сети. И чем меньше расстояние, используемое в качестве «бесконечного», тем такие периоды становятся короче.

Ограничение в 15 хопов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не может быть больше 15. Для более масштабных сетей нужно применять другие протоколы маршрутизации, например OSPF, или разбивать сеть на автономные области.

Приведенный пример хорошо иллюстрирует главную причину нестабильной работы маршрутизаторов, работающих по протоколу RIP. Эта причина коренится в самом принципе работы дистанционно-векторных протоколов - пользовании информацией, полученной из вторых рук. Действительно, маршрутизатор М2 передал маршрутизатору Ml информацию о достижимости сети 201.36.14.0, за достоверность которой он сам не отвечает. Искоренить эту причину полностью нельзя, ведь сам способ построения таблиц маршрутизации связан с передачей чужой информации без указания источника ее происхождения.

Не следует думать, что при любых отказах интерфейсов и маршрутизаторов в сетях возникают маршрутные петли. Если бы маршрутизатор Ml успел передать сообщение о недостижимости сети 201.36.14.0 раньше ложной информации маршрутизатора М2, то маршрутная петля не образовалась бы. Так что маршрутные петли даже без дополнительных методов борьбы с ними, описанными в следующем разделе, возникают в среднем не более чем в половине потенциально возможных случаев.

Методы борьбы с ложными маршрутами в протоколе RIP

Несмотря на то что протокол RIP не в состоянии полностью исключить переходные состояния в сети, когда некоторые маршрутизаторы пользуются устаревшей информацией об уже несуществующих маршрутах, имеется несколько методов, которые во многих случаях решают подобные проблемы.

Ситуация с петлей, образующейся между соседними маршрутизаторами, описанная в предыдущем разделе, надежно решается с помощью метода, получившем название расщепления горизонта (split horizon). Метод заключается в том, что маршрутная информация о некоторой сети, хранящаяся в таблице маршрутизации, никогда не передается тому маршрутизатору, от которого она получена (это следующий маршрутизатор в данном маршруте). Если маршрутизатор М2 в рассмотренном выше примере поддерживает технику расщепления горизонта, то он не передаст маршрутизатору Ml устаревшую информацию о сети 201.36.14.0, так как получил ее именно от маршрутизатора Ml.

Практически все сегодняшние маршрутизаторы, работающие по протоколу RIP, используют технику расщепления горизонта. Однако расщепление горизонта не помогает в тех случаях, когда петли образуются не двумя, а несколькими маршрутизаторами. Рассмотрим более детально ситуацию, которая возникнет в сети, в случае потери связи маршрутизатора 2 с сетью А. Пусть все маршрутизаторы этой сети поддерживают технику расщепления горизонта. Маршрутизаторы М2 и М3 не будут возвращать маршрутизатору в этой ситуации данные о сети 201.36.14.0 с метрикой 2, так как они получили эту информацию от маршрутизатора Ml. Однако они будут передавать маршрутизатору информацию о достижимости сети 201.36.14.0 с метрикой 4 через себя, так как получили эту информацию по сложному маршруту, а не от маршрутизатора Ml непосредственно. Например, маршрутизатор М2 получил эту информацию по цепочке М4-М3-М1. Поэтому маршрутизатор Ml снова может быть обманут, пока каждый из маршрутизаторов в цепочке М3-М4-М2 не вычеркнет запись о достижимости сети 1 (а это произойдет через период 3 х 180 секунд).

Для предотвращения зацикливания пакетов по составным петлям при отказах связей применяются два других приема, называемые триггерными обновлениями (triggered updates) и замораживанием изменений (hold down).

Способ триггерных обновлений состоит в том, что маршрутизатор, получив данные об изменении метрики до какой-либо сети, не ждет истечения периода передачи таблицы маршрутизации, а передает данные об изменившемся маршруте немедленно. Этот прием может во многих случаях предотвратить передачу устаревших сведений об отказавшем маршруте, но он перегружает сеть служебными сообщениями, поэтому триггерные объявления также делаются с некоторой задержкой. Поэтому возможна ситуация, когда регулярное обновление в каком-либо маршрутизаторе чуть опередит по времени приход триггерного обновления от предыдущего в цепочке маршрутизатора и данный маршрутизатор успеет передать по сети устаревшую информацию о несуществующем маршруте.

Второй прием позволяет исключить подобные ситуации. Он связан с введением тайм-аута на принятие новых данных о сети, которая только что стала недоступной. Этот тайм-аут предотвращает принятие устаревших сведений о некотором маршруте от тех маршрутизаторов, которые находятся на некотором расстоянии от отказавшей связи и передают устаревшие сведения о ее работоспособности. Предполагается, что в течение тайм-аута «замораживания изме-

нений» эти маршрутизаторы вычеркнут данный маршрут из своих таблиц, так как не получат о нем новых записей и не будут распространять устаревшие сведения по сети.

Протокол OSPF

OSPF (англ. Open Shortest Path First) — протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала (link-state technology) и использующий для нахождения кратчайшего пути алгоритм Дейкстры (Dijkstra's algorithm). Протокол OSPF был разработан IETF в 1988 году. Последняя версия протокола представлена в RFC 5709. Протокол OSPF представляет собой протокол внутреннего шлюза (Interior Gateway Protocol — IGP). Протокол OSPF распространяет информацию о доступных маршрутах между маршрутизаторами одной автономной системы.

OSPF предлагает решение следующих задач:

- Увеличение скорости сходимости (в сравнении с протоколом RIP2, так как нет необходимости выжидания многократных тайм-аутов по 30с);
- Поддержка сетевых масок переменной длины (VLSM);
- Достижимость сети (быстро обнаруживаются отказавшие маршрутизаторы, и топология сети изменяется соответствующим образом);
- Оптимальное использование пропускной способности (т.к строится минимальный остовный граф по алгоритму Дейкстры);
- Метод выбора пути.

Описание работы протокола

Маршрутизаторы обмениваются ***hello-пакетами*** через все интерфейсы, на которых активирован OSPF. Маршрутизаторы, разделяющие общий канал передачи данных, становятся соседями, когда они приходят к договоренности об определённых параметрах, указанных в их hello-пакетах.

На следующем этапе работы протокола маршрутизаторы будут пытаться перейти в состояние смежности с маршрутизаторами, находящимися с ним в пределах прямой связи (на расстоянии одного хопа). Переход в состояние смежности определяется типом маршрутизаторов, обменивающихся hello-пакетами, и типом сети, по которой передаются hello-пакеты. OSPF определяет

несколько типов сетей и несколько типов маршрутизаторов. Пара маршрутизаторов, находящихся в состоянии смежности, синхронизирует между собой базу данных состояния каналов.

Каждый маршрутизатор посылает объявление о состоянии канала маршрутизаторам, с которыми он находится в состоянии смежности. Каждый маршрутизатор, получивший объявление от смежного маршрутизатора, записывает передаваемую в нём информацию в базу данных состояния каналов маршрутизатора и рассылает копию объявления всем другим смежным с ним маршрутизатором. Рассылая объявления через зону, все маршрутизаторы строят идентичную базу данных состояния каналов маршрутизатора.

Когда база данных построена, каждый маршрутизатор использует алгоритм «кратчайший путь первым» для вычисления графа без петель, который будет описывать кратчайший путь к каждому известному пункту назначения с собой в качестве корня. Этот граф — дерево кратчайших путей. Каждый маршрутизатор строит таблицу маршрутизации из своего дерева кратчайших путей.

Типы сетей, поддерживаемые протоколом OSPF:

- Широковещательные сети со множественным доступом (Ethernet, Token Ring)
- Точка-точка (T1, E1, коммутируемый доступ)
- Не широковещательные сети со множественным доступом (Frame relay)
- Виртуальные каналы (virtual links)

В сетях со множественным доступом отношения соседства устанавливаются между всеми маршрутизаторами. Если бы все маршрутизаторы в состоянии соседства обменивались топологической информацией, это привело бы к рассылке большого количество копий LSA. Если, к примеру, количество маршрутизаторов в сети со множественным доступом равно n, то будет установлено $n(n-1)/2$ отношений соседства. Каждый маршрутизатор будет рассылать n-1 LSA своим соседям, плюс одно LSA для сети, в результате сеть сгенерирует n^2 LSA.

Для предотвращения проблемы рассылки копий LSA в сетях со множественным доступом выбираются ***выделенный маршрутизатор (DR) и запасной выделенный маршрутизатор (BDR).***

Выделенный маршрутизатор (designated router, DR) — управляет процессом рассылки LSA в сети. Каждый маршрутизатор сети устанавливает отношения смежности с DR. Информация об изменениях в сети отправляется DR маршрутизатором обнаружившим это изменение, а DR отвечает за то, чтобы эта информация была отправлена остальным маршрутизаторам сети.

Недостатком в схеме работы с DR маршрутизатором является то, что при выходе его из строя должен быть выбран новый DR. Новые отношения соседства должны быть сформированы и, пока базы данных маршрутизаторов не

синхронизируются с базой данных нового DR, сеть будет недоступна для пересылки пакетов. Для устранения этого недостатка выбирается BDR.

Резервный выделенный маршрутизатор (backup designated router, BDR). Каждый маршрутизатор сети устанавливает отношения соседства не только с DR, но и BDR. DR и BDR также устанавливают отношения соседства и между собой. При выходе из строя DR, BDR становится DR и выполняет все его функции. Так как маршрутизаторы сети установили отношения соседства с BDR, время недоступности сети минимизируется. Маршрутизатор, выбранный DR или BDR в одной присоединённой к нему сети со множественным доступом, может не быть DR (BDR) в другой присоединённой сети. Роль DR (BDR) является свойством интерфейса, а не свойством всего маршрутизатора.

Таймеры протокола

HelloInterval - Интервал времени в секундах по истечении которого маршрутизатор отправляет следующий ***hello-пакет*** с интерфейса. Для широковещательных сетей и сетей точка-точка значение по умолчанию, как правило, 10 секунд. Для не широковещательных сетей со множественным доступом значение по умолчанию 30 секунд.

RouterDeadInterval - Интервал времени в секундах по истечении которого сосед будет считаться «мертвым». Этот интервал должен быть кратным значению HelloInterval. Как правило, RouterDeadInterval равен 4 интервалам отправки hello-пакетов, то есть 40 секунд.

Wait Timer - Интервал времени в секундах по истечении которого маршрутизатор выберет DR в сети. Его значение равно значению интервала RouterDeadInterval.

RxmtInterval - Интервал времени в секундах по истечении которого маршрутизатор повторно отправит пакет на который не получил подтверждения о получении (например, Database Description пакет или Link State Request пакеты). Это интервал называется также Retransmit interval. Значение интервала 5 секунд.

Внутренний маршрутизатор (internal router) — маршрутизатор все интерфейсы которого принадлежат одной зоне. У таких маршрутизаторов только одна база данных состояния каналов.

Пограничный маршрутизатор (area border router, ABR) — соединяет одну или больше зон с магистральной зоной и выполняет функции шлюза для межзонального трафика. У пограничного маршрутизатора всегда хотя бы один интерфейс принадлежит магистральной зоне. Для каждой присоединенной зоны маршрутизатор поддерживает отдельную базу данных состояния каналов.

Магистральный маршрутизатор (backbone router) — маршрутизатор у которого всегда хотя бы один интерфейс принадлежит магистральной зоне. Определение похоже на пограничный маршрутизатор, однако магистральный

маршрутизатор не всегда является пограничным. Внутренний маршрутизатор интерфейсы которого принадлежат нулевой зоне, также является магистральным.

Пограничный маршрутизатор автономной системы (AS boundary router, ASBR) — обменивается информацией с маршрутизаторами принадлежащими другим автономным системам. Пограничный маршрутизатор автономной системы может находиться в любом месте автономной системы и быть внутренним, пограничным или магистральным маршрутизатором.

Типы объявлений о состоянии канала (LSA)

Type 1 LSA — Router LSA — объявление о состоянии каналов маршрутизатора. Эти LSA распространяются всеми маршрутизаторами. В LSA содержится описание всех каналов маршрутизатора и стоимость (cost) каждого канала. Распространяются только в пределах одной зоны.

Type 2 LSA — Network LSA — объявление о состоянии каналов сети. Распространяется DR в сетях со множественным доступом. В LSA содержится описание всех маршрутизаторов присоединенных к сети, включая DR. Распространяются только в пределах одной зоны.

Type 3 LSA — Network Summary LSA — суммарное объявление о состоянии каналов сети. Объявление распространяется пограничными маршрутизаторами. Объявление описывает только маршруты к сетям вне зоны и не описывает маршруты внутри автономной системы. Пограничный маршрутизатор отправляет отдельное объявление для каждой известной ему сети.

Когда маршрутизатор получает Network Summary LSA от пограничного маршрутизатора он не запускает алгоритм вычисления кратчайшего пути. Маршрутизатор просто добавляет к стоимости маршрута указанного в LSA стоимость маршрута к пограничному маршрутизатору. Затем маршрут к сети через пограничный маршрутизатор помещается в таблицу маршрутизации.

Type 4 LSA — ASBR Summary LSA — суммарное объявление о состоянии каналов пограничного маршрутизатора автономной системы. Объявление распространяется пограничными маршрутизаторами. ASBR Summary LSA отличается от Network Summary LSA тем, что распространяется информация не о сети, а о пограничном маршрутизаторе автономной системы.

Type 5 LSA — AS External LSA — объявления о состоянии внешних каналов автономной системы. Объявление распространяется пограничным маршрутизатором автономной системы в пределах всей автономной системы. Объявление описывает маршруты внешние для автономной системы OSPF или маршруты по умолчанию (default route) внешние для автономной системы OSPF.

Type 7 LSA — AS External LSA for NSSA — объявления о состоянии внешних каналов автономной системы в NSSA зоне. Это объявление может передаваться только в NSSA зоне. На границе зоны пограничный маршрутизатор преобразует type 7 LSA в type 5 LSA.

При разделении автономной системы на зоны, маршрутизаторам принадлежащим к одной зоне не известна информация о детальной топологии других зон.

Разделение на зоны позволяет:

Снизить нагрузку на ЦП маршрутизаторов за счёт уменьшения количества перерасчётов по алгоритму OSPF

Уменьшить размер таблиц маршрутизации

Уменьшить количество пакетов обновлений состояния канала

Каждой зоне присваивается идентификатор зоны (area ID).

Идентификатор может быть указан в десятичном формате или в формате записи IP-адреса. Однако идентификаторы зон не являются IP-адресами и могут совпадать с любым назначенным IP-адресом.

Существует несколько типов зон:

Магистральная зона (backbone area)

Магистральная зона (известная также как нулевая зона или зона 0.0.0.0) формирует ядро сети OSPF. Все остальные зоны соединены с ней, и межзональная маршрутизация происходит через маршрутизатор соединенный с магистральной зоной. Магистральная зона ответственна за распространение маршрутизирующей информации между немагистральными зонами. Магистральная зона должна быть смежной с другими зонами, но она не обязательно должна быть физически смежной; соединение с магистральной зоной может быть установлено и с помощью виртуальных каналов.

Стандартная зона (standard area)

Обычная зона, которая создается по умолчанию. Эта зона принимает обновления каналов, суммарные маршруты и внешние маршруты.

Тупиковая зона (stub area).Тупиковая зона не принимает информацию о внешних маршрутах для автономной системы, но принимает маршруты из других зон. Если маршрутизаторам из тупиковой зоны необходимо передавать информацию за границу автономной системы, то они используют маршрут по умолчанию. В тупиковой зоне не может находиться ASBR. Исключение из этого правила — ABR может быть и ASBR.

Totally stubby area. Totally stubby area не принимает информацию о внешних маршрутах для автономной системы и маршруты из других зон. Если маршрутизаторам необходимо передавать информацию за пределы зоны, то они используют маршрут по умолчанию.

Not-so-stubby area (NSSA) Зона NSSA определяет дополнительный тип LSA — LSA type 7. В NSSA зоне может находиться ASBR.

Версии протокола OSPF

OSPF версия 1

OSPF версия 2 поддерживает версию протокола IPv4

OSPF версия 3 поддерживает версию протокола IPv6

Понятие шлюза по умолчании.

Шлюз по умолчанию (англ. Default gateway), в маршрутизируемых протоколах — это адрес маршрутизатора, на который отправляется трафик, для которого невозможно определить маршрут исходя из таблиц маршрутизации. Применяется в сетях с хорошо выраженными центральными маршрутизаторами, в малых сетях, в клиентских сегментах сетей

Шлюз по умолчанию позволяет упростить координацию трафика, направляя его на центральные маршрутизаторы. В случае рабочей станции таблица маршрутизации обычно состоит (помимо маршрутов обратной петли) из локального маршрута (локального сетевого сегмента, к которому относится рабочая станция) и шлюза по умолчанию, на который отправляется весь остальной трафик. Для устройств, подключенных к одному маршрутизатору, использование шлюза по умолчанию является единственной доступной формой маршрутизации.

Типичным (локальным) адресом шлюза, принятого по умолчанию локальных сетях класса SOHO, является адрес 192.168.0.1.

1.22. Протоколы транспортного уровня

Напомним, транспортный уровень - 4-й уровень сетевой модели OSI предназначен для доставки данных без ошибок, потерь и дублирования в той последовательности, как они были переданы. При этом не важно, какие данные передаются, откуда и куда, то есть он предоставляет сам механизм передачи. Блоки данных он разделяет на фрагменты, размер которых зависит от протокола, короткие объединяет в один, а длинные разбивает.

Существует множество классов протоколов транспортного уровня, начиная от протоколов, предоставляющих только основные транспортные функции (например, функции передачи данных без подтверждения приема), и заканчивая протоколами, которые гарантируют доставку в пункт назначения нескольких пакетов данных в надлежащей последовательности, мультиплексируют несколько потоков данных, обеспечивают механизм управления потоками данных и гарантируют достоверность принятых данных.

Протоколы этого уровня предназначены для взаимодействия типа точка-точка. Пример: TCP, UDP.

Протокол UDP

Протокол UDP является одним из двух основных протоколов транспортного уровня, расположенных непосредственно над IP. Он предоставляет прикладным процессам транспортные услуги, которые не многим отличаются от услуг, предоставляемых протоколом IP. Протокол UDP обеспечивает ненадежную доставку дейтаграмм и не поддерживает соединений из конца в конец. Другими словами, его пакеты могут быть потеряны, продублированы или прийти не в том порядке, в котором они были отправлены. К заголовку IP-пакета он добавляет два поля, одно из которых, поле "порт", обеспечивает мультиплексирование информации между разными прикладными процессами, а другое поле - "контрольная сумма" - позволяет поддерживать целостность данных. Примерами сетевых приложений, использующих UDP, являются NFS и SNMP.

В то время, как задачей сетевого уровня является передача данных между произвольными узлами сети, задача транспортного уровня заключается в передаче данных между любыми прикладными процессами, выполняющимися на любых узлах сети. Действительно, после того, как пакет средствами протокола IP доставлен в компьютер-получатель, данные необходимо направить конкретному процессу-получателю. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных.

Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются *портами*. Прикладной процесс, предоставляющий некоторые услуги другим прикладным процессам (сервер), ожидает поступления сообщений в порт, специально выделенный для этих услуг. Сообщения отправляются процессами-клиентами и должны содержать запросы на предоставление услуг. Порты нумеруются, начиная с нуля. Например, сервер SNMP всегда ожидает поступлений сообщений в порт 161. Если клиент SNMP желает получить услугу, он посылает запрос в UDP-порт 161 на машину, где работает сервер. В каждом узле может быть только один сервер SNMP, так как существует только один UDP-порт 161. Данный номер порта является общеизвестным, то есть фиксированным номером, официально выделенным для услуг SNMP. Таким образом, адресом назначения, который используется на транспортном уровне, является идентификатор (номер) порта прикладного сервиса. Номер порта, задаваемый транспортным уровнем, в совокупности с номером сети и номером компьютера, задаваемыми сетевым уровнем, однозначно определяют прикладной процесс в сети.

Назначение номеров портов прикладным процессам осуществляется либо централизовано, если эти процессы представляют собой популярные общедоступные сервисы, либо локально для тех сервисов, которые еще не стали столь распространенными, чтобы за ними закреплять стандартные (зарезервированные) номера.

Централизованное присвоение сервисам номеров портов выполняется организацией Internet Assigned Numbers Authority.

Протокол TCP

В стеке протоколов TCP/IP протокол TCP работает, как и протокол UDP, на транспортном уровне. Протокол TCP предоставляет транспортные услуги, отличающиеся от услуг UDP. Вместо ненадежной доставки датаграмм без установления соединений, он обеспечивает гарантированную доставку с установлением соединений между прикладными процессами в виде байтовых потоков.

Протокол TCP используется в тех случаях, когда требуется надежная доставка сообщений. Он освобождает прикладные процессы от необходимости использовать таймауты и повторные передачи для обеспечения надежности. Наиболее типичными прикладными процессами, использующими TCP, являются FTP и TELNET. Кроме того, TCP используют система X-Window, rcp (remote copy - удаленное копирование) и другие "r-команды". Большие возможности TCP даются не бесплатно. Реализация TCP требует большой производительности процессора и большой пропускной способности сети. Внутренняя структура модуля TCP гораздо сложнее структуры модуля UDP.

Единицей данных протокола TCP является сегмент. Информация, поступающая к протоколу TCP в рамках логического соединения от протоколов более высокого уровня, рассматривается протоколом TCP как неструктурированный поток байт. Поступающие данные буферизуются средствами TCP. Для передачи на сетевой уровень из буфера "вырезается" некоторая непрерывная часть данных, которая и называется сегментом. Сегменты состоят из заголовка и блока данных. Заголовок сегмента имеет следующие поля:

Порт источника (SOURS PORT) занимает 2 байта, идентифицирует процесс-отправитель;

Порт назначения (DESTINATION PORT) занимает 2 байта, идентифицирует процесс-получатель;

Последовательный номер (SEQUENCE NUMBER) занимает 4 байта, указывает номер байта, который определяет смещение сегмента относительно потока отправляемых данных;

Подтвержденный номер (ACKNOWLEDGEMENT NUMBER) занимает 4 байта, содержит максимальный номер байта в полученном сегменте, увеличенный на единицу; именно это значение используется в качестве квитанции;

Длина заголовка (HLEN) занимает 4 бита, указывает длину заголовка сегмента TCP, измеренную в 32-битовых словах. Длина заголовка не фиксирована и может изменяться в зависимости от значений, устанавливаемых в поле Опции;

Резерв (RESERVED) занимает 6 битов, поле зарезервировано для последующего использования;

Кодовые биты (CODE BITS) занимают 6 битов, содержат служебную информацию о типе данного сегмента, задаваемую установкой в единицу соответствующих бит этого поля:

URG - срочное сообщение;

ACK - квитанция на принятый сегмент;

PSH - запрос на отправку сообщения без ожидания заполнения буфера;

RST - запрос на восстановление соединения;

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

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

Окно (WINDOW) занимает 2 байта, содержит объявляемое значение размера окна в байтах;

Контрольная сумма (CHECKSUM) занимает 2 байта, рассчитывается по сегменту;

Указатель срочности (URGENT POINTER) занимает 2 байта, используется совместно с кодовым битом URG, указывает на конец данных, которые необходимо срочно принять, несмотря на переполнение буфера;

Опции (OPTIONS) - это поле имеет переменную длину и может вообще отсутствовать, максимальная величина поля 3 байта; используется для решения вспомогательных задач, например, при выборе максимального размера сегмента;

Заполнитель (PADDING) может иметь переменную длину, представляет собой фиктивное поле, используемое для доведения размера заголовка до целого числа 32-битовых слов.

В протоколе TCP предусмотрен случай, когда приложение обращается с запросом о срочной передаче данных (бит PSH в запросе установлен в 1). В этом случае протокол TCP передает указанные данные в сеть немедленно, не ожидая заполнения буфера до уровня размера сегмента. О таких данных говорят, что они передаются вне потока - out of band.

Не все сегменты, посланные через соединение, будут одного и того же размера, однако оба участника соединения должны договориться о максимальном размере сегмента, который они будут использовать. Этот размер выбирается таким образом, чтобы при упаковке сегмента в IP-пакет он помещался туда целиком, то есть максимальный размер сегмента не должен превосходить максимального размера поля данных IP-пакета. В противном случае пришлось бы выполнять фрагментацию, то есть делить сегмент на несколько частей, для того, чтобы он вместился в IP-пакет.

Аналогичные проблемы решаются и на сетевом уровне. Для того, чтобы избежать фрагментации, должен быть выбран соответствующий максимальный размер IP-пакета. Однако при этом должны быть приняты во внимание максимальные размеры поля данных кадров всех протоколов канального уровня, используемых в сети. Максимальный размер сегмента не должен превышать минимальное значение на множестве всех MTU составной сети.

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

Однако в протоколе TCP порты используются несколько иным способом. Для организации надежной передачи данных предусматривается установление логического соединения между двумя прикладными процессами. Когда прикладной процесс начинает использовать TCP, то модуль TCP на машине клиента и модуль TCP на машине сервера начинают общаться. Эти два оконечных модуля TCP поддерживают информацию о состоянии соединения, называемого виртуальным каналом. Этот виртуальный канал потребляет ресурсы обоих оконечных модулей TCP. Канал является дуплексным: данные могут одновременно передаваться в обоих направлениях. Один прикладной процесс пишет данные в TCP-порт, они проходят по сети, и другой прикладной процесс читает их из своего TCP-порта. В рамках соединения осуществляется обязательное подтверждение правильности приема для всех переданных сообщений, и при необходимости выполняется повторная передача.

Соединение в протоколе TCP идентифицируется парой полных адресов обоих взаимодействующих процессов (оконечных точек). Адрес каждой из оконечных точек включает IP-адрес (номер сети и номер компьютера) и номер порта. Одна оконечная точка может участвовать в нескольких соединениях.

Установление соединения выполняется в следующей последовательности:

При установлении соединения одна из сторон является инициатором. Она посылает запрос к протоколу TCP на открытие порта для передачи.

После открытия порта протокол TCP на стороне процесса-инициатора посылает запрос процессу, с которым требуется установить соединение.

Протокол TCP на приемной стороне открывает порт для приема данных и возвращает квитанцию, подтверждающую прием запроса.

Для того чтобы передача могла вестись в обе стороны, протокол на приемной стороне также открывает порт для передачи и также передает запрос к противоположной стороне.

Сторона-инициатор открывает порт для приема и возвращает квитанцию.

Соединение считается установленным. Далее происходит обмен данными в рамках данного соединения.

В рамках соединения правильность передачи каждого сегмента должна подтверждаться квитанцией получателя. Квитирование - это один из традиционных методов обеспечения надежной связи. Идея квитирования состоит в следующем.

Для того, чтобы можно было организовать повторную передачу искаженных данных отправитель нумерует отправляемые единицы передаваемых данных (далее для простоты называемые кадрами). Для каждого кадра отправитель ожидает от приемника так называемую положительную квитанцию - служебное сообщение, извещающее о том, что исходный кадр был получен и данные в нем

оказались корректными. Время этого ожидания ограничено - при отправке каждого кадра передатчик запускает таймер, и если по его истечению положительная квитанция на получена, то кадр считается утерянным. Так как TCP-канал является дуплексным, то подтверждения для данных, идущих в одном направлении, могут передаваться вместе с данными, идущими в противоположном направлении. В некоторых протоколах приемник, в случае получения кадра с искаженными данными должен отправить отрицательную квитанцию - явное указание того, что данный кадр нужно передать повторно.

1.23. Протоколы прикладного уровня.

Как было рассмотрено выше, существуют два основных транспортных протокола TCP и UDP. Большинство прикладных программ пользуются только одним из них. Программист при создании прикладного ПО, выбирает тот протокол, который наилучшим образом соответствует потребностям создаваемого программного продукта. Если нужна надёжная и эффективная доставка по длинному и ненадежному каналу передачи данных, то лучше может подойти протокол TCP. Если нужна эффективность на быстрых сетях с короткими соединениями, то лучшим может быть протокол UDP. Если потребности создаваемого ПО не попадают ни в одну из этих категорий, то и выбор транспортного протокола не ясен. Однако прикладные программы могут устранять недостатки выбранного протокола. Например, если вы выбрали UDP, а вам необходима надежность, то прикладная программа должна обеспечить надежность.

Общее количество прикладных программ, доступных в сетях с TCP/IP, велико и продолжает постоянно увеличиваться.

Протоколы прикладного уровня ориентированы на конкретные прикладные задачи. Они определяют как процедуры по организации взаимодействия определенного типа между прикладными процессами, так и форму представления информации при таком взаимодействии. В этом разделе мы коротко опишем некоторые из прикладных протоколов.

Система доменных имен DNS

Соответствие между доменными именами и IP-адресами может устанавливаться как средствами локального хоста, так и средствами централизованной службы. На раннем этапе развития Internet на каждом хосте вручную создавался текстовый файл с известным именем ***hosts***. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «IP-адрес - доменное имя», например:

207.232.83.10 - www.dlink.com

По мере роста Internet, файлы hosts также росли, и создание масштабируемого решения для разрешения имен стало необходимостью. Таким решением

стала специальная служба - ***система доменных имен (Domain Name System, DNS).***

DNS - это централизованная служба, основанная на распределенной базе отображений «доменное имя - IP-адрес». Служба DNS использует в своей работе протокол типа «клиент-сервер». В нем определены DNS-серверы и DNS-клиенты. DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами о разрешении доменного имени в IP-адрес.

Служба DNS использует текстовые файлы почти такого формата, как и файл hosts, и эти файлы администратор также подготавливает вручную. Однако служба DNS опирается на иерархию доменов, и каждый сервер службы DNS хранит только часть имен сети, а не все имена, как это происходит при использовании файлов ***hosts.*** При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер. Этот сервер может хранить отображения «доменное имя - IP-адрес» для всего домена, включая все его поддомены. Однако при этом решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности. Чаще сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. (Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети.

Каждый DNS-сервер кроме таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов. Эти ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов. Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых являются широко известными (их можно узнать, например, в InterNIC).

Процедура разрешения DNS-имени во многом аналогична процедуре поиска файловой системой адреса файла по его символьному имени. Действительно, в обоих случаях составное имя отражает иерархическую структуру организации соответствующих справочников - каталогов файлов или таблиц DNS. Здесь домен и доменный DNS-сервер являются аналогом каталога файловой системы. Для доменных имен, так же как и для символьных имен файлов, характерна независимость именования от физического местоположения.

Процедура поиска адреса файла по символьному имени заключается в последовательном просмотре каталогов, начиная с корневого. При этом предварительно проверяется кэш и текущий каталог. Для определения IP-адреса по доменному имени также необходимо просмотреть все DNS-серверы, обслуживающие цепочку поддоменов, входящих в имя хоста, начиная с корневого домена. Существенным же отличием является то, что файловая система располо-

жена на одном компьютере, а служба DNS по своей природе является распределенной.

Существуют две основные схемы разрешения DNS-имен.

В **первом** варианте работу по поиску IP-адреса координирует DNS-клиент:

DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени;

DNS-сервер отвечает, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в старшей части запрошенного имени;

DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена, и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая схема взаимодействия называется ***не рекурсивной или итеративной***, когда клиент сам ***итерактивно*** выполняет последовательность запросов к разным серверам имен. Так как эта схема загружает клиента достаточно сложной работой, то она применяется редко.

Во **втором** варианте реализуется рекурсивная процедура:

DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, который обслуживает поддомен, к которому принадлежит имя клиента;

если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту; это может соответствовать случаю, когда запрошенное имя входит в тот же поддомен, что и имя клиента, а также может соответствовать случаю, когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше;

если же локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в первом варианте; получив ответ, он передает его клиенту, который все это время просто ждал его от своего локального DNS-сервера.

В этой схеме клиент перепоручает работу своему серверу, поэтому схема называется косвенной или рекурсивной. Практически все DNS-клиенты используют рекурсивную процедуру. Для ускорения поиска IP-адресов DNS-серверы широко применяют процедуру кэширования проходящих через них ответов. Чтобы служба DNS могла оперативно отрабатывать изменения, происходящие в сети, ответы кэшируются на определенное время - обычно от нескольких часов до нескольких дней.

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую использование в имени произвольного количества составных частей

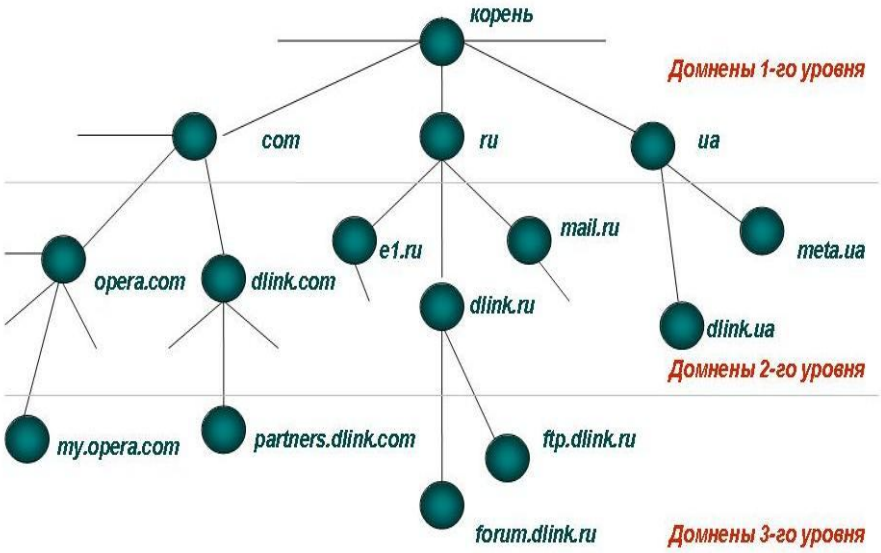


Рис. 112. Иерархическая древовидная структура DNS.

Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети. Составные части доменного имени отделяется друг от друга точкой. Например, в имени partnering.dlink.com составляющая partnering является именем одного из компьютеров в домене dlink.com.

Разделение имени на части позволяет разделить административную ответственность за назначение уникальных имен между различными людьми или организациями в пределах своего уровня иерархии. Разделение административной ответственности позволяет решить проблему образования уникальных имен без взаимных консультаций между организациями, отвечающими за имена одного уровня иерархии. Очевидно, что должна существовать одна организация, отвечающая за назначение имен верхнего уровня иерархии.

Совокупность имен, у которых несколько старших составных частей совпадают, образуют ***домен имен (domain).***

Например, имена **ftp.dlink.ru** и **dlink.ru** входят в домен в ru, так как все эти имена имеют одну общую старшую часть - имя ru.

Если один домен входит в другой домен как его составная часть, то такой домен могут называть поддоменом (subdomain), хотя название домен за ним также остается. Обычно поддомен называют по имени той его старшей составляющей, которая отличает его от других поддоменов.

Например, поддомен **dlink.ru** обычно называют поддоменом (или доменом) dlink в российском сегменте (домене) ”ru”.

Имя поддомену назначает администратор вышестоящего домена. Если в каждом домене и поддомене обеспечивается уникальность имен следующего уровня иерархии, то и вся система имен будет состоять из уникальных имен.

В доменной системе имен различают краткие имена, относительные имена и полные доменные имена.

Краткое имя - это имя конечного узла сети: хоста или порта маршрутизатора. Краткое имя - это лист дерева имен.

Относительное имя - это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, www.dlink- это относительное имя.

Полное доменное имя (fully qualified domain name, FQDN) включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой: www.dlink.ru

Необходимо подчеркнуть, что компьютеры входят в домен в соответствии со своими составными именами, при этом они могут иметь совершенно различные IP-адреса, принадлежащие к различным сетям и подсетям. Доменная система имен реализована в сети Internet, но она может работать и как автономная система имен в крупной корпоративной сети, использующей стек TCP/IP, но не связанной с Internet.

В Internet корневой домен управляется центром InterNIC. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны следовать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры (“ru”,”ua”), а для различных типов организаций - следующие обозначения, вот некоторые :

com - коммерческие организации;
gov - правительственные организации;
org - некоммерческие организации;
net - организации, поддерживающие сети.
info- информационные ресурсы
biz - только коммерческие организации
aero - для субъектов авиатранспортной индустрии
coop- кооперативы
edu - высшие учебные заведения.
int - межгосударственные организации
mil - министерство вооруженных сил США
museum - музеи
travel - для субъектов туристического бизнеса.

Каждый домен администрируется отдельной организацией, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой InterNIC делегировал свои полномочия по распределению имен доменов. В России такой организацией является РосНИИРОС, которая отвечает за делегирование имен поддоменов в домене ru.

Telnet - протокол эмуляции терминала, обычно используемый в сети Интернет и в сетях, работающих по протоколам, основанным на TCP/IP. Протокол telnet был первоначально разработан для ARPAnet и является важной частью протокола передачи данных TCP/IP.

Протокол Telnet позволяет обслуживающей машине рассматривать все удаленные терминалы как стандартные "сетевые виртуальные терминалы" строчного типа, работающие в коде ASCII, а также обеспечивает возможность согласования более сложных функций (например, локальный или удаленный эхо-контроль, страничный режим, высота и ширина экрана и т.д.). Telnet работает на базе протокола TCP.

На прикладном уровне над Telnet находится либо программа поддержки реального терминала (на стороне пользователя), либо прикладной процесс в обсуживающей машине, к которому осуществляется доступ с терминала. Это позволяет пользователю терминала или персонального компьютера, регистрироваться в системе удаленного компьютера и выполнять программы.

Создано множество реализаций для самых разных операционных систем.

Telnet - клиент-серверный протокол, и клиенты в общем случае соединяется с портом 23 на удаленном компьютере, предоставляющем такую услугу (хотя, подобно многим протоколам, используемым в сети Интернет, используемый для соединения порт можно изменить, другими словами 23 номер порта – всего лишь общий случай). Частично из-за конструкции протокола и частично из-за гибкости, обычно снабжаемой программами telnet, можно использовать программу telnet, чтобы установить интерактивное подключение TCP с некоторой другой услугой удаленного компьютера. Классическим примером такого использования клиентской части протокола может послужить соединение при помощи программы telnet с портом 25 удаленного компьютера (где обычно находиться SMTP сервер) чтобы отладить сервер почты.

Протокол telnet может быть представлен в виде ядра и наборов дополнений. Ядро протокола описано в соответствии с IETF документами RFC 854 и RFC 855, которые также собраны вместе в STD 8, который определяет только базисные эксплуатационные показатели протокола и способы определения и осуществления дополнений к нему. Имеется много дополнений, некоторые из которых были приняты как стандарты Интернет, некоторые нет.

Отмечают три главных проблемы связанные с использованием telnet, делая его плохим выбором для современных систем с точки зрения безопасности:

- Используемые по умолчанию демоны telnet имеют сетевые уязвимости;
- Telnet не шифрует никакие данные, которые посылаются через установленную связь (включая пароли), и таким образом становится воз-

можным прослушивание связи и использование пароля позже для злонамеренных целей.

- Отсутствие системы аутентификации в telnet не дает никакой гарантии, что связь, установленная между двумя удаленными хостами не будет прервана в середине.

Нежелательно использование протокола telnet в системах, для которых важна безопасность, таких как общественный Интернет.

SSH (Secure Shell) — сетевой протокол, позволяющий производить удалённое управление компьютером и передачу файлов. Сходен по функциональности с протоколом Telnet, однако использует алгоритмы шифрования передаваемой информации.

Криптографическая защита протокола SSH не фиксирована, возможен выбор различных алгоритмов шифрования. Клиенты и серверы, поддерживающие этот протокол, доступны для различных платформ. Кроме того, протокол позволяет не только использовать безопасный удалённый shell на машине, но и туннелировать графический интерфейс — X Tunnelling (только для Unix-подобных ОС или приложений, использующих графический интерфейс X Window System). SSH также способен передавать через безопасный канал (Port Forwarding) любой другой сетевой протокол, обеспечивая (при надлежащем конфигурировании) возможность безопасной пересылки не только X-интерфейса, но и, например, звука.

Поддержка SSH реализована во всех UNIX системах, и на большинстве из них в числе стандартных утилит присутствуют клиент и сервер ssh. Существует множество реализаций SSH-клиентов и для не-UNIX ОС. Большую популярность протокол получил после широкого развития программ для прослушивания сети, как альтернатива небезопасному **Telnet** решение для управления важными узлами.

SSH предоставляет 3 способа аутентификации клиента: по ip адресу клиента(небезопасно), по публичному ключу клиента и стандартный парольный метод

Схема работы

При запросе клиента сервер сообщает ему, какие методы аутентификации он поддерживает (это определяется в опции PreferredAuthentications sshd.conf) и клиент по очереди пытается проверить их. По умолчанию клиент вначале пытается аутентифицироваться своим адресом, затем публичным ключом и, если ничего не сработало, передаёт пароль, введённый с клавиатуры (при этом пароль шифруется асимметрическим шифрованием). После прохождения аутентификации одним из методов из имеющихся у клиента и сервера пар ключей генерируется сеансовый ключ симметрического шифрования. После чего все

последующие данные, передаваемые через ssh, шифруются данным ключом (обычно используется алгоритм aes с длиной ключа 128 бит). Также вместе с данными посылаются контрольные суммы формата sha или md5, что исключает подмену или иную модификацию передаваемого трафика.

SSH защищает от:

- «ip-подмены» (IP spoofing), когда удаленный (атакующий) компьютер высылает свои пакеты симулируя якобы они пришли с другого компьютера, с которого разрешен доступ. SSH защищает от подмены даже в локальной сети, когда кто-то например, решил подменить маршрутизатор сети "собой".
- «ip исходный маршрутизатор» (IP source routing), когда компьютер может симулировать что IP-пакеты приходят от другого, разрешенного компьютера (маршрутизатора).
- «DNS spoofing» , когда атакующий фальсифицирует записи DNS-сервера.
- Прослушивания нешифрованных паролей и других данных промежуточными компьютерами.
- Манипуляций над вашими данными людьми управляющими промежуточными компьютерами.

Все вышесказанное верно, лишь при использовании шифрования. Однако SSH имеет опцию шифрования "none", которая необходима лишь для отладки и ни в коем случае не должна быть использована для обычной работы.

Протоколы FTP и TFTP

Протокол FTP распространен также широко как Telnet, и также как он представляет собой клиент-серверный протокол. Он является одним из старейших протоколов семейства TCP/IP. Также как Telnet он пользуется транспортными услугами TCP.

FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

Существует множество реализаций для различных операционных систем, которые хорошо взаимодействуют между собой. Пользователь FTP может вызывать несколько команд, которые позволяют ему посмотреть каталог удален-

ной машины, перейти из одного каталога в другой, а также скопировать один или несколько файлов.

Работа FTP на пользовательском уровне содержит несколько этапов:

- Идентификация (ввод имени-идентификатора и пароля).
- Выбор каталога.
- Определение режима обмена (поблочный, поточный, ASCII или двоичный).
- Выполнение команд обмена (get, mget, dir, mdel, mput или put).
- Завершение процедуры (quit или close).

Процедура организации FTP поддерживает две логические связи между узлами (компьютерами). Одна связь служит для удаленного доступа и использует протокол Telnet. Другая связь предназначена для обмена данными. Сервер производит операцию passive open для порта 21 и ждет соединения с клиентом. Клиент осуществляет операцию active open для порта 21. Канал остается активным до завершения процедуры FTP. Канал для передачи данных (TCP) формируется каждый раз для пересылки файлов. Канал открывается перед началом пересылки и закрывается по коду end_of_file (конец файла).

Конечный пользователь взаимодействует с протокольным интерпретатором, в задачи которого входит управление обменом информацией между пользователем и файловой системой, как местной, так и удаленной. Схема взаимодействия различных частей Internet при работе FTP изображена на рис. 113

Сначала по запросу клиента формируется канал управления, который в дальнейшем используется для передачи команд от клиента и откликов от сервера. Информационный канал формируется сервером по команде клиента, он не должен существовать постоянно на протяжении всей FTP-сессии и может формироваться и ликвидироваться по мере необходимости. Канал управления может быть закрыт только после завершения информационного обмена. Для канала управления используется протокол Telnet. После того как управляющий канал сформирован, клиент может посылать по нему команды. Сервер воспринимает, интерпретирует эти команды и передает отклики.

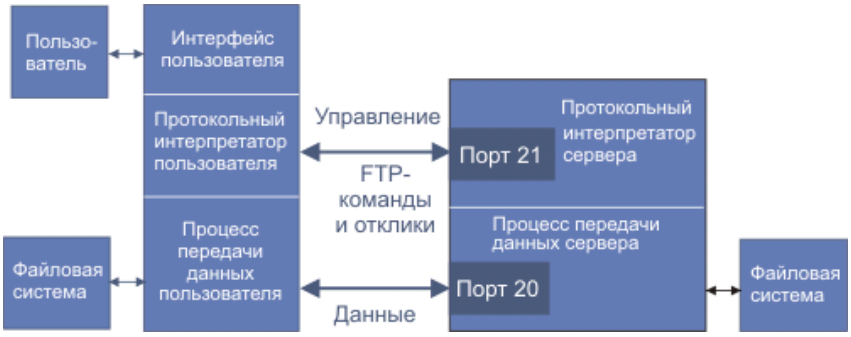


Рис. 113. Схема работы протокола FTP

TFTP (Trivial FTP, RFC-1350, -783, RFC-906, STD0033) представляет собой упрощенную версию FTP. TFTP не имеет системы безопасности и идентификации, она в отличии от FTP базируется на протоколе UDP (порт 69), а не TCP. Обычно передача осуществляется блоками по 512 байт с ожиданием подтверждения приема каждого пакета (протокол "стой-и-жди"). TFTP используется при загрузке операционной системы в бездисковые рабочие станции или для загрузки конфигурационных файлов в маршрутизатор.

Поскольку протокол не поддерживает аутентификации, единственный метод идентификации клиента — это его сетевой адрес (который может быть подделан).

Порядок работы

Сначала устанавливается связь между клиентом и сервером, для этого посылаются запросы WRQ (write) или RRQ (read). При этом сообщается имя файла и режим доступа (Mode). Предусмотрено два режима доступа:

- **netascii** — файл перед передачей перекодируется в ASCII.
- **octet** — файл передается без изменений.

В начале TFTP-пакета идет поле размером в 2 байта, определяющее тип пакета:

Read Request (RRQ) — запрос на чтение файла.

Write Request (WRQ) — запрос на запись файла.

Data (DATA) — данные, передаваемые через TFTP.

Acknowledgment (ACK) — подтверждение пакета.

Error (ERR) — ошибка.

Options Acknowledgment (OACK) — подтверждение опций.

После получения RRQ-пакета сервером, он сразу начинает передачу данных. В случае с WRQ-запросом - сервер должен прислать ACK-пакет с номером пакета 0. Сервер использует IP-адрес и номер UDP-порта клиента для идентификации последующих операций. Таким образом, ни при пересылке данных, ни при передаче подтверждений (ACK) не нужно указывать явно имя файла. Блоки данных нумеруются, начиная с 1, подтверждение получения пакета имеет тот же номер. Получение блока с размером менее 512 байт означает конец файла. Получение сигнала об ошибке прерывает обмен. При возникновении тайм-аута производится повторная передача последнего блока данных или подтверждения.

Предусмотрено шесть типов сообщений об ошибках:

0 - не определен;

1 - файл не найден;

2 - ошибка доступа;

3 - переполнение диска или превышение выделенной квоты;

4 - нелегальная TFTP-операция;

5 - неизвестный идентификатор обмена.

Всего по TFTP можно передать 32 Мб (65536 * 512 / 1024^2), однако если клиент и сервер поддерживают расширения протокола RFC 2347 и RFC 2348, то максимальный размер передаваемого файла увеличивается до 4Gb.

Протоколы HTTP и SSL

HTTP (сокр. от англ. HyperText Transfer Protocol, «протокол передачи гипертекста») - протокол прикладного уровня передачи данных (изначально — в виде гипертекстовых документов). Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом. HTTP в настоящее время повсеместно используется во Всемирной паутине для получения информации с веб-сайтов.

HTTP используется также в качестве «транспорта» для других протоколов прикладного уровня, таких как SOAP, XML-RPC, WebDAV.

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (англ. Uniform Resource Identifier - унифицированный (единообразный) идентификатор ресурса) в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть логические объек-

ты или что-то абстрактное. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т. д. Именно благодаря возможности указания способа кодирования сообщения клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

HTTP — протокол прикладного уровня, аналогичными ему являются FTP и SMTP. Обмен сообщениями идёт по обыкновенной схеме «запрос-ответ». Для идентификации ресурсов HTTP использует глобальные URI. В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами. Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако в самом протоколе не предусмотрена внутренняя поддержка состояния.

Первоначально протокол HTTP разрабатывался для доступа к гипертекстовым документам Всемирной паутины. Поэтому основными реализациями клиентов являются браузеры (агенты пользователя). Популярные браузеры :Internet Explorer, Mozilla Firefox, Opera, и др.

Использование текстового формата в протоколе порождает соответствующий недостаток - большой размер сообщений по сравнению с передачей двоичных данных. Из-за этого возрастает нагрузка на оборудование при формировании, обработке и передаче сообщений. Для решения данной проблемы в протокол встроены средства для обеспечения кэширования на стороне клиента, а также средства компрессии передаваемого контента. Нормативными документами по протоколу предусмотрено наличие прокси-серверов, которые позволяют получить клиенту документ с наиболее близкого к нему сервера. Также в протокол было внедрено diff-кодирование, чтобы клиенту передавался не весь документ, а только его изменённая часть.

И хотя протокол разрабатывался как средство работы с ресурсами сервера, у него отсутствуют в явном виде средства навигации среди этих ресурсов. Например, клиент не может явным образом запросить список доступных файлов, как в протоколе FTP. Предполагалось, что конечный пользователь уже знает URI необходимого ему документа, закачав который, он будет производить навигацию благодаря гиперссылкам. Это вполне нормально и удобно для человека, но затруднительно, когда стоят задачи автоматической обработки и анализа всех ресурсов сервера без участия человека. Решение этой проблемы лежит полностью на плечах разработчиков приложений, использующих данный протокол.

Например, со стороны клиента используются «веб-пауки» - специальные программы, которые составляют список ресурсов сервера проходя по всем найденным гиперссылкам. Со стороны сервера данная проблема решается с помо-

щью карты сайта (англ. site map) - специальной веб-страницы, где перечислены все доступные для посещения ресурсы. Она предназначена не только для людей, играя аналогичную содержанию в книге роль, но и полезна для тех же роботов-пауков позволяя уменьшить глубину - минимальное необходимое количество переходов с главной страницы. Для тех же целей служат файлы формата Sitemap, которые предназначены уже непосредственно для роботов.

Всё программное обеспечение для работы с протоколом HTTP разделяется на три больших категории:

- Серверы как основные поставщики услуг хранения и обработки информации (обработка запросов).
- Клиенты - конечные потребители услуг сервера (отправка запроса).
- Прокси для выполнения транспортных служб.

Для отличия конечных серверов от прокси в официальной документации используется термин исходный сервер (англ. origin server.). Разумеется, один и тот же программный продукт может одновременно выполнять функции клиента, сервера или посредника в зависимости от поставленных задач. В спецификациях протокола HTTP подробно описывается поведение для каждой из этих ролей.

HTTP протокол предлагает достаточно простой, парольный способ идентификации того или иного пользователя. В момент соединения с сервером, пользователь вводит пароль, пароль передается серверу в открытом, не зашифрованном виде, и далее, проверив соответствие пароля и имени пользователя, сервер открывает или не открывает затребованное соединение.

Не секрет, что можно без особых технических ухищрений просматривать данные, которыми обмениваются между собой клиенты и серверы. Был даже придуман специальный термин для этого – sniffer (рус. нюхач) . А в связи с увеличением объема использования Интернета в коммерческих целях, неизбежно вставал вопрос о защите передаваемых данных. Было создано несколько различных безопасных протоколов. Официальный протокол, разработку которого спонсировала IETF, назывался Secure HTTP (SHTTP). Помимо него, разрабатывались, и были созданы, еще несколько не официальных проектов, один из которых, под названием SSL (Secure Sockets Layer), созданный Netscape, получил большую популярность и широкое распространение. Не смотря на свою популярность, SSL не является официальным Интернет стандартом.

Протокол SSL (secure socket layer) разработанный фирмой Netscape, как протокол обеспечивающий защиту данных между сервисными протоколами (такими как HTTP, NNTP, FTP и т.д.) и транспортными протоколами (TCP/IP). Часто для него используется аббревиатура **HTTPS**. Именно эта латинская буква

"s" превращает обычный, не защищенный канал передачи данных в Интернете по протоколу HTTP, в засекреченный или защищенный.

Протокол SSL предоставляет "безопасный канал", который имеет три основные свойства:

Канал является частным. Шифрование используется для всех сообщений после простого диалога, который служит для определения секретного ключа.

Канал аутентифицирован. Серверная сторона диалога всегда аутентифицируется, в то время как клиентская - аутентифицируется опционно.

Канал надежен. Транспортировка сообщений включает в себя проверку целостности (с привлечением MAC).

Появление такого протокола как SSL было вполне закономерным явлением. С одной стороны остаются все возможности сервисных протоколов (для программ-серверов), плюс к этому все данные передаются в зашифрованном виде. И раскодировать их довольно трудно. Следует отметить, что SSL не только обеспечивает защиту данных в Интернете, но так же производит опознание сервера и клиента (server/client authentication).

Использование SSL

Чаще всего, этот протокол используется в составе любого Интернет-ресурса, осуществляющего манипуляции с личными или финансовыми данными посещающих его пользователей Интернета. Чаще всего, это банки, Интернет-магазины или любые другие виртуальные места, в которых приходящие по своим делам пользователи, вынуждены передавать свои личные, и зачастую, секретные данные. Этого может потребовать и простая регистрация, и процедура оплаты какого-либо товара, или любая другая процедура, при которой пользователи вынуждены честно выдавать свои паспортные данные, PIN коды и пароли.

Итак, главным назначением SSL-протокола, является обеспечение приватного и надежного способа обмена информацией между двумя удаленно взаимодействующими приложениями. Протокол реализуется в виде двухслойной (многослойной) среды, специально предназначенной для безопасного переноса секретной информации, через не засекреченные каналы связи. В качестве первого слоя, в такой среде используется некоторый надежный транспортный протокол; TCP к примеру. По слову "транспортный", не трудно догадаться, что TCP берет на себя функции "несущей", и в дальнейшем, становится извозчиком, для всех лежащих выше слоев (протоколов). Вторым по счету слоем, накладываемым на TCP, является SSL Record Protocol. Вместе, эти два слоя, TCP и SSL Record Protocol, формируют своеобразное ядро SSL. В дальнейшем, это ядро становится первичной герметизирующей оболочкой, для всех последующих более сложных протокольных инфраструктур. В качестве одной из таких структур, используется SSL Handshake Protocol - позволяющий серверу и кли-

енту идентифицировать друг друга и согласовывать криптографические алгоритмы и ключи, перед тем как приложения, работающие на серверной и клиентской стороне, смогут начать передачу или прием информационных байтов в защищенном режиме.

Одним из не мало важных преимуществ SSL, является его полная программно-платформенная независимость. Протокол разработан на принципах переносимости, и идеология его построения, не зависит, от тех приложений, в составе которых он используется. Помимо этого, важно и то, что поверх протокола SSL, могут прозрачно накладываться и другие протоколы; либо для еще большего увеличения степени защиты целевых информационных потоков, либо, для адаптации криптографических способностей SSL под какую-нибудь другую, вполне определенную задачу.

Использование SSL начинается в тот момент, когда пользователь вводит в адресной строке своего браузера URL начинающийся с аббревиатуры HTTPS. В результате, он подключается к порту за номером 443, который для SSL обычно используется по умолчанию (для стандартного HTTP соединения, чаще всего используется порт 80). В процессе подключения, браузер пользователя (в дальнейшем клиент), посылает серверу приветственное сообщение (hello message). В свою очередь сервер, также должен посылать клиенту свое приветственное сообщение. Приветственные сообщения, являются первичными, инициализирующими сообщениями и содержат информацию, используемую при дальнейшей настройке открываемого секретного канала. В общем случае, приветственное сообщение устанавливает четыре основных параметра: версия протокола, идентификатор сессии, способ шифрования, метод компрессии, а также, два специально сгенерированных случайных числа; и сервер, и клиент, генерируют такие числа независимо друг от друга, а затем, просто обмениваются ими друг с другом.

После получения приветственного сообщения от клиента, сервер отсылает свой сертификат, если таковой у него имеется. Также, при необходимости, сервер может послать и некое ключевое сообщение, например в случае отсутствии сертификата. Если сервер авторизирован (т.е. имеет соответствующий сертификат), он может потребовать и клиентский сертификат, если того потребует выбранный способ шифрования данных. После этого, производится еще ряд промежуточных обменных операций, в процессе которых, производится окончательное уточнение выбранного алгоритма шифрования, ключей и секретов, и далее, сервер посылает клиенту некое финальное сообщение, после чего обе стороны приступают к обмену зашифрованной информации.

На практике, процесс обмена ключами и сертификатами, иногда может занимать относительно много времени. С этой целью, часто предусматривается возможность повторного использования одних и тех же идентификационных данных. Бывают ситуации, когда после установления соединения с SSL-сервером, у пользователя появляется желание открыть еще одно окно браузера, и через него, осуществить еще одно подключение к тому же SSL-серверу. В

этом случае, чтобы не повторять весь цикл предварительных обменных операций, браузер может отправить серверу идентификатор сессии предыдущего соединения, и если сервер примет этот идентификатор, весь набор шифровочных и компрессионных параметров, будет взят от предыдущего соединения.

SSL как таковой, теоретически, может обеспечить практически полную защиту любого Интернет соединения. Однако, программы так или иначе использующие SSL протокол, является порой самым уязвимым местом этой технологии. Именно из-за ошибок в этих программах, возможна почти полная потеря, всех, достигнутых после использования SSL щитов и заслонов. К таким программным инструментам, прежде всего, относятся активно используемые нами Интернет-браузеры.

Одним из самых показательных критериев уровня защиты, является размер используемых ключей. Чем больше этот размер, тем соответственно надежнее защита. Браузеры в основном используют три размера: 40, 56 и 128 бит, соответственно. Причем, 40-а битный вариант ключа недостаточно надежен. Таким образом, предпочтительнее использовать именно 128-ми битные ключи.

Но размер ключа, не будет играть решающий роли, если в защите браузера имеется внутренняя брешь. Сообщения об открытии таких брешей, в тех или иных браузерах, появляются с регулярными интервалами. Такая брешь напоминает открытую форточку в протапливаемой комнате - все тепло мгновенно выветривается.

Все эти и им подобные прорехи, не идут ни в какое сравнение с той угрозой, которую могут представлять для пользователя вовремя не отозванные сертификаты. Дело в том, что браузеры обычно поставляются с неким, вполне определенным набором действительных сертификатов, но автоматического механизма проверки этой годности по прошествии некоторого времени - не существует. Таким образом, возможно, что действие, того или иного, используемого вашим браузером сертификата, уже, давно кончилось; мог истечь срок годности, мог быть потерян контроль над личным ключом соответствующим этому сертификату и.т.д. В любом из этих случаев, сертификат автоматически отзывается, и помещается в специальный, так называемый revocation list, или список не годных сертификатов, создаваемый и обновляемый тем или иным сертификационным сообществом (CA). Теперь, если не удалить такой сертификат из вашего браузера, он по прежнему будет числиться как годный, со всеми вытекающими отсюда последствиями.

Следует заметить, что идея, заложенная в протоколе SSL безусловно, хороша. Хотя у нее есть и свои плюсы, и свои минусы, но в целом, этот протокол можно назвать одним из наиболее удачных решений проблемы защиты пользовательских данных при их распространении "открытым" каналом. Этот протокол вполне бы мог стать некой сетевой панацеей. Но, к сожалению, практика, показывает что идея это еще не решение. Без соответствующей практической составляющей, идея так и остается идеей, а потому, пользователи безусловно, должны помнить, что символ замка, появляющийся в строке состояния их Ин-

тернет-браузеров, еще не гарантия того, что все наши секреты и тайны находятся под действительно надежной защитой

Протокол DHCP

DHCP (англ. Dynamic Host Configuration Protocol, протокол динамической конфигурации узла) - это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Протокол DHCP представляет собой стандартный протокол, определенный RFC 1541 (заменен на RFC 2131), который позволяет серверу динамически присваивать клиентам IP-адреса и сведения о конфигурации. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

Формат: Список

Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

IP-адрес маршрутизатора по умолчанию;
маска подсети;
адреса серверов DNS;
имя домена DNS.

Формат: Список

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP

Рассмотрим пример процесса получения IP-адреса клиентом от сервера DHCP. Предположим, клиент ещё не имеет собственного IP-адреса, но ему известен его предыдущий адрес - 192.168.1.100. Процесс состоит из четырёх этапов.

Обнаружение DHCP

Вначале клиент выполняет широковещательный запрос по всей физической сети с целью обнаружить доступные DHCP-серверы. Он отправляет сообщение типа DHCPDISCOVER, при этом в качестве IP-адреса источника указывается 0.0.0.0 (так как компьютер ещё не имеет собственного IP-адреса), а в качестве адреса назначения — широковещательный адрес 255.255.255.255.

Клиент заполняет несколько полей сообщения начальными значениями:

В поле xid помещается уникальный идентификатор транзакции, который позволяет отличать данный процесс получения IP-адреса от других, протекающих в то же время.

Формат: Список

В поле chaddr помещается аппаратный адрес (MAC-адрес) клиента.

В поле опций указывается последний известный клиенту IP-адрес. В данном примере это 192.168.1.100. Это необязательно и может быть проигнорировано сервером.

Сообщение DHCPDISCOVER может быть распространено за пределы локальной физической сети при помощи специально настроенных агентов ретрансляции DHCP, перенаправляющих поступающие от клиентов сообщения DHCP серверам в других подсетях.

Предложение DHCP

Получив сообщение от клиента, сервер определяет требуемую конфигурацию клиента в соответствии с указанными сетевым администратором настройками. В данном случае DHCP-сервер согласен с запрошенным клиентом адре-

сом 192.168.1.100. Сервер отправляет ему ответ (DHCPOFFER), в котором предлагает конфигурацию. Предлагаемый клиенту IP-адрес указывается в поле yiaddr. Прочие параметры (такие, как адреса маршрутизаторов и DNS-серверов) указываются в виде опций в соответствующем поле.

Это сообщение DHCP-сервер отправляет хосту, пославшему DHCPDISCOVER, на его MAC. Клиент может получить несколько различных предложений DHCP от разных серверов; из них он должен выбрать то, которое его «устраивает».

Запрос DHCP

Выбрав одну из конфигураций, предложенных DHCP-серверами, клиент отправляет запрос DHCP (DHCPREQUEST). Он рассылается широковещательно; при этом к опциям, указанным клиентом в сообщении DHCPDISCOVER, добавляется специальная опция — идентификатор сервера — указывающая адрес DHCP-сервера, выбранного клиентом (в данном случае — 192.168.1.1).

Подтверждение DHCP

Сервер получив запрос DHCPREQUEST подтверждает его и направляет подтверждение (DHCPACK) клиенту. После этого клиент должен настроить свой сетевой интерфейс, используя предоставленные опции.

Если после получения подтверждения (DHCPACK) от сервера клиент обнаруживает, что указанный сервером адрес уже используется в сети, он рассылает широковещательное сообщение отказа DHCP (DHCPDECLINE), после чего процедура получения IP-адреса повторяется. Использование IP-адреса другим клиентом можно обнаружить, выполнив запрос ARP.

Если по каким-то причинам сервер не может предоставить клиенту запрошенный IP-адрес, или если аренда адреса удаляется администратором, сервер рассылает широковещательное сообщение отмены DHCP (DHCPNAK). При получении такого сообщения соответствующий клиент должен повторить процедуру получения адреса.

Клиент может явным образом прекратить аренду IP-адреса. Для этого он отправляет сообщение освобождения DHCP (DHCPRELEASE) тому серверу, который предоставил ему адрес в аренду. В отличие от других сообщений DHCP, DHCPRELEASE не рассылается широковещательно.

Информация DHCP

Сообщение информации DHCP (DHCPINFORM) предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т. п.) теми клиентами, которым не нужен ди-

намический IP-адрес (то есть адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения (DHCPACK) без выделения IP-адреса.

1.24. Общие сведения о сетевых службах и ресурсах

Пара модулей «клиент - сервер» обеспечивает совместный доступ пользователей к определенному типу ресурсов, например к файлам. В этом случае говорят, что пользователь имеет дело с ***файловой службой (сервисом).*** Обычно сетевая операционная система поддерживает несколько видов сетевых служб для своих пользователей - ***файловую службу, службу печати, службу электронной почты, службу удаленного доступа*** и т. п.

Файловый сервис

Файловый сервис организует удаленный доступ, совместное использование, быстрый перенос и тиражирование, резервное копирование файлов. Этот сервис предусматривает наличие централизованных хранилищ файлов, эффективное использование дискового пространства. Сетевой файловый сервис повышает эффективность хранения и поиска информации.

Основными функциями файлового сервиса являются: передача файлов, хранение файлов и миграция данных, синхронизация изменений файлов, архивирование файлов, (т.н. миграцию данных).

Сетевым файловым сервисом передачи файлов называется любой сервис, который сохраняет, извлекает или перемещает файлы для сетевых клиентов. Этот вид файлового сервиса позволяет обрабатывать данные намного эффективнее, чем это делается с использованием таких носителей информации, как дискеты и ленты, транспортируемые людьми из одного места в другое. Легкость, с которой файлы могут передаваться, не зависит от их размера и расстояния передачи. Сервис передачи файлов не только увеличивает эффективность работы организации, но и обеспечивает доступ к информации, которая недоступна в бессетевой среде.

Важным аспектам применения сервиса передачи файлов является возможность регулировать права доступа к информации, например, разрешить передачу по сети важной информации только уполномоченным лицам. Использование паролей и различных методов шифрования позволяет повысить уровень безопасности файловой системы.

Быстрое увеличение объема информации привело к разработке разнообразных накопителей: магнитных и оптических дисков, дискет, лент и пр.

Различают следующие виды хранения:

- оперативное (online) - на жестких дисках;

- резервное (nearline) - с помощью стримеров с автоматической сменой лент и подобных устройств;
- архивное (offline) - на магнитных лентах и оптических дисках.

По мере старения данных и уменьшения обращений к ним, информацию можно перемещать с дорогих оперативных жестких дисков на более дешёвые долговечные архивные носители. Перемещение данных с одного носителя на другой или из одного места в другое называется ***миграцией данных.*** В файловом сервисе может быть установлен критерий перемещения файлов, например, на основании возраста данных или их размера.

Рабочие место человека в современном мире во все большей степени зависит от мобильных вычислительных средств, в частности, от портативного компьютера и переносных устройств (КПК, смартфон и пр.). Таким мобильным устройствам требуется особый вид файлового сервиса. Мобильные компьютеры не всегда подключены к сети и доступны в ней. Файлы, необходимые пользователю для работы на мобильном компьютере, обычно копируются с сетевого файлового сервера. Однако первоначальный файл на сервере может оказаться измененным другим пользователем, или в программе почтовый клиент могут произойти изменения (получение/отправка почты). Тогда копия на мобильном компьютере будет содержать устаревшую информацию. Чтобы пользователь мобильного компьютера мог узнавать о происходящих на файловом сервере изменениях, необходим особый вид файлового сервиса, называемый синхронизацией изменений файлов.

Синхронизация изменений файлов — это сетевой сервис, который сравнивает время и дату сохранения файлов и определяет, какой из файлов был изменен последним. Этот сервис может также отслеживать, кому принадлежит конкретный файл, и были ли сделаны промежуточные изменения. С помощью этой информации все копии автоматически приводятся в соответствие с последней версией файла. Если изменения были произведены в двух копиях файла, сервис синхронизации изменений файлов должен быть в состоянии читать информацию, содержащуюся в похожих файлах, и интеллектуально объединять изменения.

Архивирование, или дублирование файлов представляет собой создание на случай аварии копий-дубликатов важных данных на магнитных лентах или других носителях. Архивирование файлов упрощается при объединении всех устройств хранения данных. На основе централизованного хранения файлов и управления ими один администратор может дублировать информацию, хранящуюся на нескольких файл-серверах. Кроме того, специализированные накопители и программное обеспечение, используемые в вычислительных сетях, позволяют собирать данные большого объема и управлять ими.

Сервис печати

Сервис печати— это сетевые приложения, которые управляют доступом к принтерам и факсимильному оборудованию. Сервис печати принимает запросы заданий печати, интерпретирует форматы заданий печати и конфигурации принтеров, управляет очередями печати и организует взаимодействие с сетевыми принтерами и факсимильным оборудованием для сетевых клиентов.

Сервис печати позволяет пользователям коллективно получать доступ к устройствам печати через ограниченное количество интерфейсов (как правило, устройство печати имеет один, реже два интерфейса). Совместно использовать дорогостоящее специализированное оборудование печати, уменьшать количество требуемых принтеров, размещать принтеры в наиболее удобных местах, устранять ограничения расстояний между компьютером пользователя и устройством печати, организовывать и обрабатывать очереди запросов на печать.

Аппаратное решение, призванное облегчить пользователям сети доступ к принтерам, представлено компанией **D-Link,** семейством принт-серверов **DPR.**

Рис. 114. Пример использования принт-сервера D-Link.

Сервис сообщений

Сервис сообщений позволяет организовать обмен сообщениями между пользователями сети, оперируя текстовой, графической, звуковой и видеоинформацией. В отличие от файлового сервиса, сервис сообщений тесно связан с коммуникационным взаимодействием между пользователями, сетевыми приложениями и документами. Сервис сообщений помогает пользователям передавать сообщения, генерируемые компьютерами и людьми, работать с объектно-ориентированным программным обеспечением и объектами, распределенными по сети, маршрутизировать и разделять данные с помощью приложений автоматизации ***документооборота*** и ***объектно-связанных*** документов, организовывать и поддерживать каталоги информации о пользователях и устройствах. Сервис сообщений предоставляет пользователю возможность не только передавать, но и сохранять все сообщения. В некоторых случаях он используется ком-

пьютерами (серверами сети), чтобы извещать пользователей о наступлении каких-либо событий. ***Электронная почта*** является одной из реализаций сервиса сообщений и представляет собой электронную передачу сообщений между двумя или несколькими компьютерами в сети.

Электронная почта способна передавать не только текстовые сообщения, но и графические, видео- и звуковые данные. Особый вид почты - речевая или голосовая почта. Системы речевой почты — это специализированные компьютеры, включенные в сеть. Объектно-ориентированные приложения - это компьютерные программы, которые объединяют меньшие приложения для выполнения сложных задач.

Приложения для рабочих групп используются для управления документооборотом. Приложения управления документооборотом интеллектуально маршрутизируют формы, замечания и документы между клиентами сети и используются для управления многопользовательскими распределенными деловыми процессами. Для организации службы сообщений применяется ***сервис каталога***. Серверы сети регулярно обмениваются изменениями, происходящими в каталогах, с помощью межсерверных сообщений. Благодаря синхронизации информации об объектах сети, хранящейся на разных серверах, пользователю при отправке сообщения не нужно знать местоположение объекта, указывать его адрес и определять маршрут - достаточно лишь указать имя объекта назначения.

Сервис приложений

Сервис приложений— это вид сетевого сервиса, который запускает программы для сетевых клиентов. Сервис приложений дает возможность пользователям совместно использовать не только данные (как в файловом сервисе), но и вычислительную мощность сервера. Задача сервиса приложений - координация оборудования и программного обеспечения для работы приложений и утилит на наиболее подходящей платформе.

Главные преимущества сервиса приложений — специализация серверов, расширяемость и развитие. Сервер приложений, если он выделен для выполнения конкретных задач, может быть оптимизирован для их решения за счет использования специализированного оборудования. В результате увеличивается быстродействие, повышается надежность и появляется возможность лучше организовывать контроль целостности и защиты данных. Одним из наиболее распространенных видов серверов приложений являются ***базы данных «клиент-сервер».***

Немаловажна и возможность наращивания вычислительной мощности сервера приложений, так как это приводит к одновременному увеличению производительности всех клиентов. Сетевой сервис приложений может обеспечить недорогие варианты наращивания вычислительной мощности. Преимущества расширяемости и развития зависят от возможности применения той же опера-

ционной системы и приложений на новом компьютере или, наоборот, тех же приложений в новой операционной системе. При этом может не потребоваться обновление аппаратных и программных средств клиента, так как увеличение производительности всей системы достигается увеличением производительности только одного ее компонента — сервера.

Сервис баз данных

Предназначен для организации централизованного хранения, поиска и обеспечения защиты данных. Этот сервис обеспечивает хранение, восстановление и поиск информации в базах данных на серверах, позволяя сетевым клиентам управлять данными и их представлением. Приложения баз данных, позволяющие клиентам запрашивать данные у специализированных серверов, называются ***базами данных «клиент-сервер».*** Приложения баз данных «клиент-сервер» распределяют и оптимизируют задачи, составляющие процесс запроса и предоставления данных.

Этот сервис реализуется серверами баз данных и программно-аппаратными комплексами. В качестве примера можно привести, серии дисковых накопителей DNS, DSN от компании D-Link.

Дисковый массив ***D-Link xStack Storage*** 4x1GbE iSCSI SAN **DSN-1100-10** разработан для надежного хранения данных в сетях малых и средних предприятий. DSN-1100, как и более старшее устройство в линейке дисковых массивов D-Link - DSN-3200-10 построено на одинаковой аппаратной платформе System-on-a-Chip (SoC). Система реализована на iSCSI System-on-a-Chip (SoC) 10 Гбит, что позволяет обрабатывать до 80 тысяч операций ввода/вывода в секунду, и обеспечивают возможность установки 5 x 1ТБ дисков (DSN-1100 поддерживает диски большего объема).

Сетевой сервис баз данных выполняет следующие задачи:

- оптимизирует хранение, поиск и извлечение записей баз данных;
- снижает время доступа пользователей к информации;
- управляет территориальным местоположением информации в сети;
- обеспечивает защиту данных;
- логически организует данные подразделений организации.

Координация распределенных данных. В крупных организациях возможно разделение задач и данных между несколькими подразделениями. При со-

вместном использовании информации необходимо знать, кто и какими данными управляет и где они должны храниться. Сетевой сервис баз данных для достижения прозрачного совместного использования данных применяет тактику распределения данных. Он разделяет управление частями базы данных между вычислительными системами различных подразделений. Система управления базой данных (СУБД), координируя изменения, происходящие в различных вычислительных системах, ответственна за то, чтобы база данных выглядела как единая логическая сущность.

Пример реализации программно-аппаратного комплекса реализующий сервис баз данных, представлен компанией **D-Link**, семейством устройств **DNS и DSN.** В линейке этик устройств одно и много дисковые решения, позволяющие организовать безопасное и надёжное хранение данных.

Тиражирование (репликация)

Информация из локальных баз данных обычно извлекается намного быстрее, чем из удаленных, так как для этого используется высокоскоростная локальная сеть и не загружаются каналы удаленного доступа. Поэтому пользователи предпочитают работать с локальными данными. Чтобы обеспечить такую возможность, нужно создать несколько копий наборов данных и расположить их в непосредственной близости от потребителей этой информации. Но если существует более одной копии базы данных, возникает проблема синхронизации изменений, вносимых в эту базу, - содержимое всех копий должно быть идентичным.

Тиражирование (replication) создает и синхронизирует несколько копий базы данных в сети. В настоящее время программное обеспечение баз данных использует два метода синхронизации реплицированных данных:

Тиражирование главной базы данных. Все изменения вносятся только в главную базу данных, а СУБД обеспечивает внесение изменений, записанных в главную базу, во все ее копии.

Тиражирование локальных баз данных. Ответственность за запись дополнений и изменений возлагается на локальные базы данных. Локальная часть СУБД вносит изменения в свою локальную базу, а затем должна скоординировать внесенные дополнения и изменения со всеми остальными копиями.

Система управления базами данных (СУБД) - специализированная программа (чаще комплекс программ), предназначенная для организации и ведения базы

Современные тенденции развития информационно вычислительных сетей

Главной тенденцией развития вычислительной техники в настоящее время является дальнейшее расширение сфер применения компьютерной техники и, как следствие, переход от отдельных машин к их системам – распределённым вычислительным системам и комплексам разнообразных конфигураций с широким диапазоном функциональных возможностей и характеристик.

Сегодня мы являемся свидетелями смены основной информационной среды общества. Удельные объемы информации, получаемой обществом по компьютерным сетям возрастают из года в год, в то же время объёмы информации получаемые традиционными информационными каналами (радио, телевидение, печать) неуклонно снижаются. Можно сказать, что традиционные средства распространения информации интегрируются в компьютерные сети. Примеры тому – радио и теле вещание в информационно вычислительных сетях, газеты в электронном виде.

Наиболее перспективные, территориально распределенные многомашинные вычислительные сети (вычислительные системы) - ориентируются не столько на вычислительную обработку информации, сколько на коммуникационные информационные услуги: электронную почту, системы телеконференций, передача голоса и информационно-справочные системы. И главными требованиями к информационно вычислительным сетям становятся скорость передачи данных и надёжность всей инфраструктуры в целом. Уходят в прошлое такие технологии как ADSL , появляются новые ориентированные на волоконно-оптическую и беспроводную среду передачи данных.

Потребность в увеличении пропускной способности на уровне доступа (проблема т.н. «первой мили») приобретает первоочередную важность. Это объясняется тем, что уже сегодня одной семье могут понадобиться, к примеру, четыре канала телевидения высокой четкости или широкоэкранное цифровое изображение. Стандарт **IEEE 802.3av** представляет собой расширение стандарта 802.3ah, EFM. Ратифицированный в 2009 г. он определяет технологию **10 Гбит/с EPON**. Между коммутационным узлом и домашней сетью развертывается распределительная сеть, по которой через оптическое волокно подается 10 Гбит/с для 32 домохозяйств.

Продуктовая линейка D-Link включает различные продукты GE-PON, в том числе коммутатор GE-PON DPN-3012-E, а также абонентские (оконечные) устройства с одним или несколькими портами. Серии DPN-301 (DPN-301/L/T) и DPN-304 (DPN-304/L/T) поддерживают дальность передачи до 10км или 20км. DPN-301/T, DPN-304/T обеспечивают дальность передачи по оптическому кабелю до 10км, в то время как DPN-301L, DPN-304L – до 20км. DPN-301T также поддерживает подключение CATV.

Рис. 115. DPN-3012-E

Рис. 116. DPN-304

Для того чтобы удовлетворить потребность в еще большей пропускной способности, в ноябре 2006 г. проектная группа IEEE P802 учредила «группу исследования высоких скоростей» (High Speed Study Group), которая в декабре 2007 г. под эгидой рабочей группы **IEEE 802.3ba** получила «запрос на авторизацию проекта» (Project Authorization Request, PAR) о разработке стандарта Ethernet на **40/100 Гбит/с** со следующими задачами:

- поддержка исключительно полнодуплексного режима;
- поддержка обоих форматов кадров (CSMA/CD и Ethernet V2.0);
- сохранение минимальной и максимальной длины кадров;
- поддержка оптических транспортных сетей (Optical Transport Network, OTN);
- скорость передачи данных 40 и 100 Гбит/с.

Результатом деятельности проектной группы IEEE P802, стало принятие этого стандарта в 2010 году.

В области беспроводных технологий передачи данных, организация IEEE объявила о планах по разработке стандарта ***802.11ac*** для Wi-Fi, который обещает стать одним из ключевых нововведений в сфере беспроводной передачи данных в ближайшие два года. Ожидается, что новый стандарт, будет использовать каналы шириной 80 МГц или даже 160 МГц. В перспективе разработка сможет обеспечить пропускную способность эквивалентную Gigabit Ethernet: 1 Гбит/с, что более чем в три раза превышает характеристики недавно утвержденного стандарта 802.11n (600 Мбит/с). На данный момент проект находится на стадии

обсуждения. Предположительно испытания начнутся в конце 2011 года, а окончательное утверждение стандарта произойдет в декабре 2012.

Вместе с тем пока Wi-Fi только планирует подобраться к отметке 1 Гбит/с, организация ***Wireless Gigabit Alliance***, ответственная за продвижение беспроводной 60-ГГц технологии, уже заявила о завершении работ над первой версией спецификации ***WiGig(802.11ad).***. Новый стандарт предусматривает более чем в десять раз большую пропускную способность по сравнению с самыми быстрыми современными сетями Wi-Fi. При этом, что немаловажно, сохранена обратная совместимость с существующими на рынке Wi-Fi устройствами.

Несмотря на высокую производительность технологии ***WiGig***, она уступает современному Wi-Fi по дальности действия. Если Wi-Fi в помещениях позволяет связывать устройства на расстоянии в несколько десятков метров, то ***WiGig*** гарантирует качественное соединение на расстоянии всего 10 метров. Впрочем, во многих случаях этого может оказаться вполне достаточно для организации домашней беспроводной сети. Напомним, недавно представленный стандарт ***WHDI 1.0*** имеет дальность связи в тридцать метров, но его максимальная скорость передачи данных не превышает 3 Гбит/с.

Кроме того организация ***WHDI LLC*** заявила о завершении работ над спецификацией беспроводного интерфейса ***Wireless Home Digital Interface (WHDI).*** Новый стандарт предусматривает передачу высококачественного несжатого видео 1080p/60 Гц на расстояние до ста футов (более тридцати метров), при этом стены – не помеха. WHDI позволяет пользователям строить беспроводные HD-сети у себя дома и наслаждаться новейшими интерактивными сервисами. Источниками видео высокого разрешения, которое передается на телевизоры (а их в квартире может быть несколько), могут выступать самые разнообразные устройства, включая настольные персональные компьютеры, ноутбуки и нетбуки, смартфоны, карманные плееры. Подключение устройств с логотипом WHDI удобное и простое, и не требует прокладки кабелей.

Спецификацией предусмотрена пропускная способность сети до трёх гигабит в секунду в 40-МГц полосе 5-ГГц диапазона. Задержка сигнала составляет менее одной миллисекунды. Также в WHDI предусмотрена поддержка защиты контента HDCP 2.0.

Разработчики перспективных технологий кроме увеличения пропускной способности информационно вычислительных систем стремятся повысить эффективность их использования. С этой целью, например, разработан стандарт ***802.3az, энергоэффективные сети Ethernet (Energy Efficient Ethernet).*** Лавинообразно растущий сетевой сегмент может внести значительный вклад в экономию энергии. Суть идеи заключается в переводе соединений в режим низкого энергопотребления (Low Power), когда передавать данные не требуется. Режим Low Power реализуется путем уменьшения скорости передачи вплоть до нуля. И хотя этот стандарт официально ратифицирован в октябре 2010 года, многие производители сетевого оборудования учли его требования в своих новых продуктах.

В частности, компания D-Link реализовала данный стандарт на семействе гигабитных коммутаторов под маркой «Green Ethernet».

Рис. 117. DES-1210-28

4. ПРИЛОЖЕНИЕ А. Примерные схемы применения оборудования D-Link.

Формат: Список

Предположим, что в неком учреждении (или частном строении) необходимо организовать локальную вычислительную сеть с использованием беспроводных технологий. В этой сети планируется создание системы *видео наблюдения*, *файлового хранилища*, совместного использования *принтера*, а так же использование технологий передачи данных для просмотра мультимедиа контента. Дополнительное условие – подключение видеокамеры наблюдения в удалённом обособленном месте, например в чердачном помещении (подвале, крытый металлический ангар, мастерские и т.п.).

Все настройки оборудования D-Link будем осуществлять используя WEB интерфейс. В качестве программ будем использовать популярные интернет браузеры. Для примера одно из устройств настроим используя операционную систему Linux и соответственный браузер. Сразу хочется отметить , что сетевое оборудование компании D-Link , не предъявляет каких то специальных требований в выборе операционных систем., поэтому пользователи вольны в выборе программного обеспечения .

В реализации данного задания будем использовать следующее оборудование:

DIR-855 - беспроводной 2,4 ГГц (802.11n) 4-х портовый гигабитный маршрутизатор, до 300 Мбит/с;

DCS-2121 - беспроводная мегапиксельная Интернет-камера;

DNS-323 - сетевой дисковый массив с 2 отсеками для жестких дисков;

DPR-1020 - многофункциональный USB принт-сервер;

DSM-320RD - беспроводной медиа-плеер с DVD-плеером и Card-ридером;

DHP-300 - сетевой адаптер для электрических сетей;

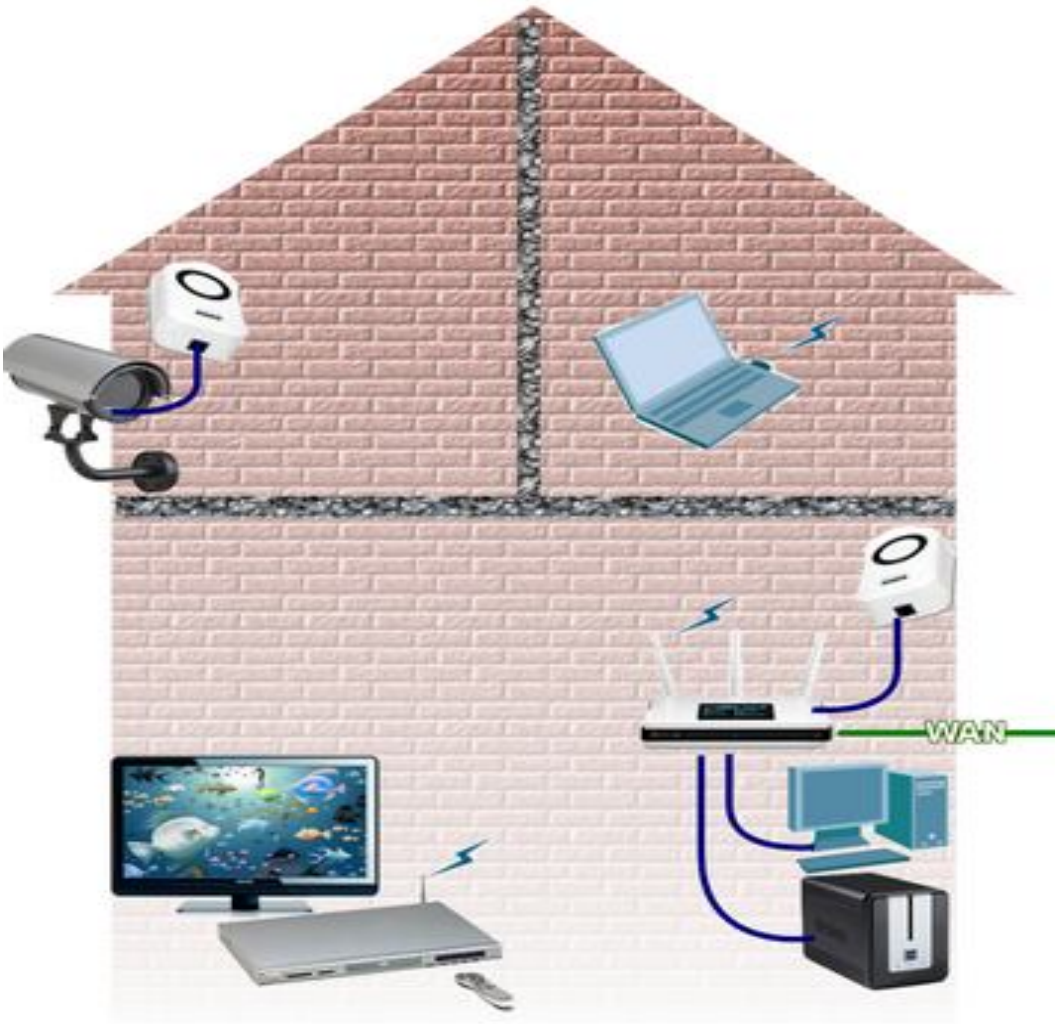


Рис. 118. Предполагаемая схема домашней ЛВС

Из перечисленного выше оборудования становится ясно, что центральным устройством будет скорее всего - DIR-855. Поэтому задача номер один – настроить это устройство, в том числе настроить и беспроводную связь. Кратко ознакомимся с этим устройством:

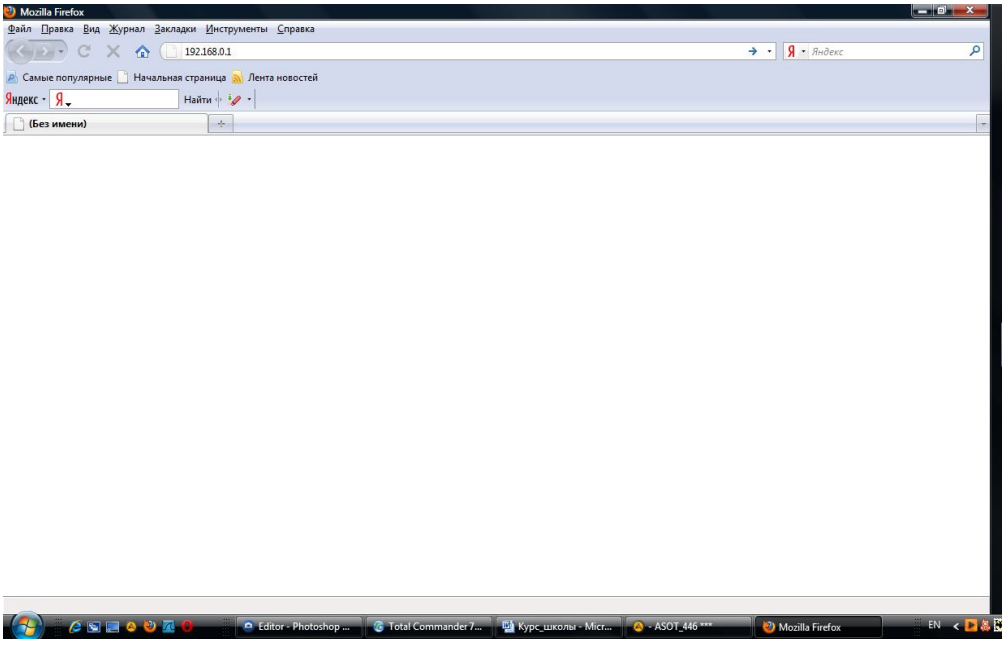
Гигабитный маршрутизатор DIR-855 серии XTREME N TM DUO (802.11n) обеспечивает скорость до 300 Мбит/с , при этом обратно совместим с устройствами 802.11g и 802.11b. Благодаря технологии XTREME N TM и трем внешним антеннам, этот маршрутизатор обеспечивает расширенный радиус действия беспроводной сети для больших домов и офисов, а также для пользователей, работающих с приложениями, требовательными к полосе пропускания. Устройство позволяет создать безопасную беспроводную

сеть для совместного использования фотографий, файлов, музыки, видео, принтеров и сетевых массивов.

DIR-855 поддерживает одновременно два частотных диапазона 2,4 ГГц и 5,0 ГГц и оснащен ЖК-дисплеем и встроенным коммутатором с 4 портами 10/100/1000 Мбит/с, к которому можно подключать проводные гигабитные устройства для онлайн игр и быстрой передачи файлов. В качестве WEB-браузера в данном случае используем программу Mozilla Firefox.

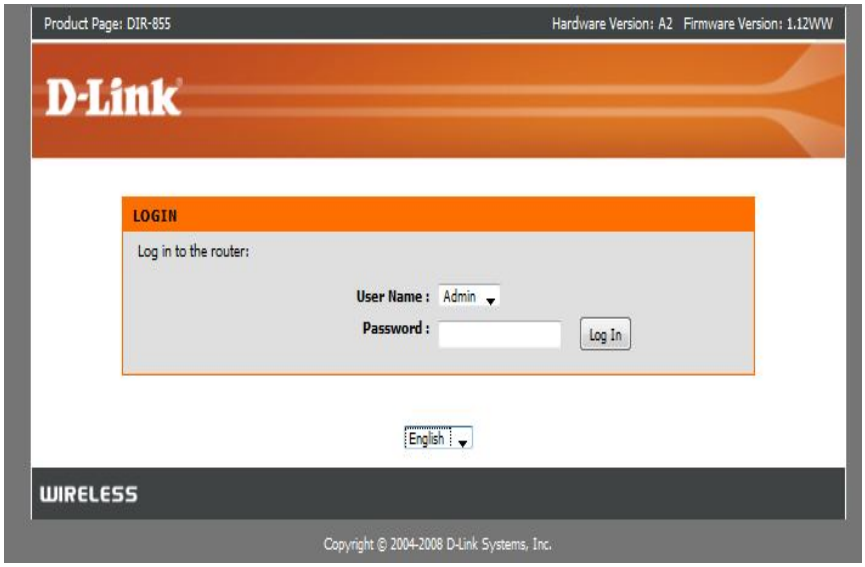
Перед началом установки, читаем прилагаемую документацию.

Запускаем интернет – браузер, в данном случае , это Mozilla Firefox. В адресной строке набираем : 192.168.0.1 нажимаем кнопку «Enter».

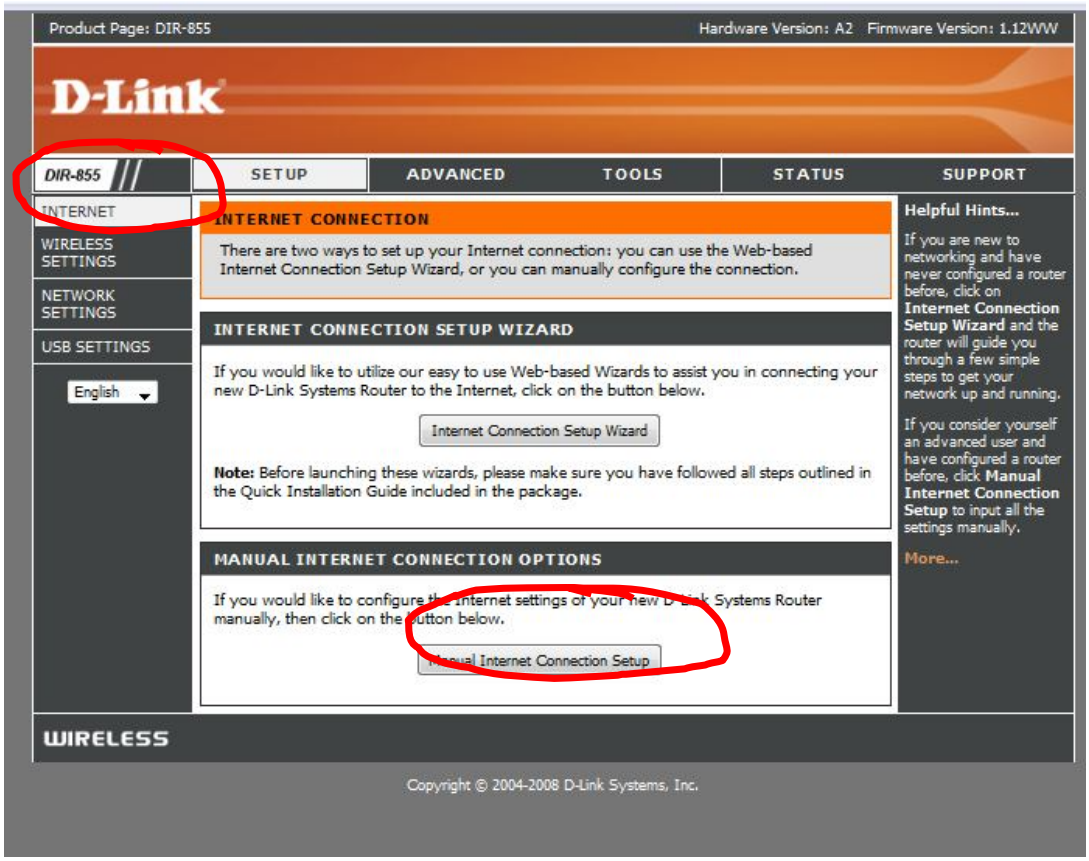


в появившемся окне приветствия в поле « User name» вводим : admin

поле «password» оставляем пустым и нажимаем кнопку «Enter».



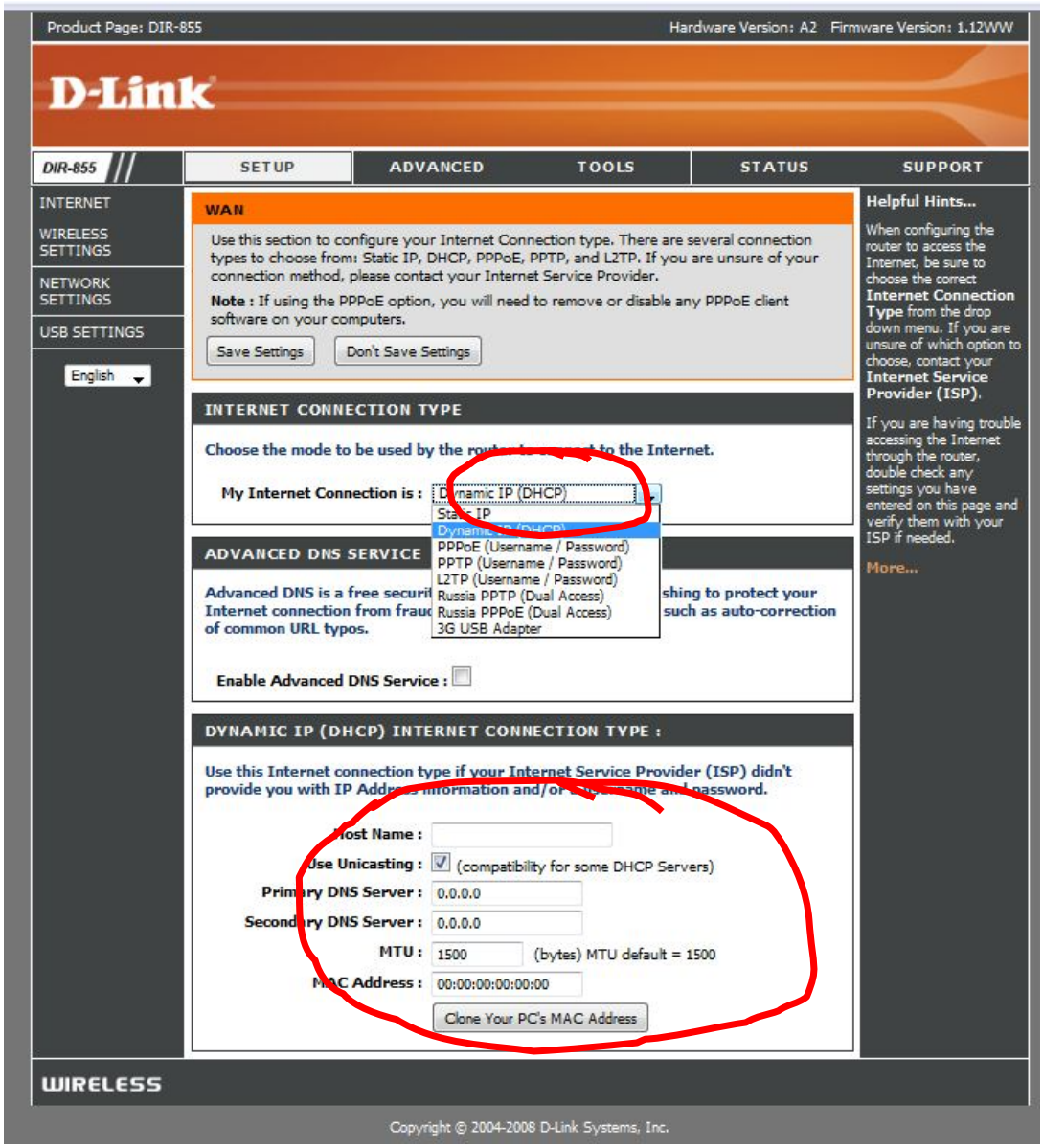
Если предыдущие манипуляции были произведены верно, то откроется главная страница настройки данного устройства. Выбираем в меню настройки: ИНТЕРНЕТ (верхняя строчка в боковом меню, с лева), и нажимаем « Manual Internet Connection Setup» (ручная настройка ИНТЕРНЕТ соединения)



Прежде всего мы должны знать настройки ИНТЕРНЕТ, чтобы ввести их в устройство. Эти данные обычно записаны в договоре на предоставление услуг доступа к ИНТЕРНЕТ, с провайдером (поставщиком услуги доступа). Так же в договоре описан и способ доступа , а так же пароли и данные о маршрутизаторе провайдера, серверах DNS и другая информация касающееся настроек доступа. Рассмотрим два способа соединения с провайдером:

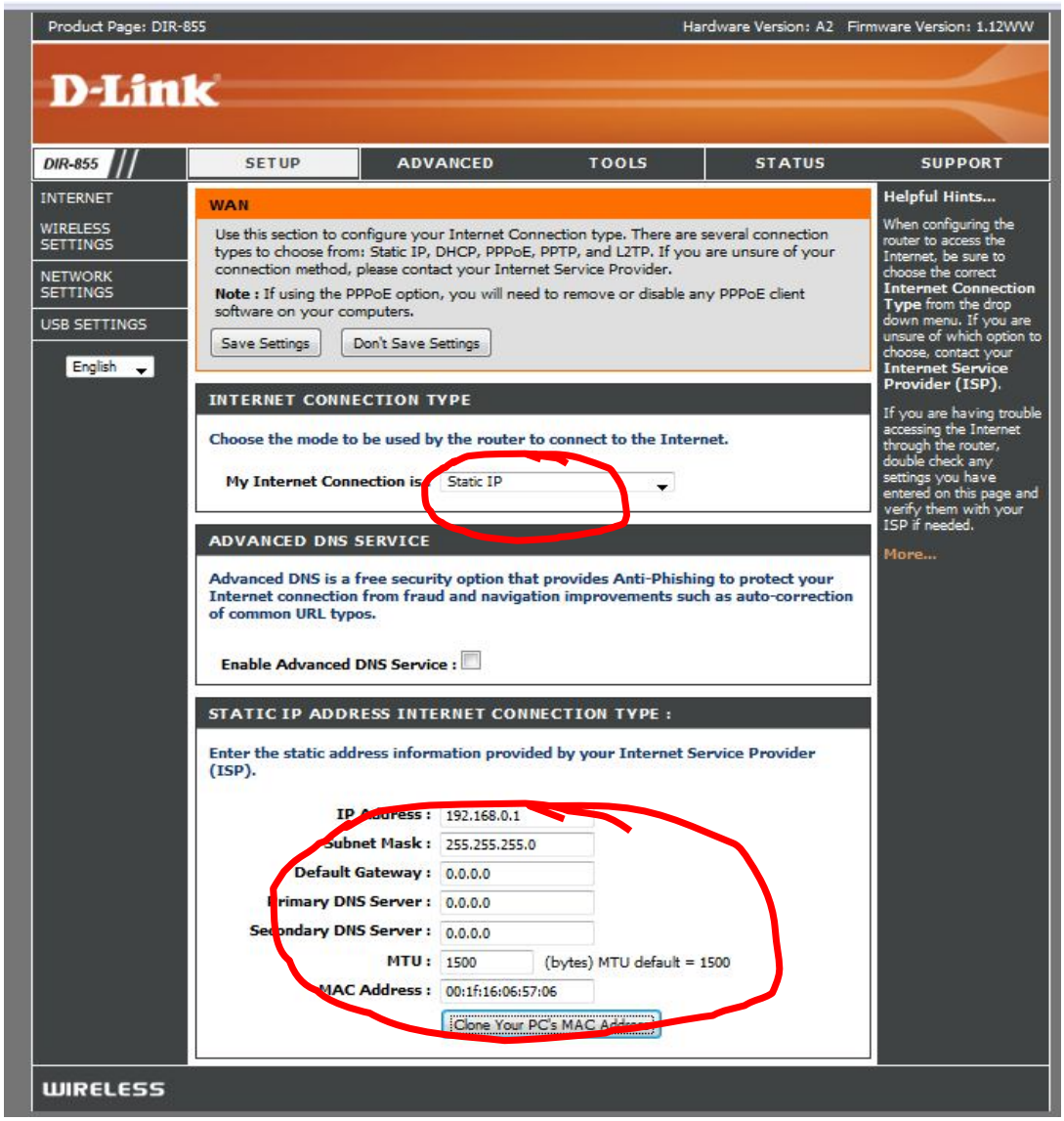
Случай, когда все основные настройки получаем автоматически .

Итак, в ниспадающем меню « INTERNET Connection Type» выбираем необходимый режим работы, в данном случае это «Dynamic IP», заполняем поля касающиеся имени , серверов DNS , и после этого нажимаем на кнопку «Save settings»



Вариант подключения к провайдеру, когда IP-адрес присвоен статический , и все настройки необходимо ввести в ручную . Итак, в ниспадающем меню «INTERNET Connection Type» выбираем пункт «Static IP», ниже заполняем поля касающиеся нашего IP-адреса, адресов маршрутизатора(шлюза) провайдера (gateway), серверов DNS (все эти данные содержатся, как правило, в договоре на оказание услуги доступа в ИНТЕРНЕТ) и после этого нажимаем на кнопку «Save settings». Как и в предыдущем случае , через несколько секунд устройство перезагрузится с новыми настройками.


Product Page: DIR-855
Hardware Version: A2 Firmware Version: 1.12WW
D-Link
DIR-855
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS
USB SETTINGS
English
WAN
Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP, and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.
Note : If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.
Save Settings
Don't Save Settings
INTERNET CONNECTION TYPE
Choose the mode to be used by the router to connect to the Internet.
My Internet Connection is :
Static IP
Static IP
Dynamic IP (DHCP)
PPPoE (Username / Password)
PPTP (Username / Password)
L2TP (Username / Password)
Russia PPTP (Dual Access)
Russia PPPoE (Dual Access)
3G USB Adapter
ADVANCED DNS SERVICE
Advanced DNS is a free securit
shing to protect your Internet connection from fraud
such as auto-correction of common URL typos.
Enable Advanced DNS Service :
STATIC IP ADDRESS INTERNET CONNECTION TYPE :
Enter the static address information provided by your Internet Service Provider (ISP).
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
MTU : 1500 (bytes) MTU default = 1500
MAC Address : 00:1f:16:06:57:06
Clone Your PC's MAC Address
Helpful Hints...
When configuring the router to access the Internet, be sure to choose the correct Internet Connection Type from the drop down menu. If you are unsure of which option to choose, contact your Internet Service Provider (ISP).
If you are having trouble accessing the Internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.
More...
WIRELESS

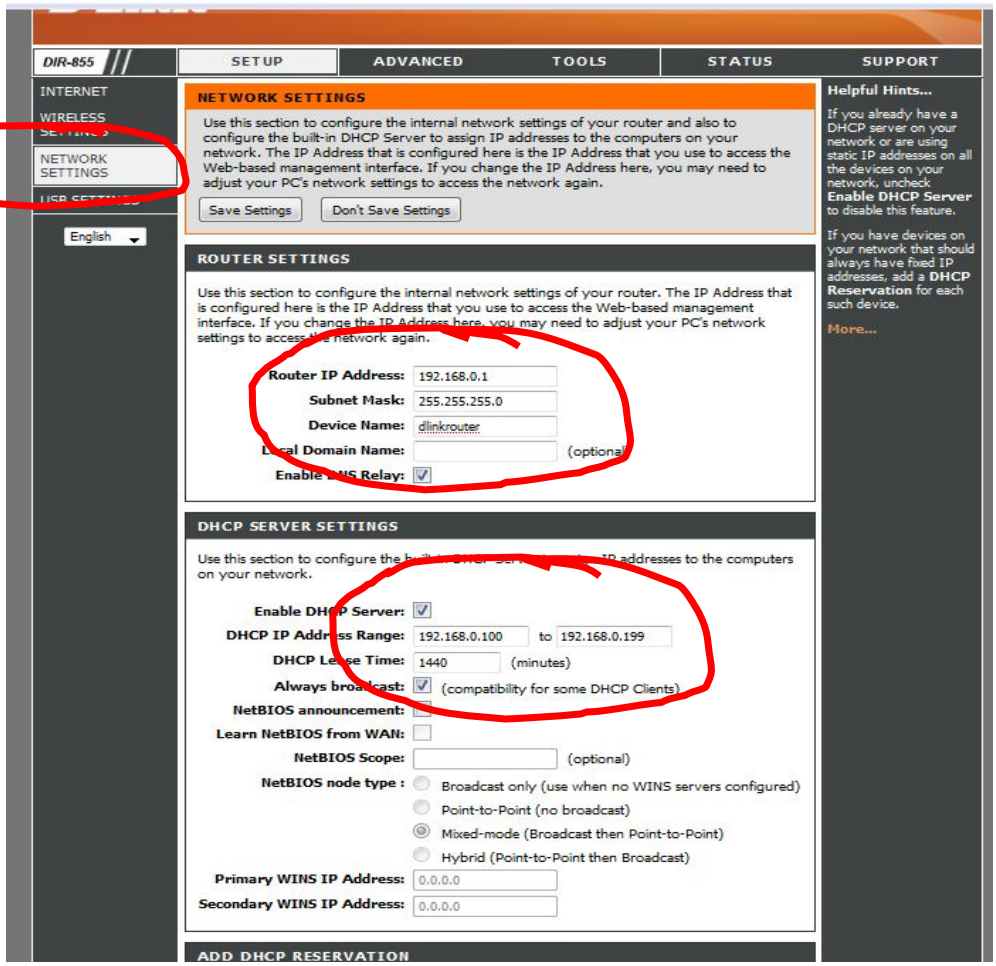


Рассмотренные два варианта подключения к сети ИНТЕРНЕТ, не являются обязательными и окончательными. Настройки подключения к ИНТЕРНЕТ вводятся в зависимости от предлагаемого провайдером типа подключения .

После того как , настройки подключения к ИНТЕРНЕТ установлены, необходимо ввести настройки локальной вычислительной сети:

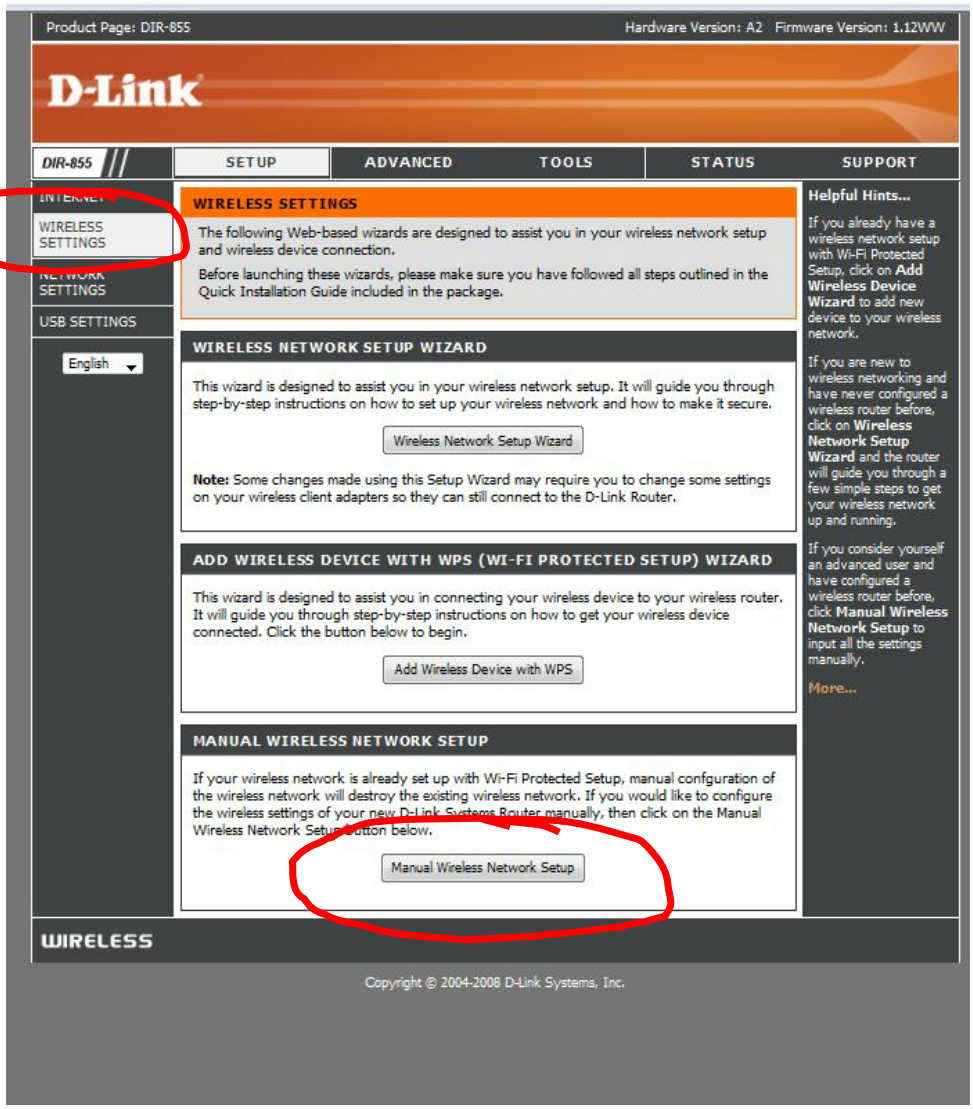
Нажимаем на боковую кнопку «Network Settings», и устанавливаем локальный IP-адрес, маску подсети, имя устройства , при необходимости имя домена. Так же , если мы хотим , чтобы подключённое к этому устройству оборудование автоматически получали сетевые адреса, активируем DHCP сервер, указываем при этом диапазон адресов выдаваемых устройствам. Необходимо

помнить , что если мы хотим активировать в своей сети службу DHCP, то мы должны указать IP- адрес данного устройства на всём своём оборудовании как шлюз по умолчанию (default gateway). Если необходимо производим другие настройки , и после всего этого нажимаем на кнопку «Save settings». Как и в предыдущем случае , через несколько секунд устройство перезагрузится с новыми (теперь уже и LAN) настройками.



Мы помним, что рассматриваемое нами устройство имеет в своём составе средства беспроводной связи. Поэтому настроим и этот раздел.

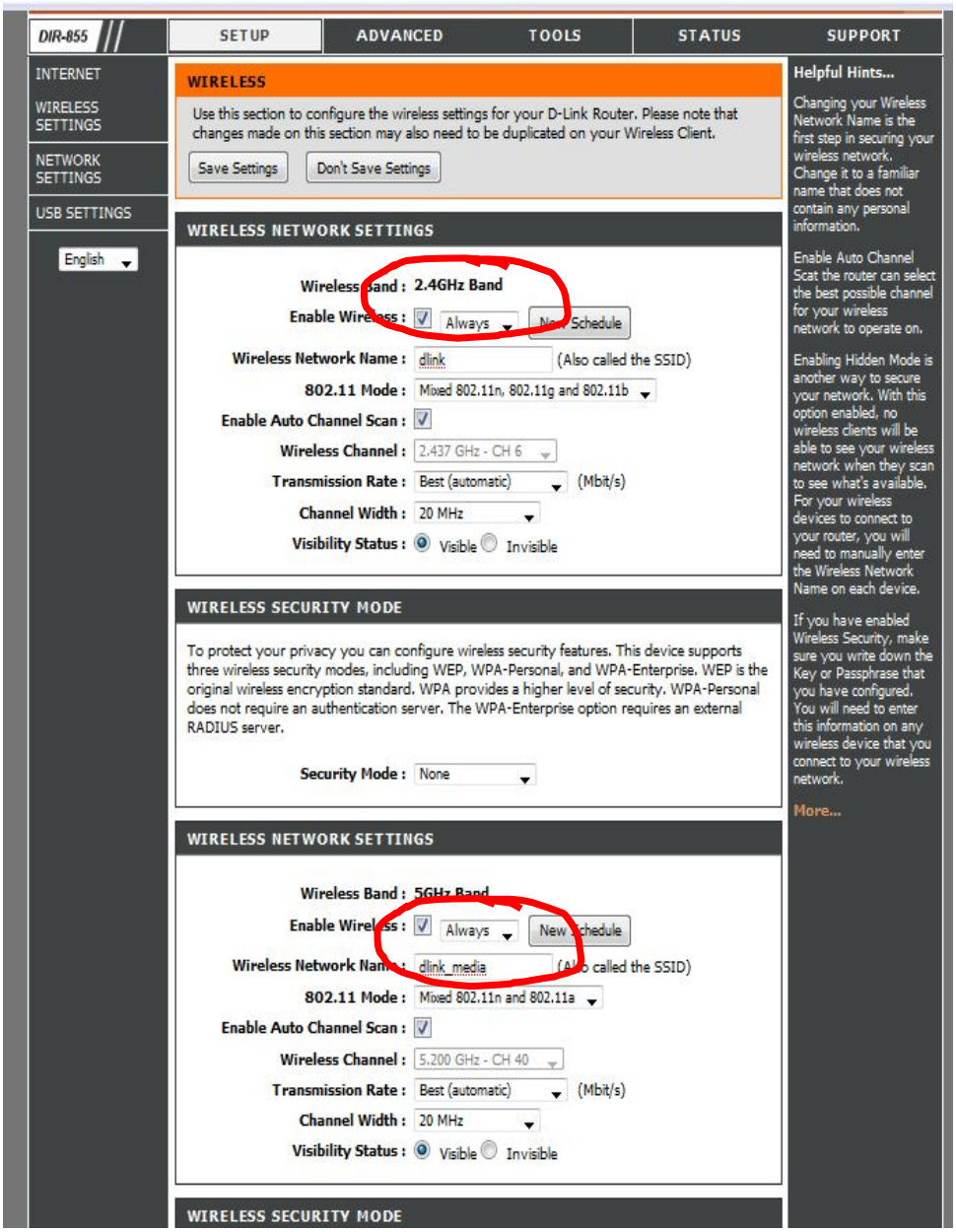
Нажимаем на боковой панели кнопку «Wireless Setting» , и после этого кнопку « Manual Wireless Network Setup»



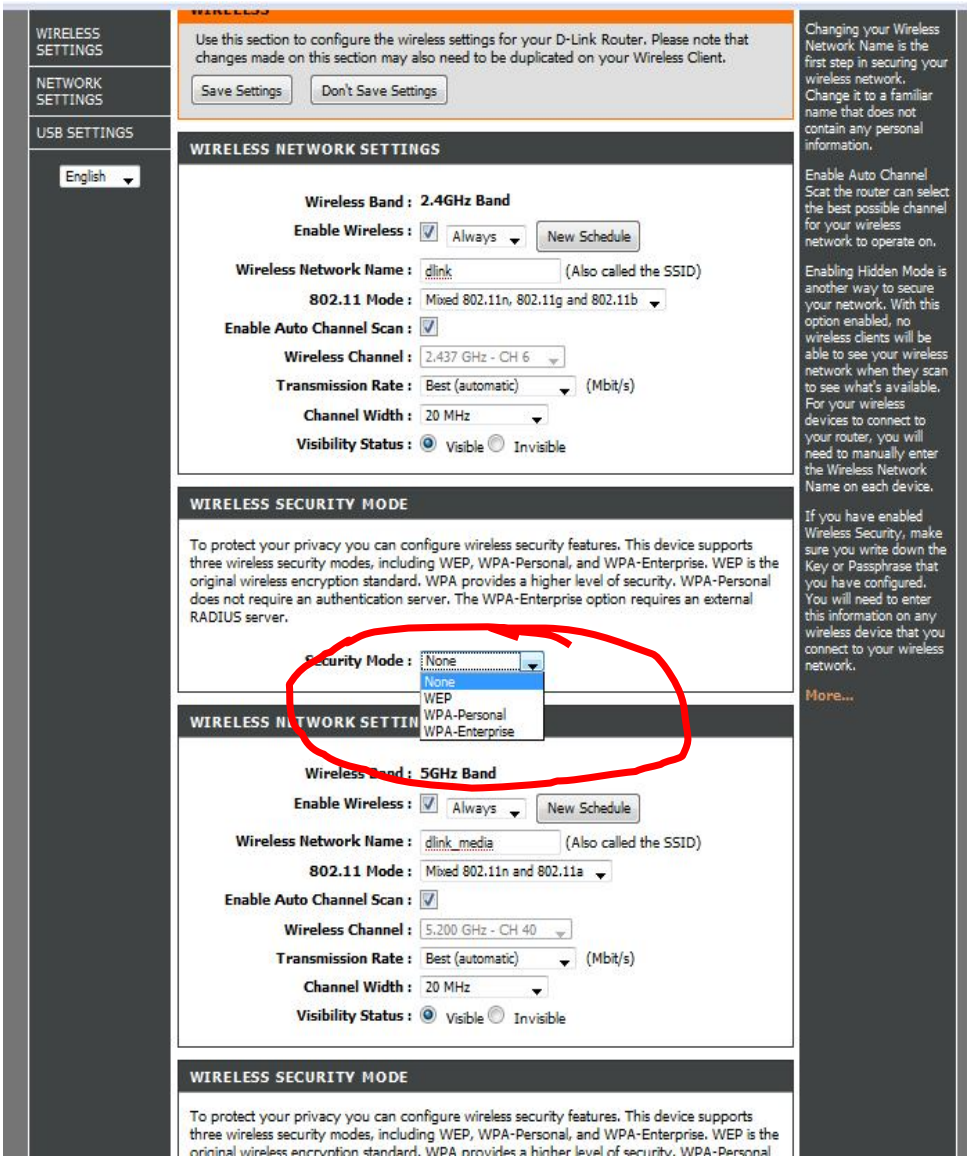
Данное устройство поддерживает два частотных диапазона 2,4 и 5 ГГц, нужно помнить , что настраиваются эти диапазоны отдельно друг от друга (в том числе и раздел безопасности) , и по необходимости использования. Т.е. если , например, используется только диапазон 2,4 ГГц, то диапазон 5 ГГц вообще не активируется.

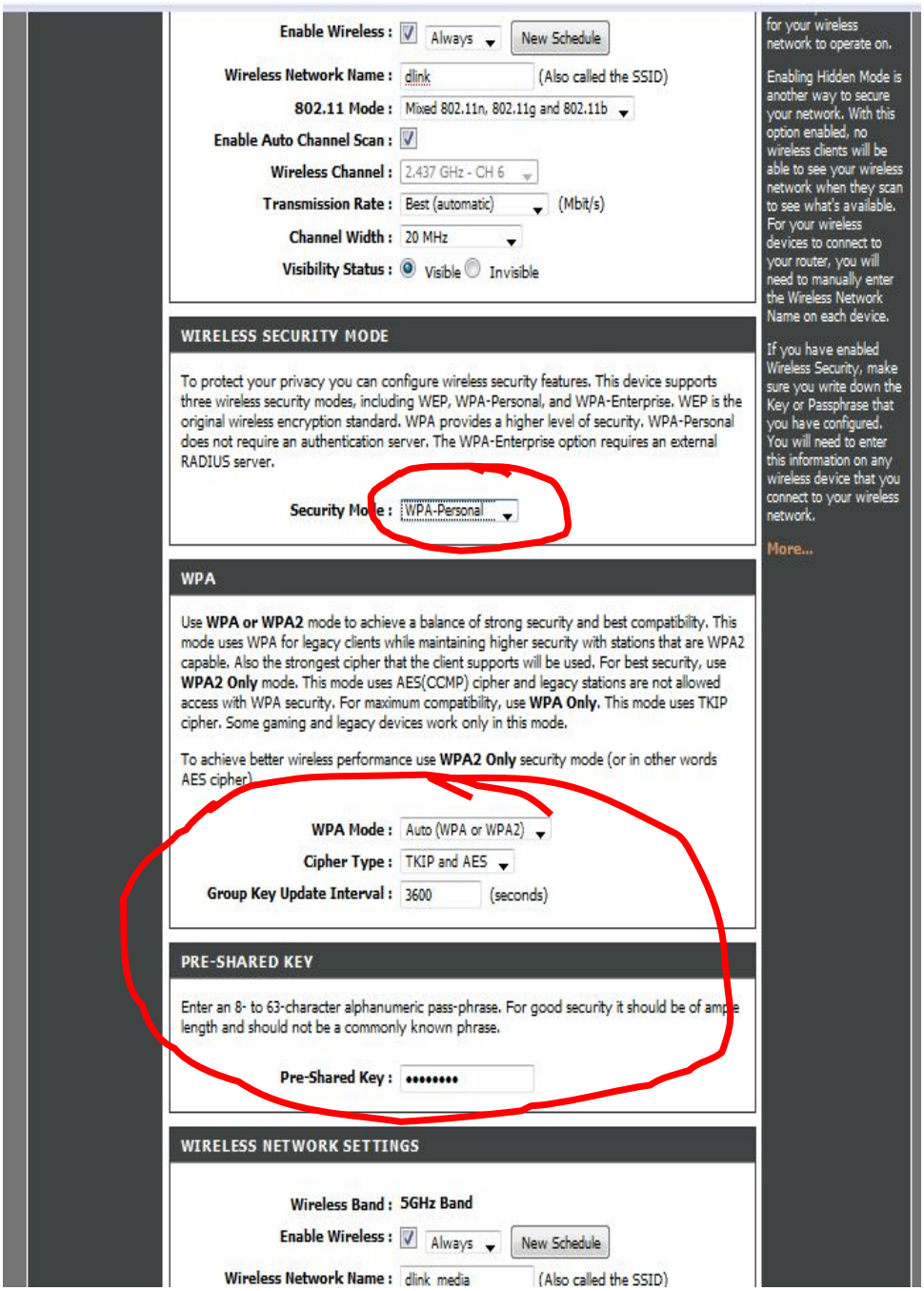
В данном примере используются оба частотных диапазона .

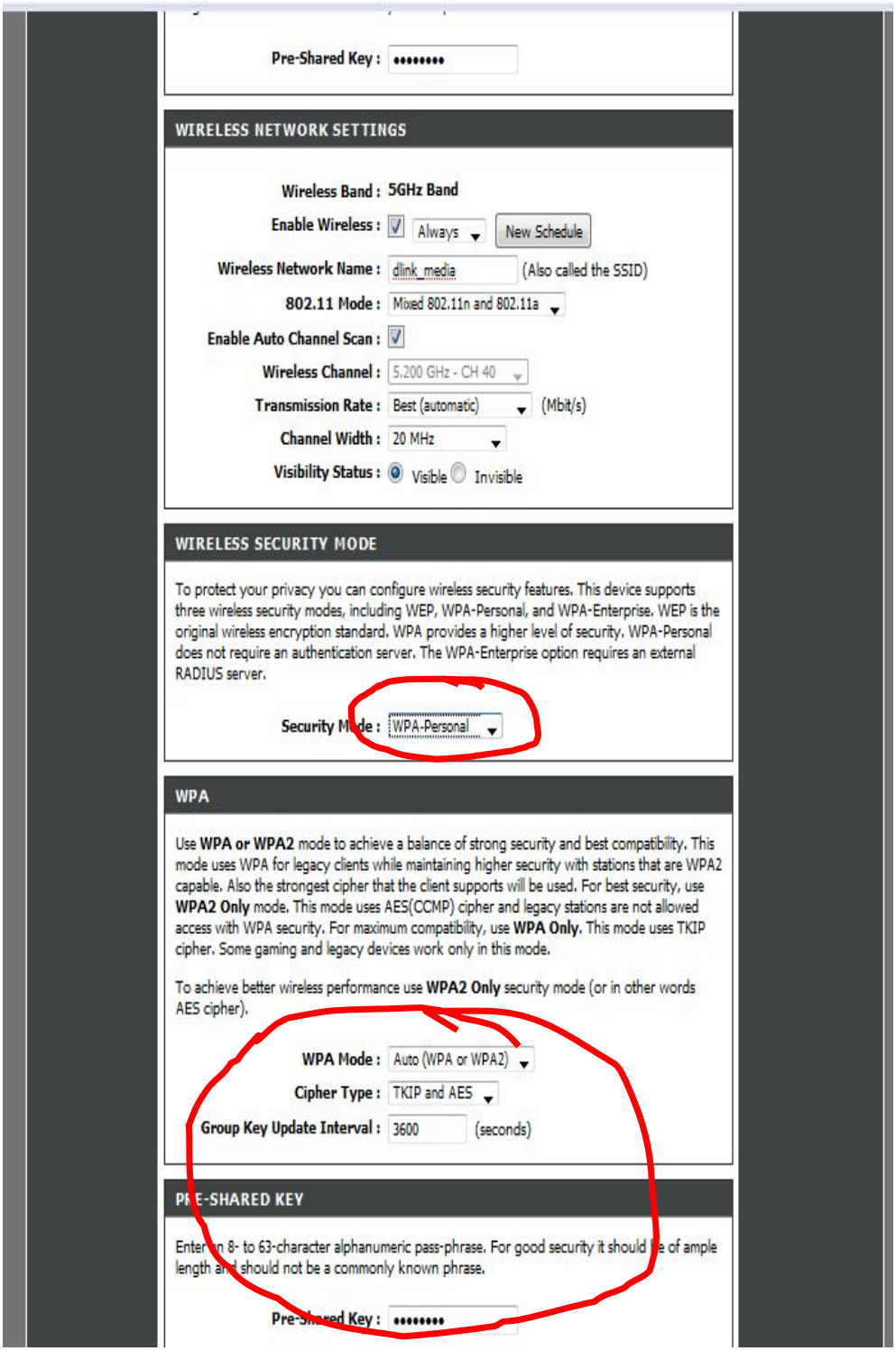
Итак, произведём настройки беспроводной сети: указываем имя сети , режим работы точки доступа (в зависимости от имеющихся абонентских беспроводных устройств)

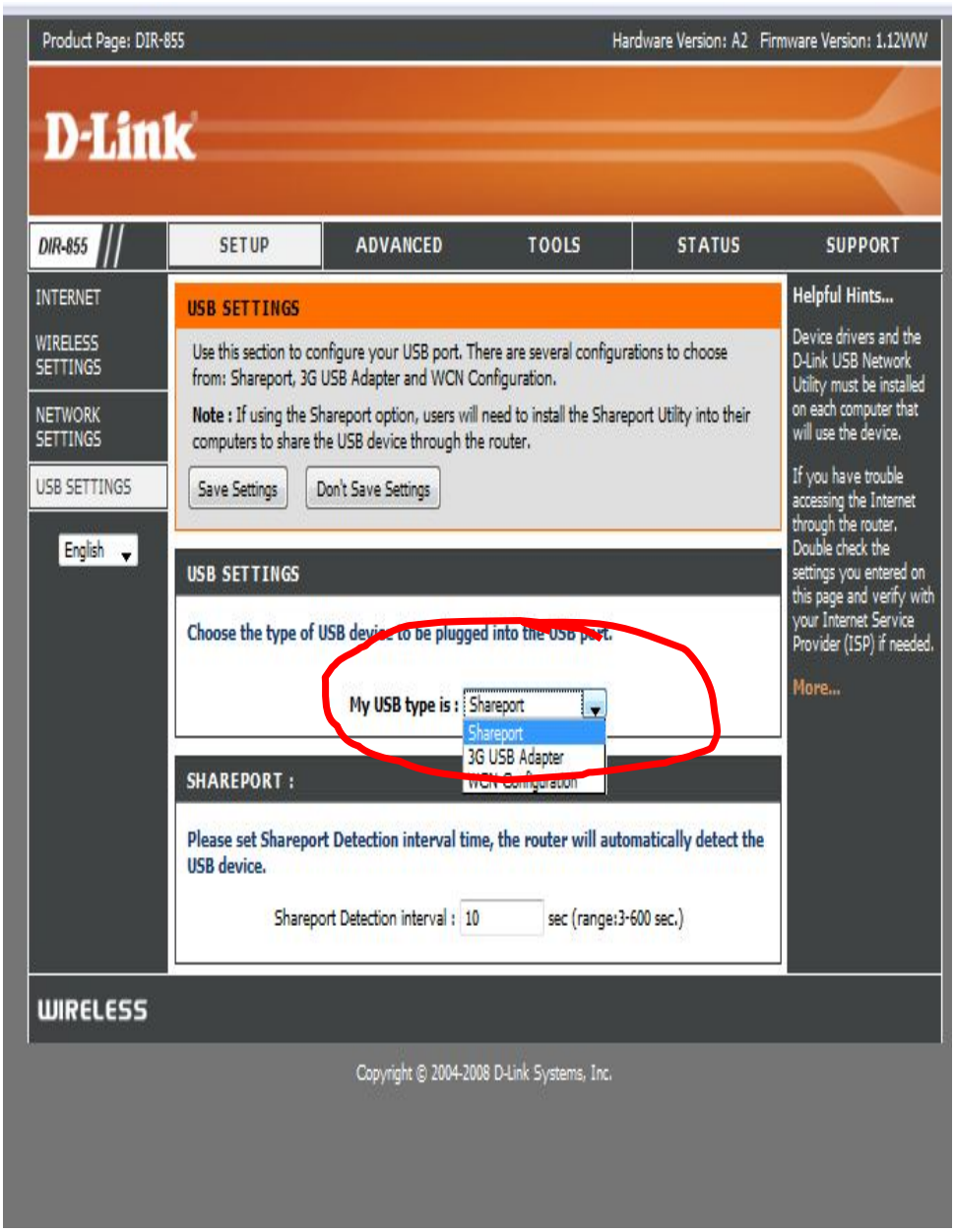


В разделе «Wireless Security Mode» выбираем режим шифрования данных принятый в существующей (или вновь настраиваемой) беспроводной сети


WIRELESS SETTINGS
NETWORK SETTINGS
USB SETTINGS
English
Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.
Save Settings
Don't Save Settings
WIRELESS NETWORK SETTINGS
Wireless Band : 2.4GHz Band
Enable Wireless : Always New Schedule
Wireless Network Name : dlink (Also called the SSID)
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan :
Wireless Channel : 2.437 GHz - CH 6
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20 MHz
Visibility Status : Visible Invisible
WIRELESS SECURITY MODE
To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.
Security Mode : None
None
WEP
WPA-Personal
WPA-Enterprise
WIRELESS NETWORK SETTIN
Wireless Band : 5GHz Band
Enable Wireless : Always New Schedule
Wireless Network Name : dlink_media (Also called the SSID)
802.11 Mode : Mixed 802.11n and 802.11a
Enable Auto Channel Scan :
Wireless Channel : 5.200 GHz - CH 40
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20 MHz
Visibility Status : Visible Invisible
WIRELESS SECURITY MODE
To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the
Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.
Enable Auto Channel Scat the router can select the best possible channel for your wireless network to operate on.
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
If you have enabled Wireless Security, make sure you write down the Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.
More...


Enable Wireless :
Always
New Schedule
Wireless Network Name :
dlink
(Also called the SSID)
802.11 Mode :
Mixed 802.11n, 802.11g and 802.11b
Enable Auto Channel Scan :
Wireless Channel :
2.437 GHz - CH 6
Transmission Rate :
Best (automatic)
(Mbit/s)
Channel Width :
20 MHz
Visibility Status :
Visible
Invisible
WIRELESS SECURITY MODE
To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.
Security Mode :
WPA-Personal
WPA
Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.
To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).
WPA Mode :
Auto (WPA or WPA2)
Cipher Type :
TKIP and AES
Group Key Update Interval :
3600
(seconds)
PRE-SHARED KEY
Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.
Pre-Shared Key :
••••••••
WIRELESS NETWORK SETTINGS
Wireless Band :
5GHz Band
Enable Wireless :
Always
New Schedule
Wireless Network Name :
dlink_media
(Also called the SSID)
for your wireless network to operate on.
Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.
If you have enabled Wireless Security, make sure you write down the Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.
More...


Pre-Shared Key : ••••••••
WIRELESS NETWORK SETTINGS
Wireless Band : 5GHz Band
Enable Wireless : Always New Schedule
Wireless Network Name : dlink_media (Also called the SSID)
802.11 Mode : Mixed 802.11n and 802.11a
Enable Auto Channel Scan :
Wireless Channel : 5.200 GHz - CH 40
Transmission Rate : Best (automatic) (Mbit/s)
Channel Width : 20 MHz
Visibility Status : Visible Invisible
WIRELESS SECURITY MODE
To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.
Security Mode : WPA-Personal
WPA
Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.
To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher).
WPA Mode : Auto (WPA or WPA2)
Cipher Type : TKIP and AES
Group Key Update Interval : 3600 (seconds)
PRE-SHARED KEY
Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.
Pre-Shared Key : ••••••••

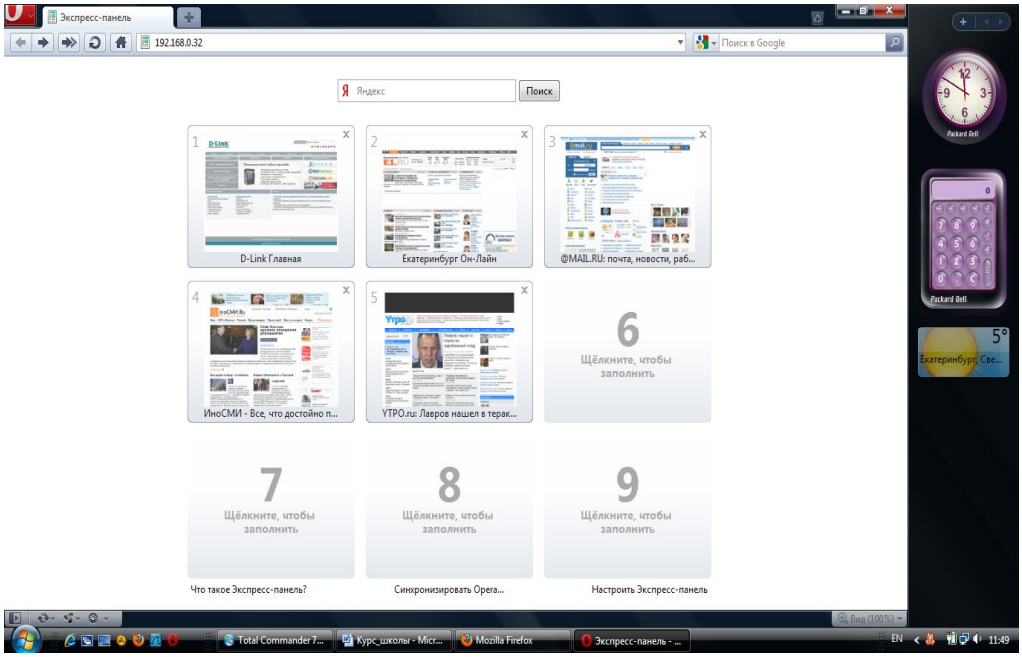

Product Page: DIR-855
Hardware Version: A2 Firmware Version: 1.12WW
D-Link
DIR-855
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS
USB SETTINGS
English
USB SETTINGS
Use this section to configure your USB port. There are several configurations to choose from: Shareport, 3G USB Adapter and WCN Configuration.
Note : If using the Shareport option, users will need to install the Shareport Utility into their computers to share the USB device through the router.
Save Settings
Don't Save Settings
USB SETTINGS
Choose the type of USB device to be plugged into the USB port.
My USB type is : Shareport
Shareport
3G USB Adapter
SHAREPORT :
Please set Shareport Detection interval time, the router will automatically detect the USB device.
Shareport Detection interval : 10 sec (range:3-600 sec.)
Helpful Hints...
Device drivers and the D-Link USB Network Utility must be installed on each computer that will use the device.
If you have trouble accessing the Internet through the router. Double check the settings you entered on this page and verify with your Internet Service Provider (ISP) if needed.
More...
WIRELESS
Copyright © 2004-2008 D-Link Systems, Inc.

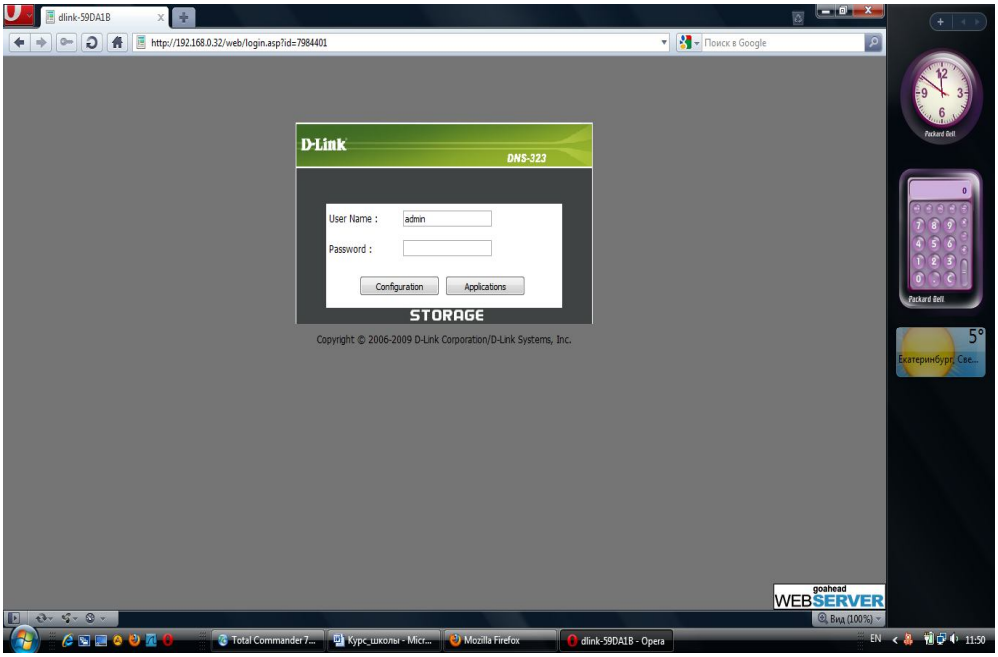
Файловое хранилище (файл-сервер) очень легко и достаточно качественно решается с использованием аппаратных решений, например используя DNS-323. Что позволяет это устройство?

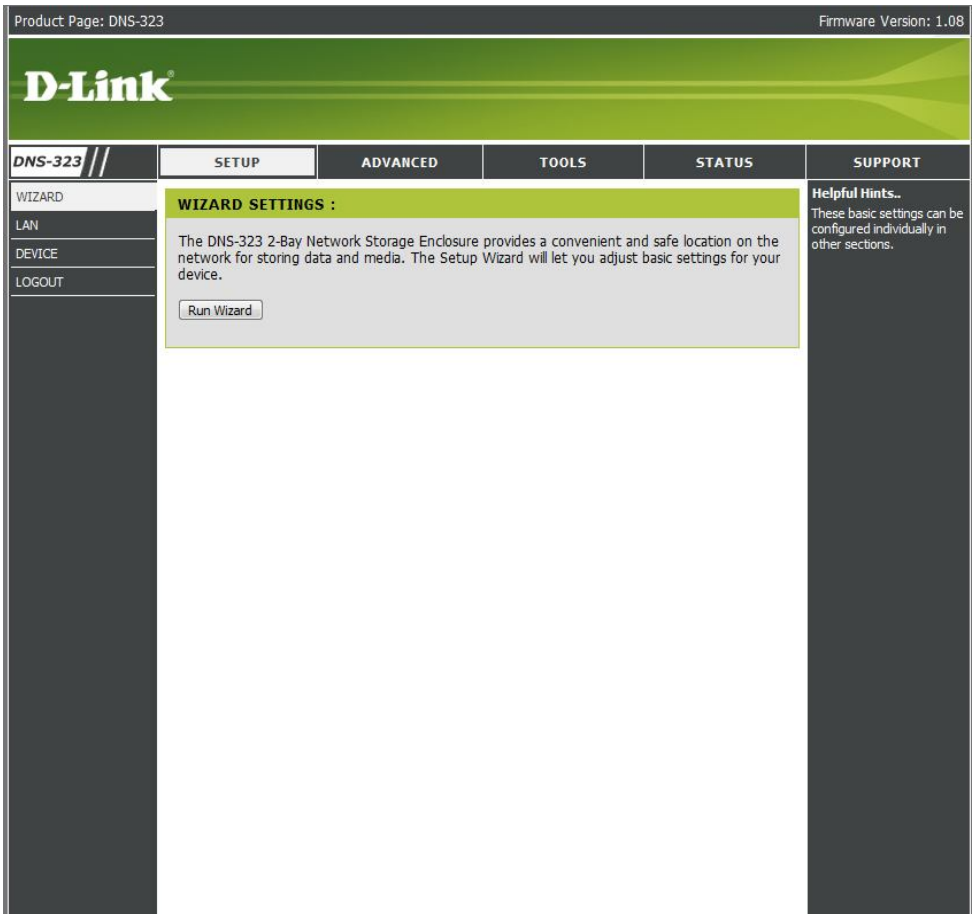
Сетевой дисковый массив DNS-323 с 2 отсеками для жестких дисков SATA предоставляет пользователям возможность совместного использования документов, файлов, и цифровых медиафайлов в домашней или офисной сети. Благодаря встроенному FTP-серверу возможен удаленный доступ к файлам через Интернет. DNS-323 обеспечивает защиту данных, предоставляя доступ к файлам по локальной сети или через Интернет только определенным пользователям или группам пользователей с правом чтения или чтения/записи каталогов.

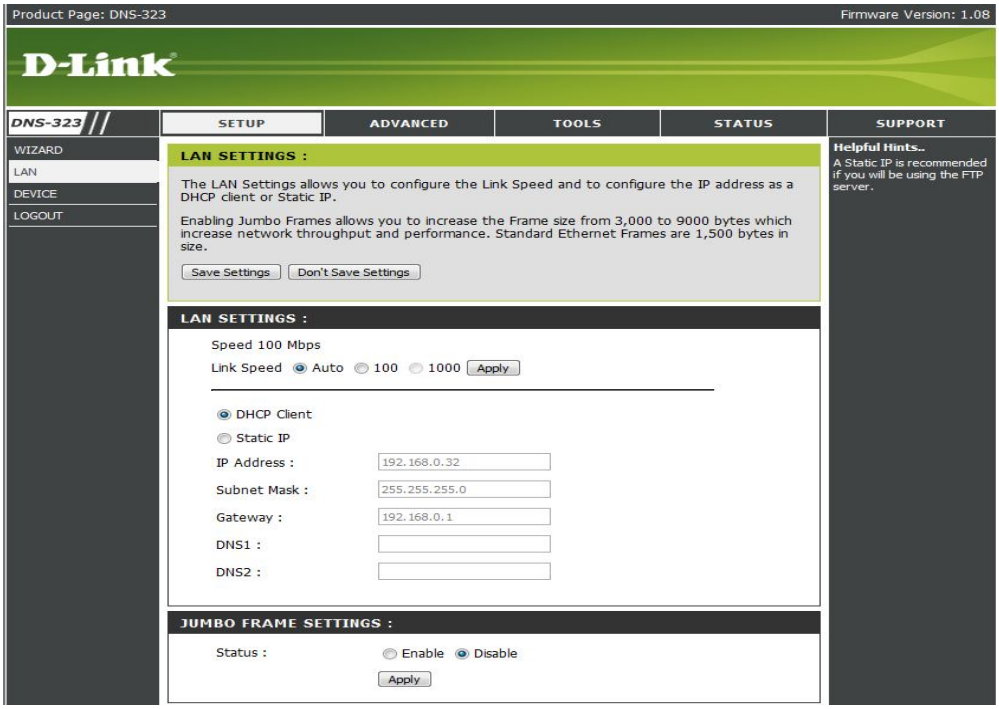
По сути это устройство является специализированным компьютером со специализированной операционной системой основная задача которого реализация файловых сервисов.

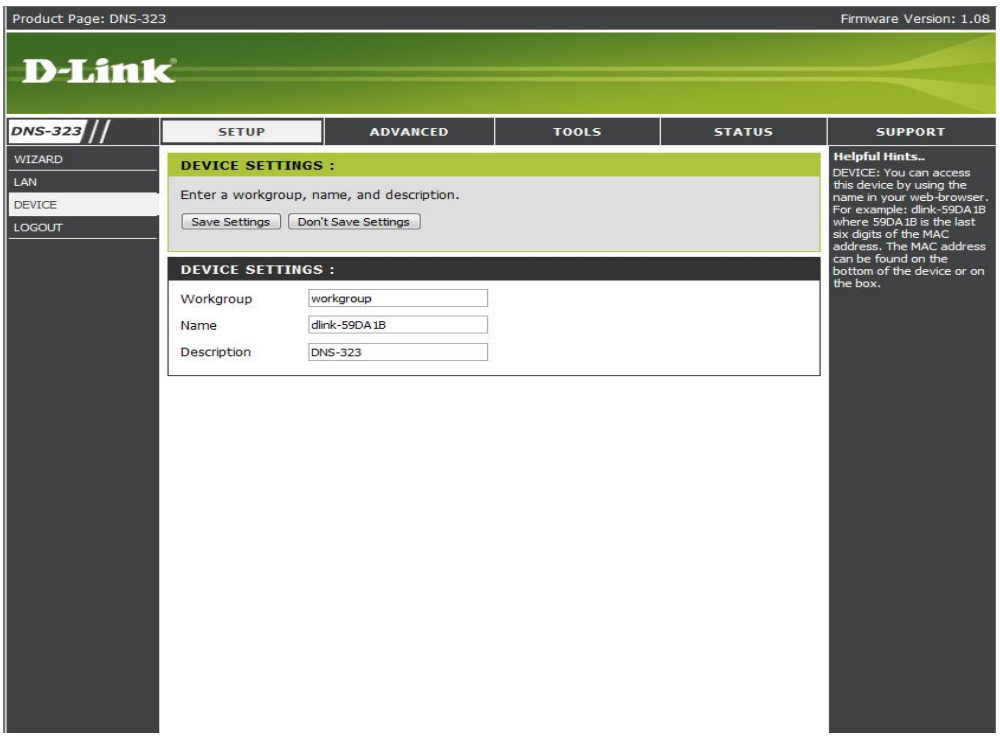
В DNS-323 доступны 4 различных режима работы с жесткими дисками (Standard, JBOD, RAID 0, RAID 1), позволяющих пользователям выбрать необходимую конфигурацию. В режиме Standard для использования доступны два отдельных жестких диска. Режим JBOD объединяет оба диска в один. Режим RAID 0 обеспечивает высокую производительность за счет разделения записи и чтения между двумя жесткими дисками. При использовании режима RAID 1 содержимое одного жесткого диска дублируется на другой, что обеспечивает максимальную надежность. Если один из жестких дисков выходит из строя, второй продолжает функционировать в полном объеме.

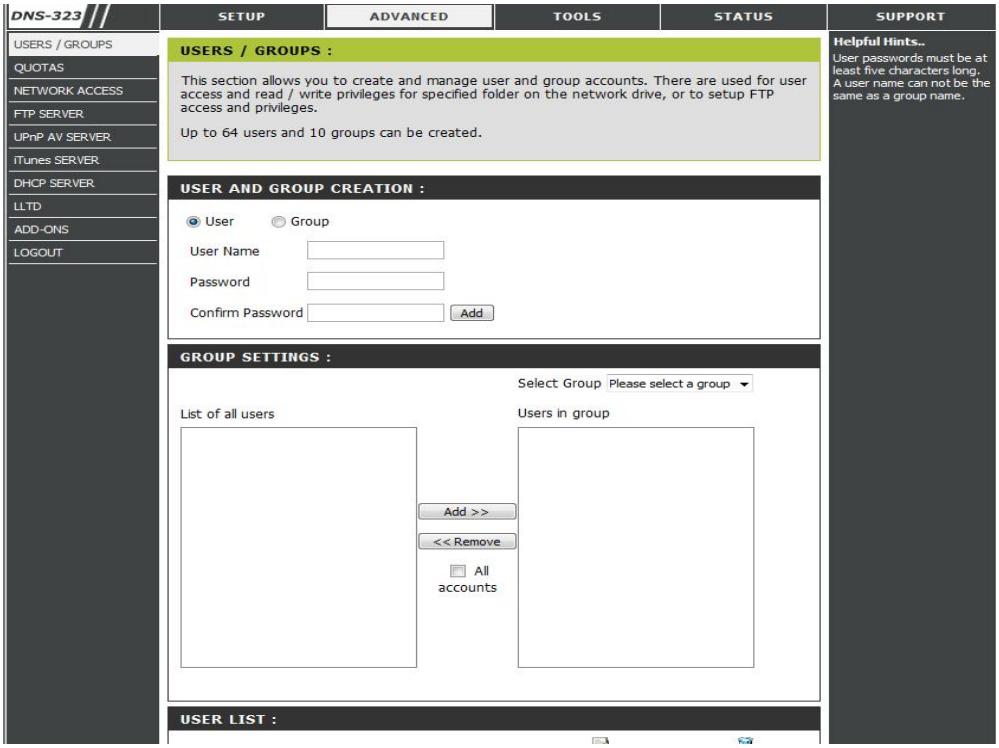

Экспресс-панель
192.168.0.32
Поиск в Google
Яндекс
Поиск
D-Link Главная
Екатеринбург Он-Лайн
@MAIL.RU: почта, новости, раб...
ИноСМИ - Все, что достойно п...
УТРО.ru: Лавров нашел в терак...
6
Щёлкните, чтобы заполнить
7
Щёлкните, чтобы заполнить
8
Щёлкните, чтобы заполнить
9
Щёлкните, чтобы заполнить
Что такое Экспресс-панель?
Синхронизировать Opera...
Настроить Экспресс-панель
Total Commander 7...
Курс_школы - Micr...
Mozilla Firefox
Экспресс-панель - ...
11:49

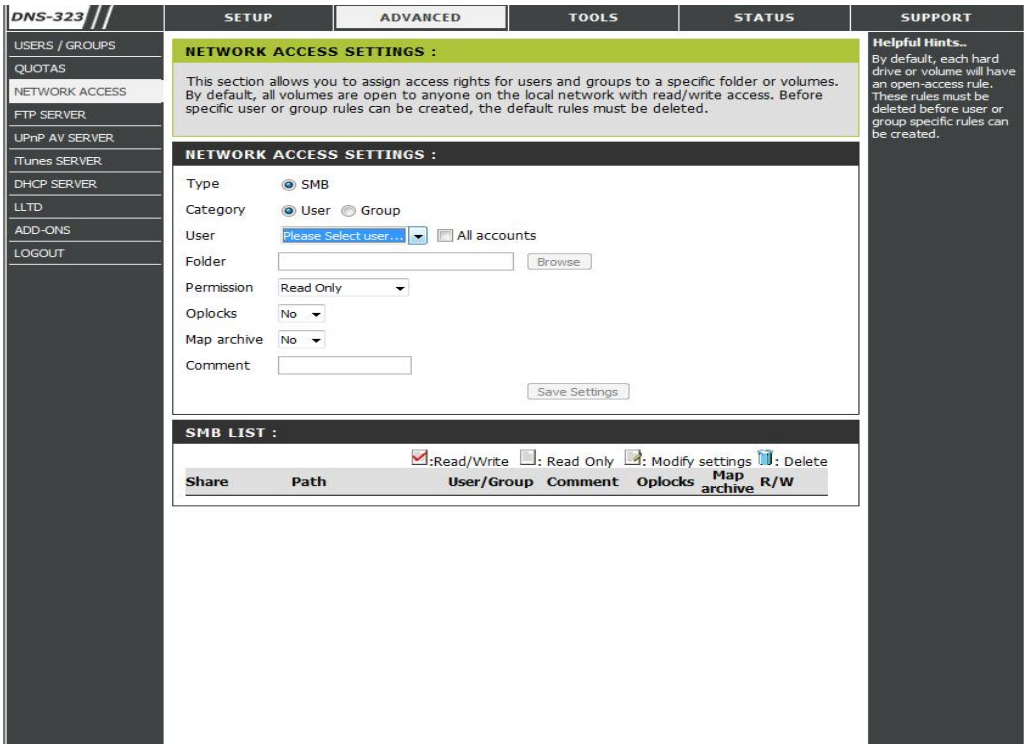

dlink-59DA1B
http://192.168.0.32/web/login.asp?id=7984401
Поиск в Google
D-Link
DNS-323
User Name :
admin
Password :
Configuration
Applications
STORAGE
Copyright © 2006-2009 D-Link Corporation/D-Link Systems, Inc.
goahead
WEBSERVER
Total Commander 7...
Курс_школы - Micr...
Mozilla Firefox
dlink-59DA1B - Opera
11:50


Product Page: DNS-323
Firmware Version: 1.08
D-Link
DNS-323
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
WIZARD
LAN
DEVICE
LOGOUT
WIZARD SETTINGS :
The DNS-323 2-Bay Network Storage Enclosure provides a convenient and safe location on the network for storing data and media. The Setup Wizard will let you adjust basic settings for your device.
Run Wizard
Helpful Hints..
These basic settings can be configured individually in other sections.


Product Page: DNS-323
Firmware Version: 1.08
D-Link
DNS-323
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
WIZARD
LAN
DEVICE
LOGOUT
LAN SETTINGS :
The LAN Settings allows you to configure the Link Speed and to configure the IP address as a DHCP client or Static IP.
Enabling Jumbo Frames allows you to increase the Frame size from 3,000 to 9000 bytes which increase network throughput and performance. Standard Ethernet Frames are 1,500 bytes in size.
Save Settings
Don't Save Settings
LAN SETTINGS :
Speed 100 Mbps
Link Speed Auto 100 1000 Apply
DHCP Client
Static IP
IP Address : 192.168.0.32
Subnet Mask : 255.255.255.0
Gateway : 192.168.0.1
DNS1 :
DNS2 :
JUMBO FRAME SETTINGS :
Status : Enable Disable
Apply
Helpful Hints..
A Static IP is recommended if you will be using the FTP server.


Product Page: DNS-323
Firmware Version: 1.08
D-Link
DNS-323
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
WIZARD
LAN
DEVICE
LOGOUT
DEVICE SETTINGS :
Enter a workgroup, name, and description.
Save Settings
Don't Save Settings
DEVICE SETTINGS :
Workgroup workgroup
Name dlink-59DA1B
Description DNS-323
Helpful Hints..
DEVICE: You can access this device by using the name in your web-browser. For example: dlink-59DA1B where 59DA1B is the last six digits of the MAC address. The MAC address can be found on the bottom of the device or on the box.


DNS-323
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
USERS / GROUPS
QUOTAS
NETWORK ACCESS
FTP SERVER
UPnP AV SERVER
iTunes SERVER
DHCP SERVER
LLTD
ADD-ONS
LOGOUT
USERS / GROUPS :
This section allows you to create and manage user and group accounts. There are used for user access and read / write privileges for specified folder on the network drive, or to setup FTP access and privileges.
Up to 64 users and 10 groups can be created.
USER AND GROUP CREATION :
User
Group
User Name
Password
Confirm Password
Add
GROUP SETTINGS :
Select Group
Please select a group
List of all users
Users in group
Add >>
<< Remove
All accounts
USER LIST :
Helpful Hints..
User passwords must be at least five characters long.
A user name can not be the same as a group name.


DNS-323
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
USERS / GROUPS
QUOTAS
NETWORK ACCESS
FTP SERVER
UPnP AV SERVER
iTunes SERVER
DHCP SERVER
LLTD
ADD-ONS
LOGOUT
NETWORK ACCESS SETTINGS :
This section allows you to assign access rights for users and groups to a specific folder or volumes. By default, all volumes are open to anyone on the local network with read/write access. Before specific user or group rules can be created, the default rules must be deleted.
NETWORK ACCESS SETTINGS :
Type
SMB
Category
User
Group
User
Please Select user...
All accounts
Folder
Browse
Permission
Read Only
Oplocks
No
Map archive
No
Comment
Save Settings
SMB LIST :
:Read/Write
: Read Only
: Modify settings
: Delete
Share
Path
User/Group
Comment
Oplocks
Map archive
R/W
Helpful Hints..
By default, each hard drive or volume will have an open-access rule. These rules must be deleted before user or group specific rules can be created.

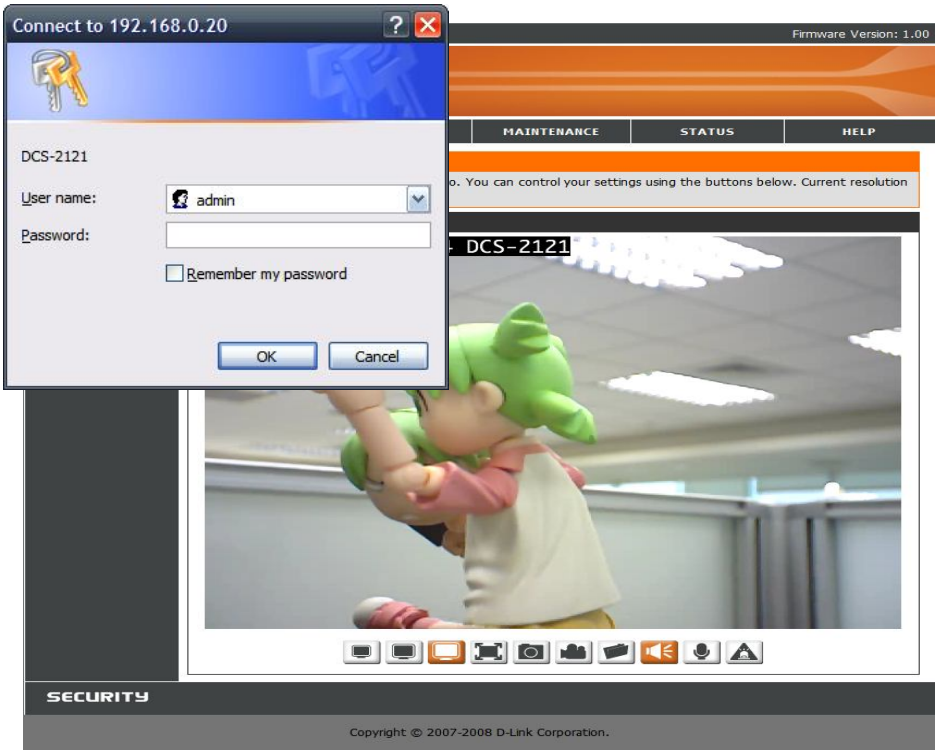
Почему в качестве системы видеонаблюдения предлагается использовать интернет камеры? Просто потому что имея транспортную систему а виде ЛВС, глупо не воспользоваться ей, и строить дополнительно систему видеонаблюдения. Итак, как мы увидим ниже, интернет камеры органично вписываются в ЛВС, к тому же могут использоваться в беспроводных решениях.

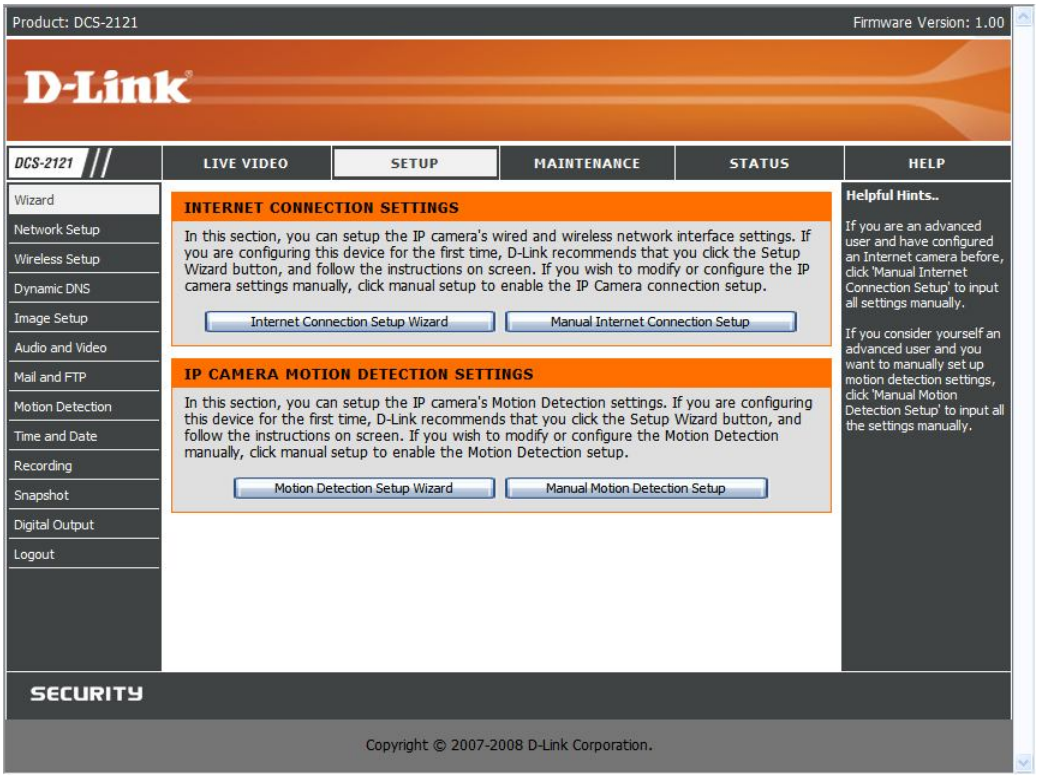
DCS-2121 – универсальное решение для малого офиса и дома. В отличие от стандартных Web-камер DCS-2121 является полной системой со встроенным процессором и Web-сервером, который передает высококачественное видеоизображение для безопасности и наблюдения. Можно получить удаленный доступ к DCS-2121 и управлять камерой из любого компьютера или ноутбука по локальной сети или Интернет через Web-браузер. Простая установка и интуитивный Web-интерфейс предоставляют легкую интеграцию с Ethernet/Fast Ethernet или беспроводной сетью 802.11g.

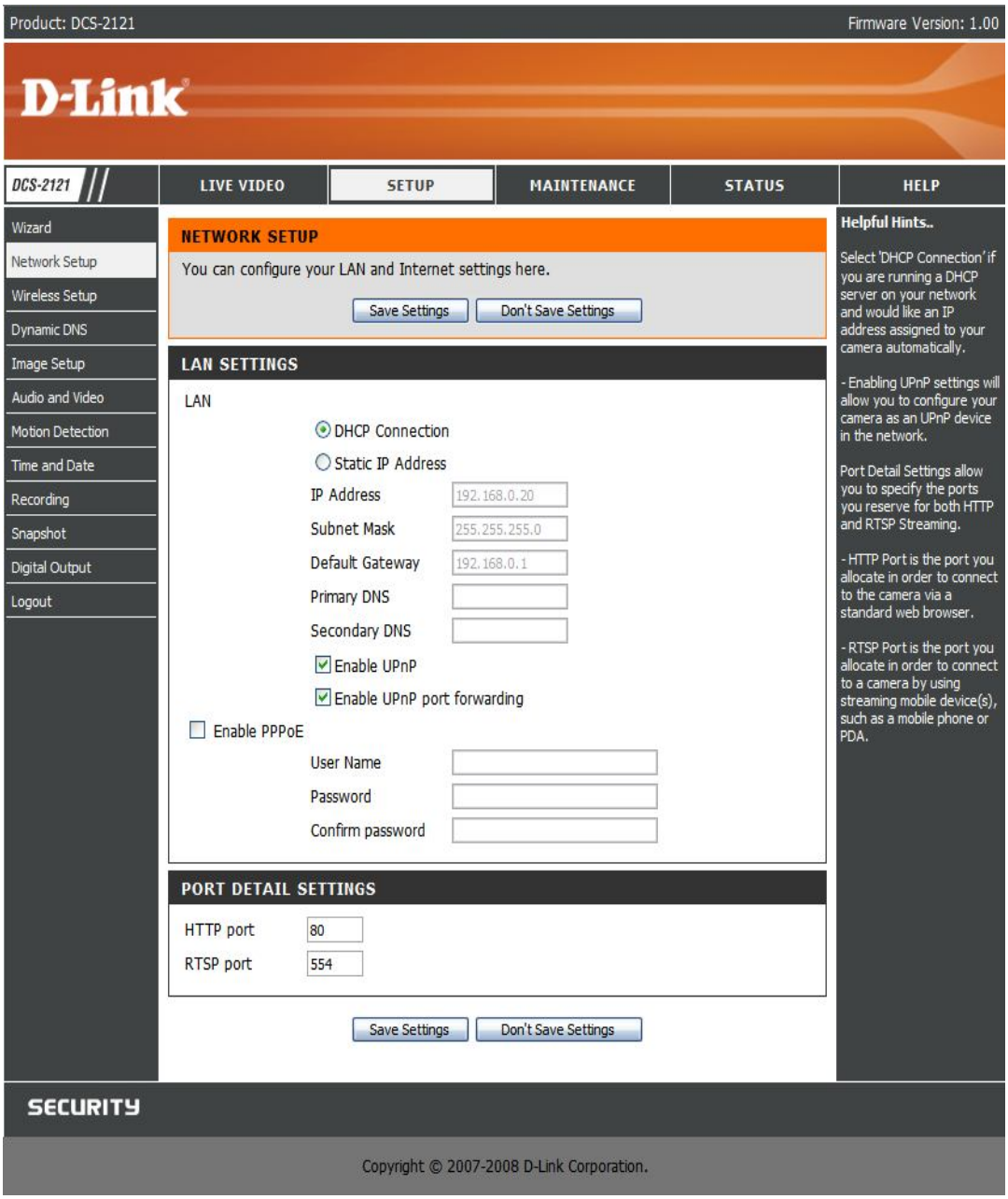
DCS-2121 также имеет функции удаленного управления и обнаружения движения для комплексного и эффективного решения домашней безопасности.

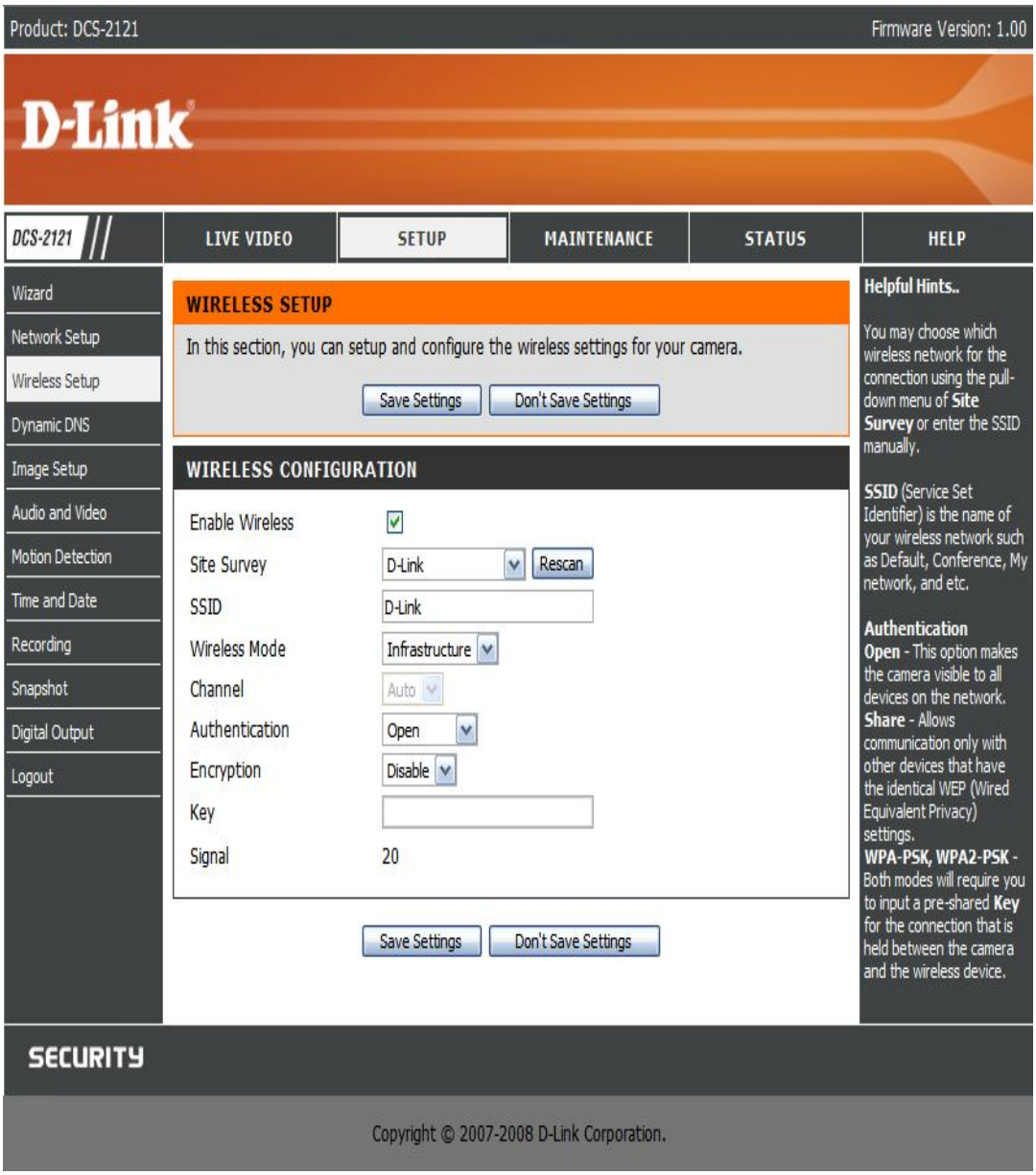
DCS-2121 может подключаться к беспроводной сети 802.11g и к сети Ethernet/Fast Ethernet, что делает DCS-2121 удобным для интеграции с существующей сетью. DCS-2121 работает с обычными сетями на скорости 10 Мбит/с (Ethernet) или 100 Мбит/с (Fast Ethernet), с беспроводными маршрутизаторами 802.11g или точками доступа.

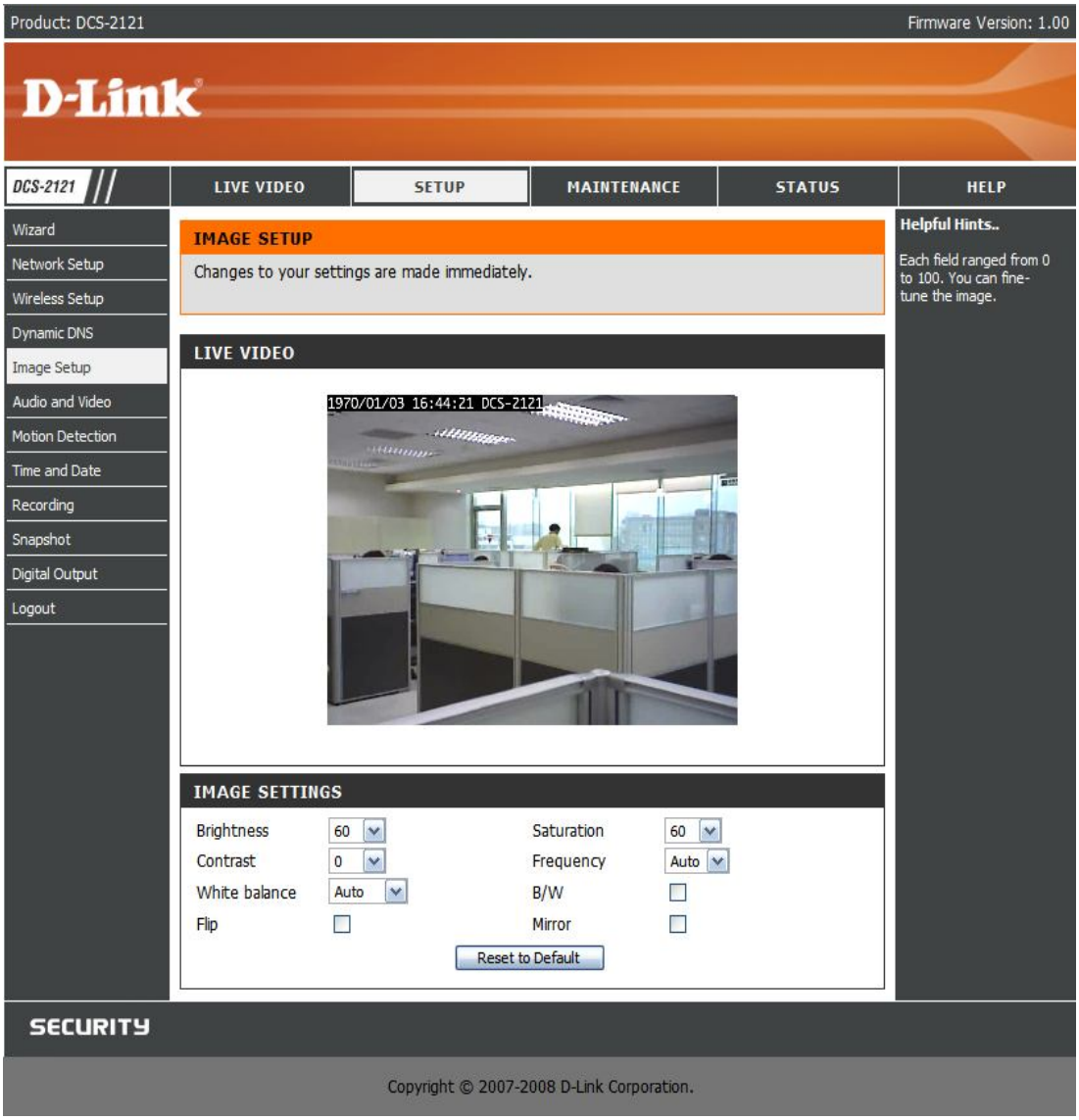
Используя функции захвата кадров и записи можно сохранять стоп-кадры и записывать видео и аудио из Web-браузера непосредственно на локальный жесткий диск без установки специального программного обеспечения, что делает камеру удобной для захвата кадров в любой момент из удаленного местонахождения. DCS-2121 позволяет записывать видео непосредственно на локальный сетевое хранилище без использования специального компьютера для хранения видеофайлов.

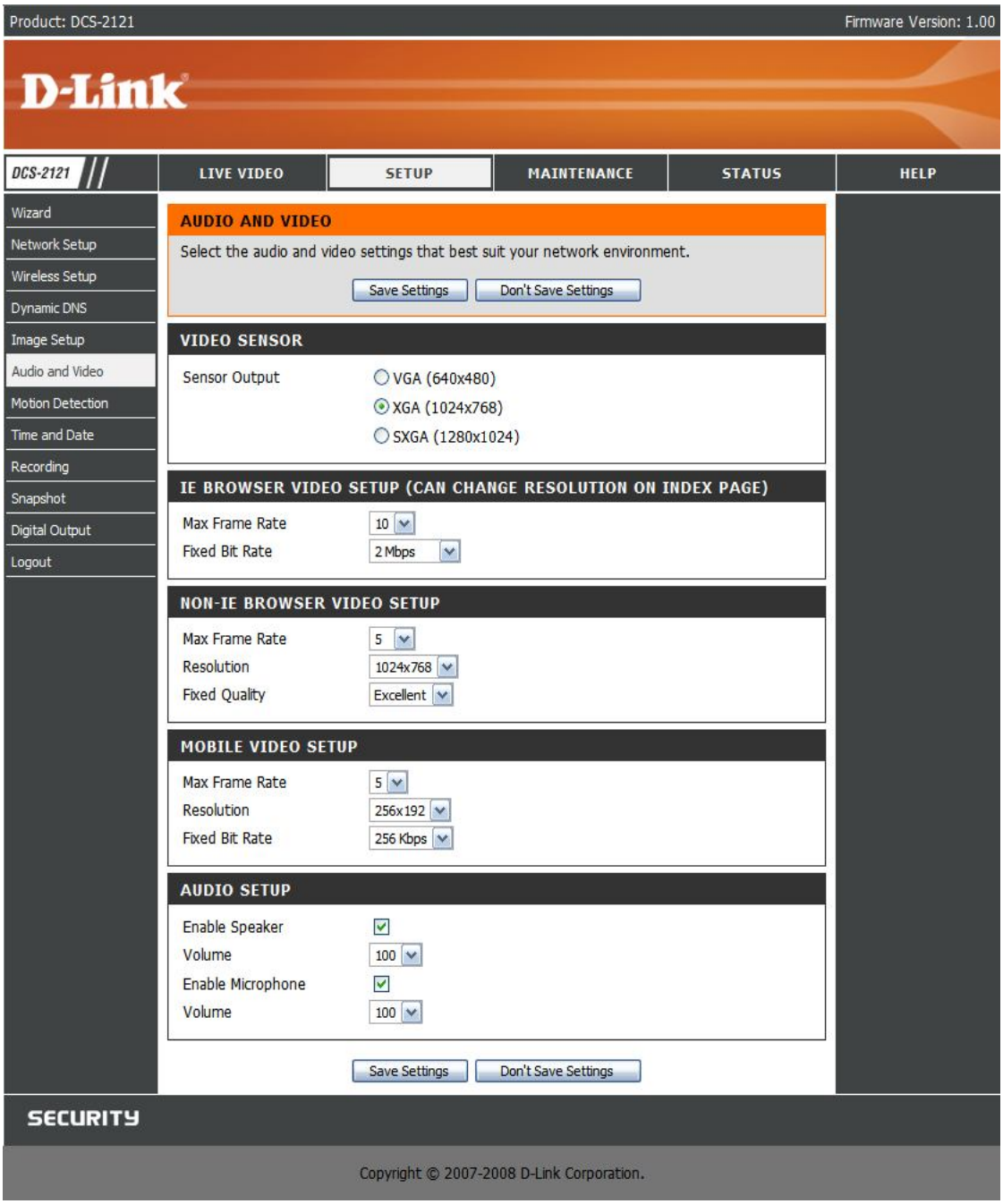

Connect to 192.168.0.20
DCS-2121
User name:
admin
Password:
Remember my password
OK
Cancel
Firmware Version: 1.00
MAINTENANCE
STATUS
HELP
You can control your settings using the buttons below. Current resolution
DCS-2121
SECURITY
Copyright © 2007-2008 D-Link Corporation.

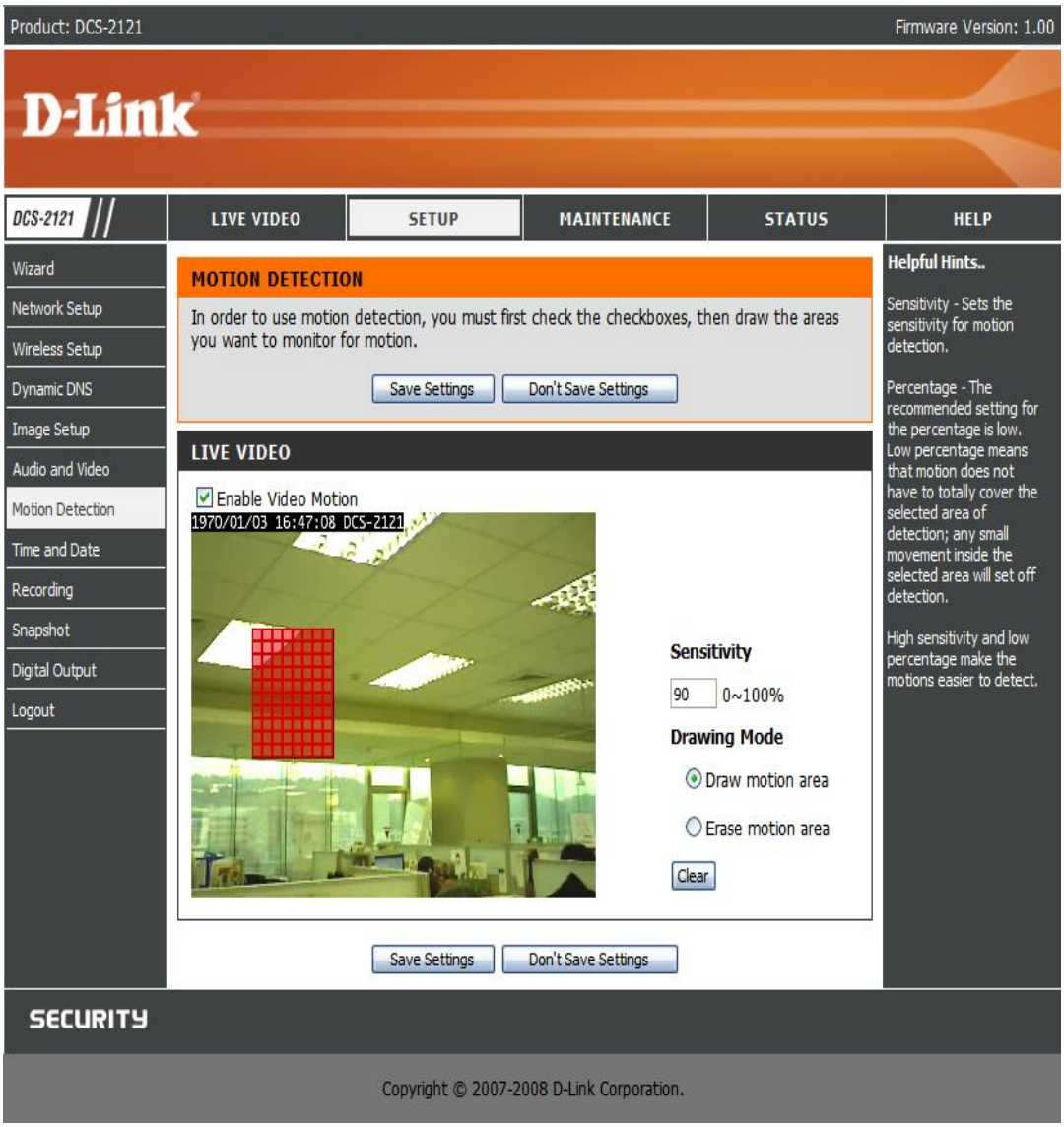

Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Mail and FTP
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
INTERNET CONNECTION SETTINGS
In this section, you can setup the IP camera's wired and wireless network interface settings. If you are configuring this device for the first time, D-Link recommends that you click the Setup Wizard button, and follow the instructions on screen. If you wish to modify or configure the IP camera settings manually, click manual setup to enable the IP Camera connection setup.
Internet Connection Setup Wizard
Manual Internet Connection Setup
IP CAMERA MOTION DETECTION SETTINGS
In this section, you can setup the IP camera's Motion Detection settings. If you are configuring this device for the first time, D-Link recommends that you click the Setup Wizard button, and follow the instructions on screen. If you wish to modify or configure the Motion Detection manually, click manual setup to enable the Motion Detection setup.
Motion Detection Setup Wizard
Manual Motion Detection Setup
Helpful Hints..
If you are an advanced user and have configured an Internet camera before, click 'Manual Internet Connection Setup' to input all settings manually.
If you consider yourself an advanced user and you want to manually set up motion detection settings, click 'Manual Motion Detection Setup' to input all the settings manually.
SECURITY
Copyright © 2007-2008 D-Link Corporation.

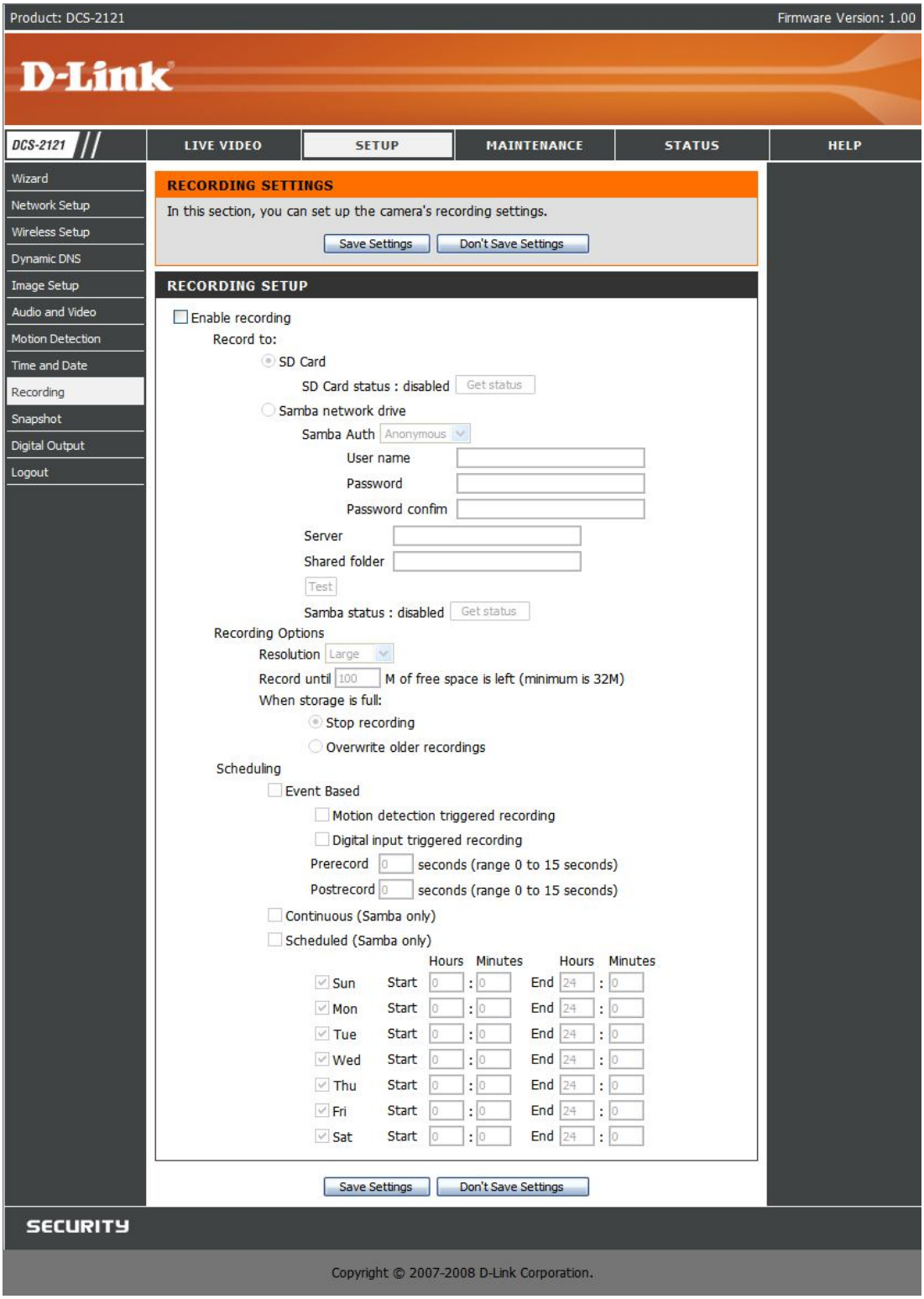

Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
NETWORK SETUP
You can configure your LAN and Internet settings here.
Save Settings
Don't Save Settings
LAN SETTINGS
LAN
DHCP Connection
Static IP Address
IP Address
192.168.0.20
Subnet Mask
255.255.255.0
Default Gateway
192.168.0.1
Primary DNS
Secondary DNS
Enable UPnP
Enable UPnP port forwarding
Enable PPPoE
User Name
Password
Confirm password
PORT DETAIL SETTINGS
HTTP port
80
RTSP port
554
Save Settings
Don't Save Settings
Helpful Hints..
Select 'DHCP Connection' if you are running a DHCP server on your network and would like an IP address assigned to your camera automatically.
- Enabling UPnP settings will allow you to configure your camera as an UPnP device in the network.
Port Detail Settings allow you to specify the ports you reserve for both HTTP and RTSP Streaming.
- HTTP Port is the port you allocate in order to connect to the camera via a standard web browser.
- RTSP Port is the port you allocate in order to connect to a camera by using streaming mobile device(s), such as a mobile phone or PDA.
SECURITY
Copyright © 2007-2008 D-Link Corporation.

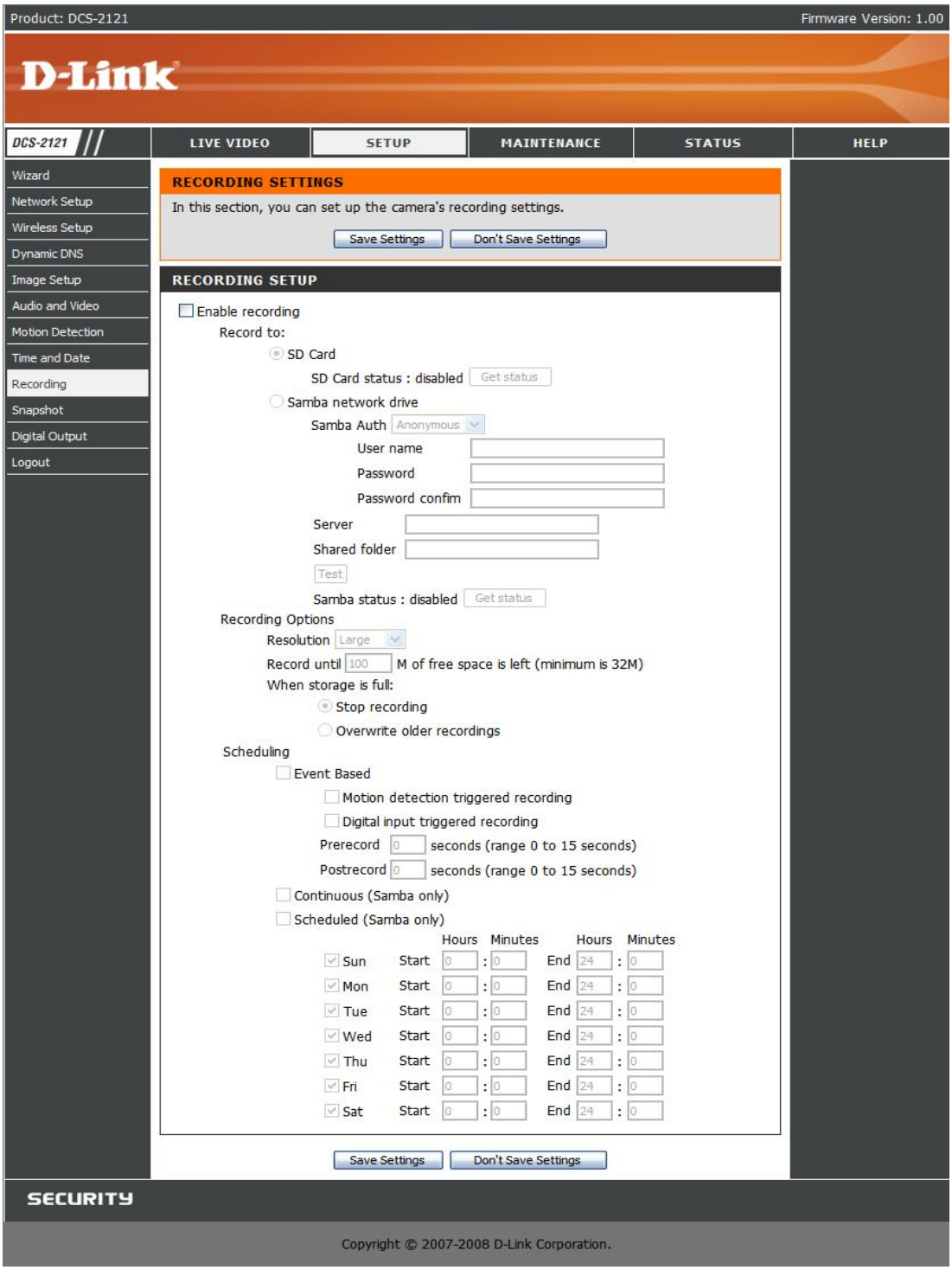

Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
WIRELESS SETUP
In this section, you can setup and configure the wireless settings for your camera.
Save Settings
Don't Save Settings
WIRELESS CONFIGURATION
Enable Wireless
Site Survey
D-Link
Rescan
SSID
D-Link
Wireless Mode
Infrastructure
Channel
Auto
Authentication
Open
Encryption
Disable
Key
Signal
20
Save Settings
Don't Save Settings
Helpful Hints..
You may choose which wireless network for the connection using the pull-down menu of Site Survey or enter the SSID manually.
SSID (Service Set Identifier) is the name of your wireless network such as Default, Conference, My network, and etc.
Authentication
Open - This option makes the camera visible to all devices on the network.
Share - Allows communication only with other devices that have the identical WEP (Wired Equivalent Privacy) settings.
WPA-PSK, WPA2-PSK - Both modes will require you to input a pre-shared Key for the connection that is held between the camera and the wireless device.
SECURITY
Copyright © 2007-2008 D-Link Corporation.

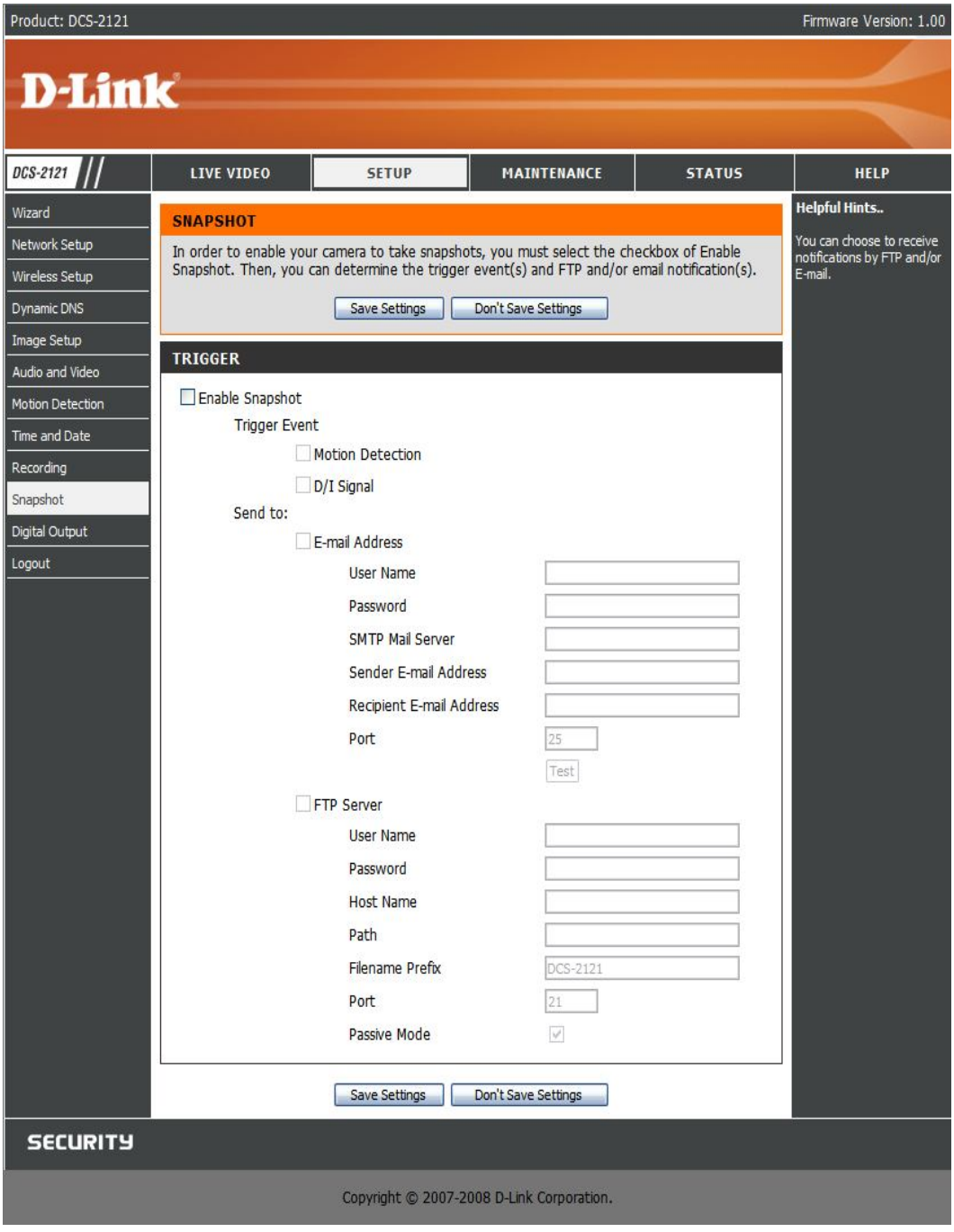

Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
IMAGE SETUP
Changes to your settings are made immediately.
LIVE VIDEO
1970/01/03 16:44:21 DCS-2121
IMAGE SETTINGS
Brightness 60
Contrast 0
White balance Auto
Flip
Saturation 60
Frequency Auto
B/W
Mirror
Reset to Default
Helpful Hints..
Each field ranged from 0 to 100. You can fine-tune the image.
SECURITY
Copyright © 2007-2008 D-Link Corporation.


Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
AUDIO AND VIDEO
Select the audio and video settings that best suit your network environment.
Save Settings
Don't Save Settings
VIDEO SENSOR
Sensor Output
VGA (640x480)
XGA (1024x768)
SXGA (1280x1024)
IE BROWSER VIDEO SETUP (CAN CHANGE RESOLUTION ON INDEX PAGE)
Max Frame Rate
10
Fixed Bit Rate
2 Mbps
NON-IE BROWSER VIDEO SETUP
Max Frame Rate
5
Resolution
1024x768
Fixed Quality
Excellent
MOBILE VIDEO SETUP
Max Frame Rate
5
Resolution
256x192
Fixed Bit Rate
256 Kbps
AUDIO SETUP
Enable Speaker
Volume
100
Enable Microphone
Volume
100
Save Settings
Don't Save Settings
SECURITY
Copyright © 2007-2008 D-Link Corporation.


Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
MOTION DETECTION
In order to use motion detection, you must first check the checkboxes, then draw the areas you want to monitor for motion.
Save Settings
Don't Save Settings
LIVE VIDEO
Enable Video Motion
1970/01/03 16:47:08 DCS-2121
Sensitivity
90
0~100%
Drawing Mode
Draw motion area
Erase motion area
Clear
Save Settings
Don't Save Settings
Helpful Hints..
Sensitivity - Sets the sensitivity for motion detection.
Percentage - The recommended setting for the percentage is low. Low percentage means that motion does not have to totally cover the selected area of detection; any small movement inside the selected area will set off detection.
High sensitivity and low percentage make the motions easier to detect.
SECURITY
Copyright © 2007-2008 D-Link Corporation.


Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
RECORDING SETTINGS
In this section, you can set up the camera's recording settings.
Save Settings
Don't Save Settings
RECORDING SETUP
Enable recording
Record to:
SD Card
SD Card status : disabled
Get status
Samba network drive
Samba Auth
Anonymous
User name
Password
Password confim
Server
Shared folder
Test
Samba status : disabled
Get status
Recording Options
Resolution
Large
Record until
100
M of free space is left (minimum is 32M)
When storage is full:
Stop recording
Overwrite older recordings
Scheduling
Event Based
Motion detection triggered recording
Digital input triggered recording
Prerecord
seconds (range 0 to 15 seconds)
Postrecord
seconds (range 0 to 15 seconds)
Continuous (Samba only)
Scheduled (Samba only)
Hours
Minutes
Hours
Minutes
Sun
Mon
Tue
Wed
Thu
Fri
Sat
Start
End
Save Settings
Don't Save Settings
SECURITY
Copyright © 2007-2008 D-Link Corporation.


Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
RECORDING SETTINGS
In this section, you can set up the camera's recording settings.
Save Settings
Don't Save Settings
RECORDING SETUP
Enable recording
Record to:
SD Card
SD Card status : disabled
Get status
Samba network drive
Samba Auth
Anonymous
User name
Password
Password confim
Server
Shared folder
Test
Samba status : disabled
Get status
Recording Options
Resolution
Large
Record until
100
M of free space is left (minimum is 32M)
When storage is full:
Stop recording
Overwrite older recordings
Scheduling
Event Based
Motion detection triggered recording
Digital input triggered recording
Prerecord
0
seconds (range 0 to 15 seconds)
Postrecord
0
seconds (range 0 to 15 seconds)
Continuous (Samba only)
Scheduled (Samba only)
Hours
Minutes
Hours
Minutes
Sun
Start
End
Mon
Tue
Wed
Thu
Fri
Sat
Save Settings
Don't Save Settings
SECURITY
Copyright © 2007-2008 D-Link Corporation.


Product: DCS-2121
Firmware Version: 1.00
D-Link
DCS-2121
LIVE VIDEO
SETUP
MAINTENANCE
STATUS
HELP
Wizard
Network Setup
Wireless Setup
Dynamic DNS
Image Setup
Audio and Video
Motion Detection
Time and Date
Recording
Snapshot
Digital Output
Logout
SNAPSHOT
In order to enable your camera to take snapshots, you must select the checkbox of Enable Snapshot. Then, you can determine the trigger event(s) and FTP and/or email notification(s).
Save Settings
Don't Save Settings
TRIGGER
Enable Snapshot
Trigger Event
Motion Detection
D/I Signal
Send to:
E-mail Address
User Name
Password
SMTP Mail Server
Sender E-mail Address
Recipient E-mail Address
Port
25
Test
FTP Server
User Name
Password
Host Name
Path
Filename Prefix
DCS-2121
Port
21
Passive Mode
Save Settings
Don't Save Settings
Helpful Hints..
You can choose to receive notifications by FTP and/or E-mail.
SECURITY
Copyright © 2007-2008 D-Link Corporation.

Там где нет возможности (или необходимости) прокладки проводных кабелей Ethernet, и в силу других причин невозможно организовать беспроводную сеть, может оказать помощь устройство DHP-300.

DHP-300 D-Link является сетевым адаптером нового поколения для электрических сетей, предоставляющим простую в использовании технологию для высококачественной передачи Интернет-видео, музыки, игр и голоса через стандартные домашние розетки электропитания. Обеспечивая скорость передачи данных до 200 Мбит/с, этот адаптер предоставляет достаточную пропускную способность, позволяя домашним пользователям использовать существующую электрическую сеть для расширения возможностей домашней сети.

DHP-300 идеален для подключения сетевых мультимедиа устройств, обычно расположенных вблизи розеток электропитания. Любые Ethernet-устройства, такие как широкополосные маршрутизаторы, компьютеры, телевизоры высокой четкости, цифровые видеорекордеры, игровые консоли, принт-серверы или медиаплееры D-Link могут быть подключены к домашней сети. Этот адаптер является идеальным решением при использовании таких приложений, как потоковое аудио/видео, совместный доступ к музыкальным файлам и многопользовательские онлайновые игры.

Поддержка QOS обеспечивает приоритезацию трафика. Адаптер поддерживает настраиваемое пользователем шифрование данных и 802.1Q VLAN для защиты домашней сети от злоумышленников.

Как правило с помощью DHP-300 создаются т.н. Ethernet-мост через сеть электро питания. Адаптер DHP-300 подключается непосредственно к электрической розетке , а в его розетку разъёма 8P8C (RG45), с помощью патч-корда подключается компьютер (игровая приставка, интернет камера наблюдения, или любое другое сетевое устройство) Электрический ток не влияет на передачу данных, т.к. передается на другой частоте.

Настройка данного устройства проста, не требует специальных навыков и подробно описана в инструкции поставляемой в комплекте с устройством. Хочется обратить внимание, что сеть передачи данных создаваемая устройствами DHP-300, поверх электрической сети, имеет название (Net ID) и сетевой пароль для шифрования трафика, эти параметры в целях безопасности следует настроить.

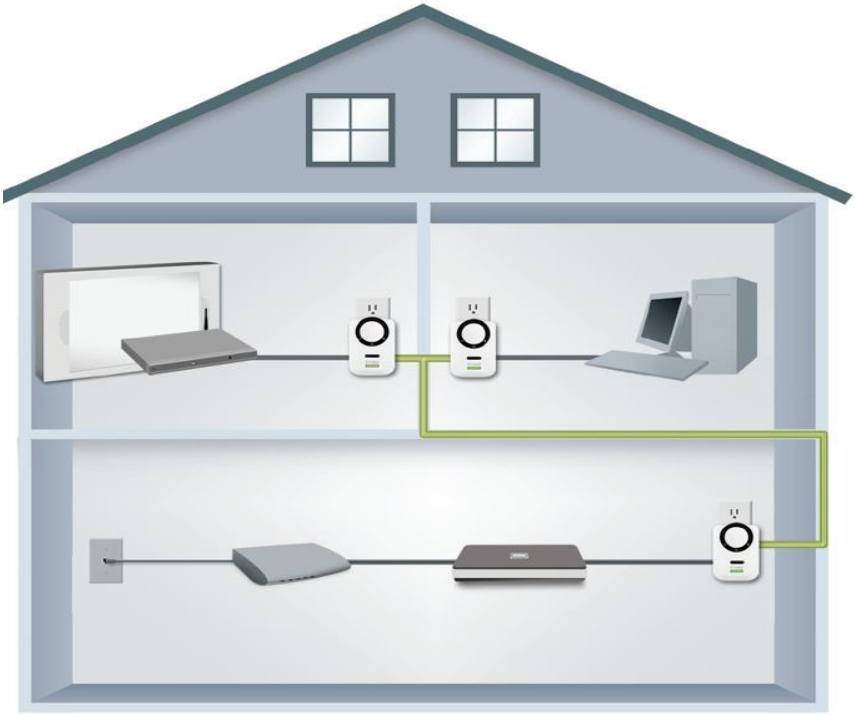
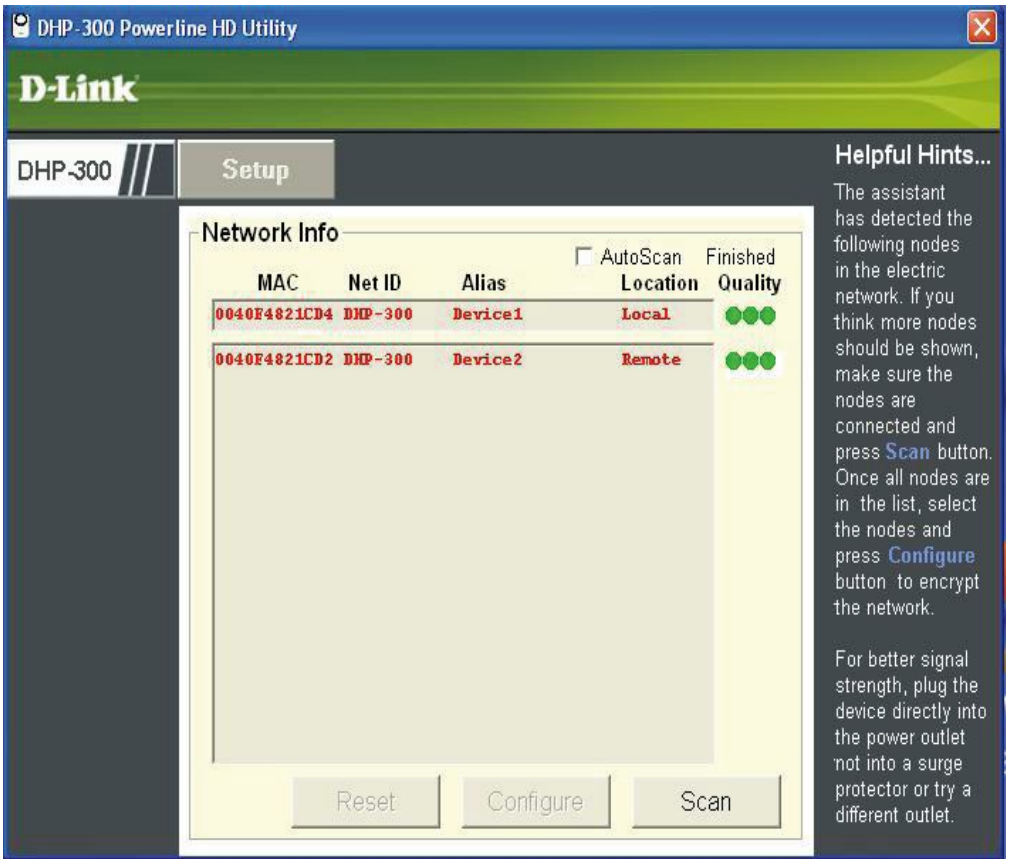


Рис. 119. Применение DHP-300 , используя электро проводку

Рис. 120.Ярлык программы



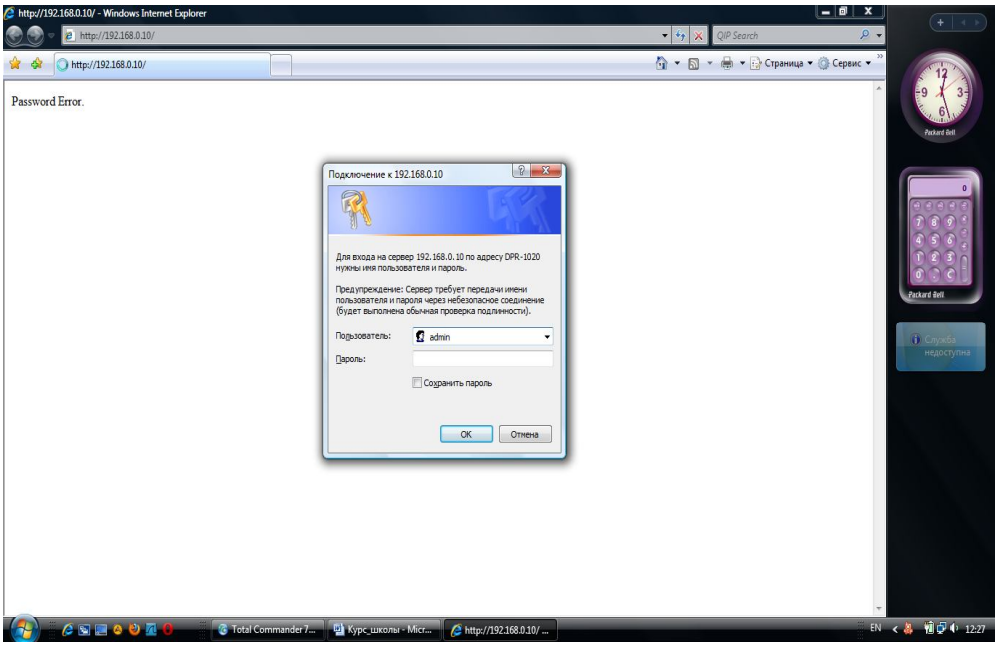
Следующее устройство , которое позволит реализовать сервис печати – DPR-1020.

Многофункциональный принт-сервер DPR-1020 с USB-портом обеспечивает совместный доступ пользователей в сети к принтеру или к МФУ, поддерживающему функции печати и сканирования. Принт-сервер позволяет нескольким пользователям со своих компьютеров выполнять отправку документов в очереди печати и факса.

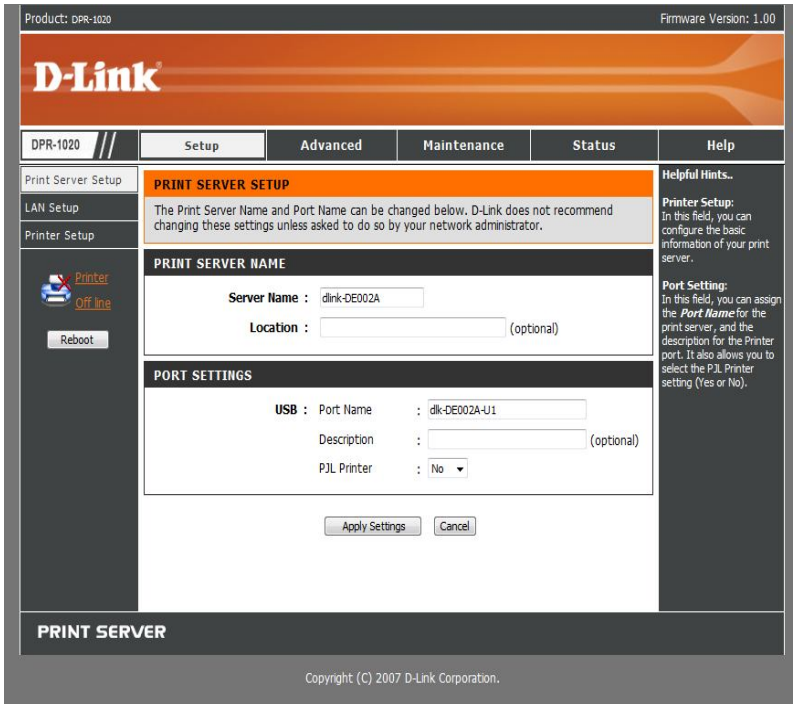
Рис. 121. DPR-1020

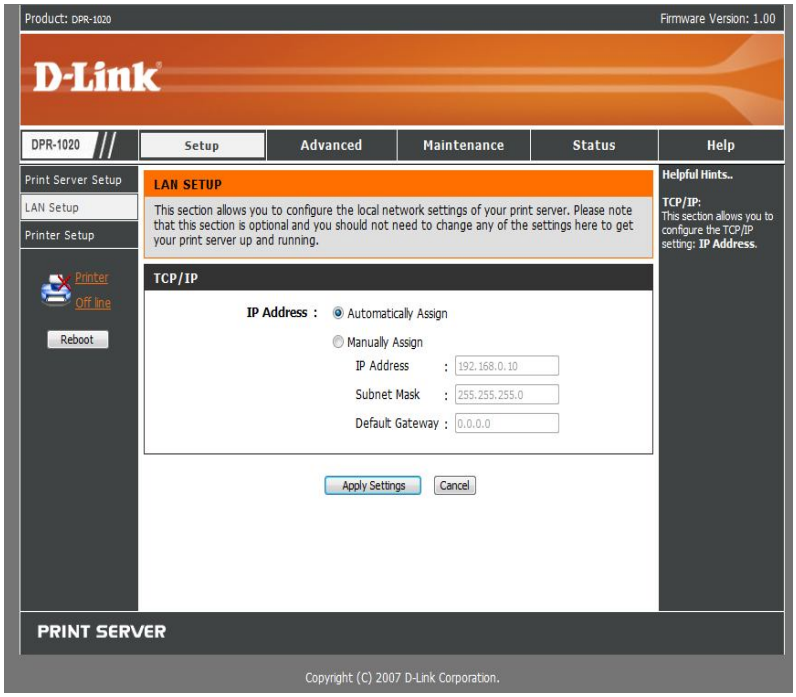
С помощью одного стильного и компактного устройства организуется совместный доступ пользователей в сети к принтеру и оборудованию с такими функциями, как печать, факс и сканирование. Благодаря мощному CPU, буферу памяти большого размера, высокоскоростному USB-порту 2.0, скорости передачи данных до 1000Мбит/с, DPR-1020 делает работу в сети быстрой и эффективной.

На подключенном к DPR-1020 МФУ может одновременно выполняться печать, сканирование и отправка факса, что значительно повышает производительность по сравнению с программными принт-серверами. Кроме того, принт-сервер DPR-1020 поддерживает несколько операционных систем, включая Windows NT/2000/XP/Vista, Apple MacOS с AppleTalk, Linux и Unix, предоставляя пользователям гибкость при работе в независимости от сетевого окружения.



Порядок настройки устройства очень прост и интуитивно понятен.





И последнее устройство из списка данного задания - DSM-320RD

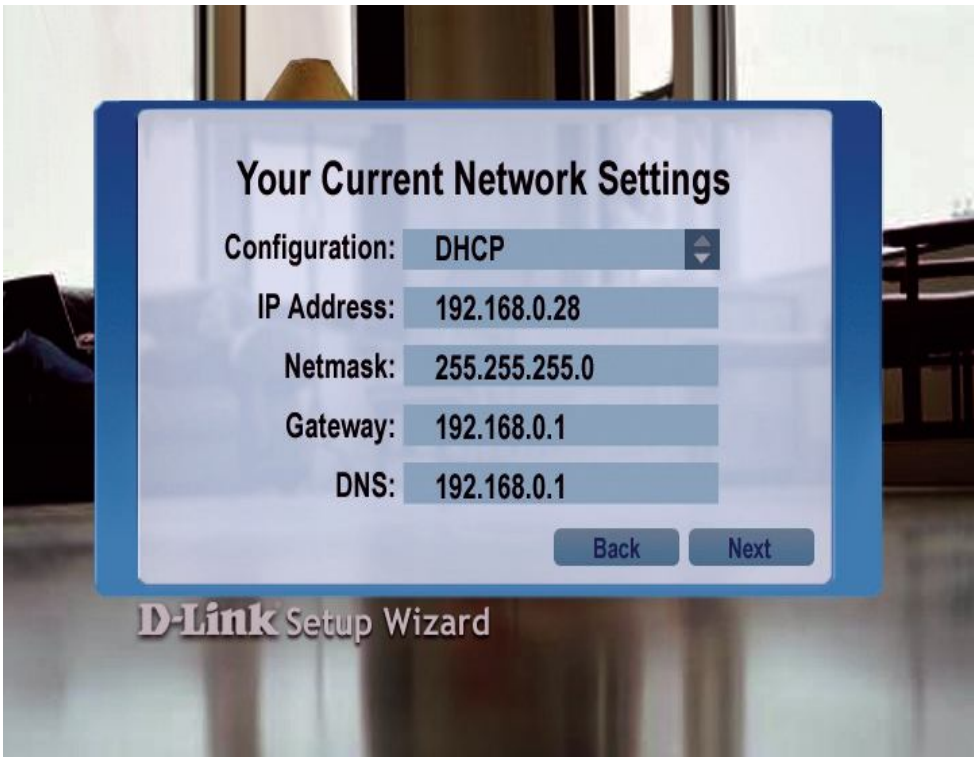
Медиаплеер D-Link MediaLounge DSM-320RD является беспроводным медиаплеером с поддержкой DVD и Card-ридера, подключающий ваш домашний развлекательный центр к домашней сети и позволяющий передавать по беспроводной сети музыку, фотографии, видео от компьютера к телевизору или стерео системе. Используя протокол беспроводной передачи 802.11g, DSM-320RD может передавать потоки мультимедийных данных от вашего компьютера (или устройства хранения информации) по беспроводной сети с высокой скоростью или с использованием кабеля Ethernet. Медиаплеер DSM-320RD обеспечит мгновенный доступ к аудио и видео информации и фотографиям и проигрывание/просмотр данных с помощью домашнего развлекательного центра.

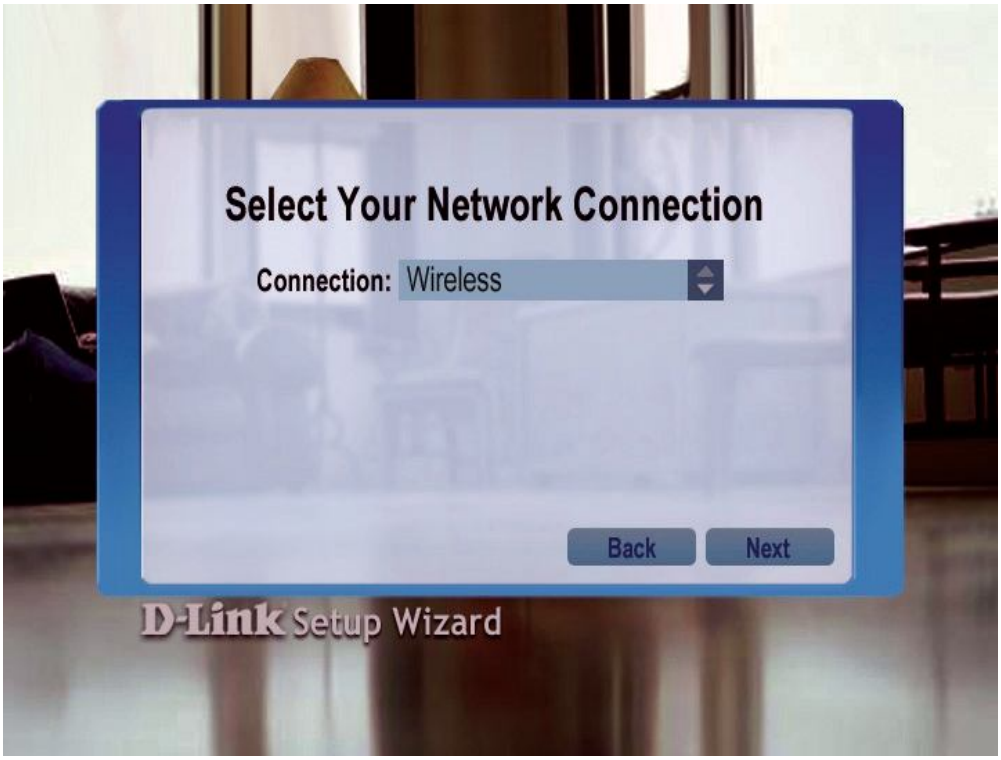
DSM-320RD легко интегрируется в существующую проводную или беспроводную сеть. Благодаря использованию метода построчной развертки, можно смотреть любимые DVD в высоком разрешении (используя телевизоры с высоким разрешением) с хорошим качественным звучанием. Кроме DVD-формата, DVD-плеер также поддерживает диски следующих форматов: SVCD, VCD, CD-R, DVD-RW, CD-RW, CD-MP3. DSM-320RD оборудован встроенным Card-ридером 5-в-1, который позволяет просматривать фотографии, аудио и

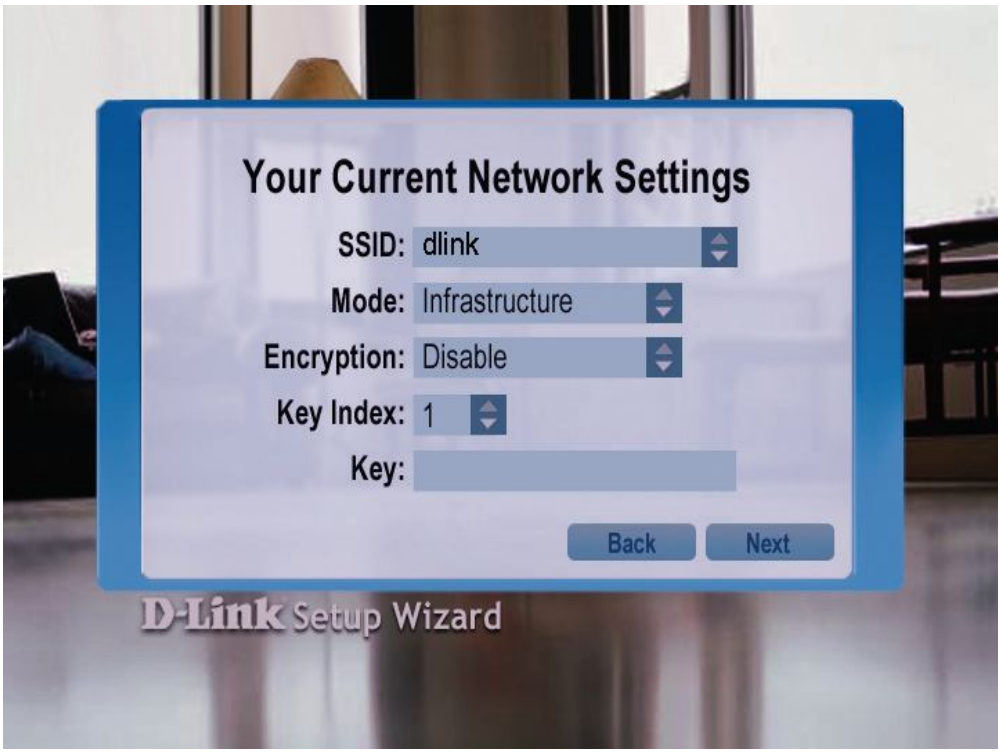
видео данные, хранящиеся на запоминающих устройствах. Поддерживаются следующие популярные типы устройств хранения информации: SD, Memory Stick, MMC, и Compact Flash (I и II типа).

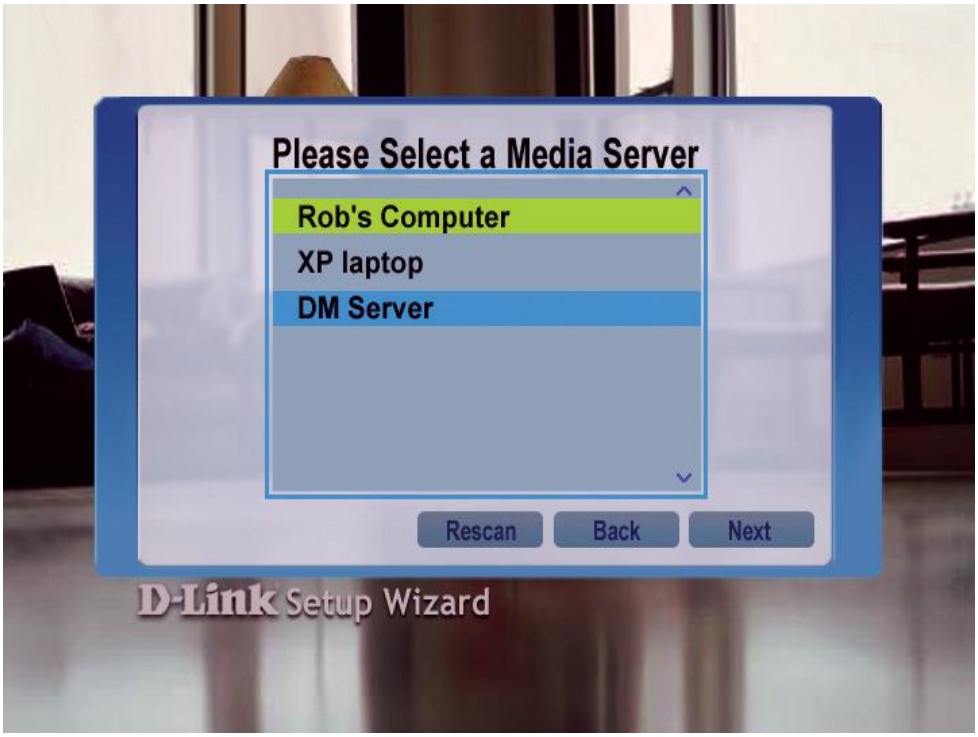
Можно получить доступ к тысячам песен из любой жилой комнаты вашего дома. Благодаря поддержке протокола WMC, музыкальные файлы (защищенные WMDRM) могут передаваться от вашего компьютера в любую комнату.

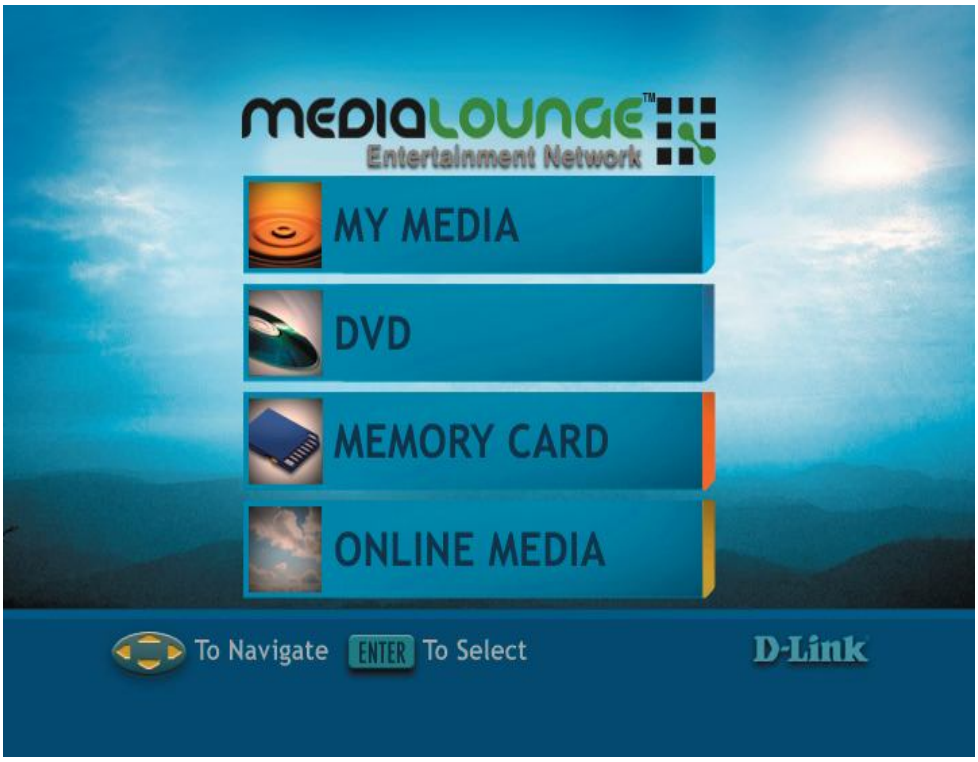
Медиаплеер DSM-320RD прост в установке. Благодаря поддержке протокола WCN (Windows Connect Now) настройка беспроводного соединения осуществляется проще, чем когда-либо ранее. Необходимо просто запустить Wireless Network Setup Wizard из Windows XP Service Pack 2 и перенести настройки беспроводной сети


Your Current Network Settings
Configuration: DHCP
IP Address: 192.168.0.28
Netmask: 255.255.255.0
Gateway: 192.168.0.1
DNS: 192.168.0.1
Back
Next
D-Link Setup Wizard


Select Your Network Connection
Connection: Wireless
Back
Next
D-Link Setup Wizard


Your Current Network Settings
SSID: dlink
Mode: Infrastructure
Encryption: Disable
Key Index: 1
Key:
Back
Next
D-Link Setup Wizard


Please Select a Media Server
Rob's Computer
XP laptop
DM Server
Rescan
Back
Next
D-Link Setup Wizard


MEDIALOUNGE™
Entertainment Network
MY MEDIA
DVD
MEMORY CARD
ONLINE MEDIA
To Navigate
ENTER
To Select
D-Link

5. ПРИЛОЖЕНИЕ В. Глоссарий

Формат: Список

1

3G (англ. third generation). Технологии мобильной связи 3 поколения — набор услуг, который объединяет как высокоскоростной мобильный доступ с услугами сети Интернет, так и технологию радиосвязи, которая создаёт канал передачи данных.

3GPP (англ. 3rd Generation Partnership Project). Рабочая группа, разрабатывающая спецификации для мобильной телефонии третьего поколения.

4G. Перспективное (четвёртое) поколение мобильной связи, характеризующееся высокой скоростью передачи данных и повышенным качеством голосовой связи. К четвёртому поколению принято относить перспективные технологии, позволяющие осуществлять передачу данных со скоростью, превышающей 100 Мбит/с.

8P8C (англ. 8 Position 8 Contact). Унифицированный разъём, используемый в телекоммуникациях, имеет 8 контактов и защёлку. Часто ошибочноhttp://ru.wikipedia.org/wiki/8P8C - cite_note-0 называется RJ45 или RJ-45.

10Base-F. Реализация стандарта IEEE 802.3 Ethernet с использованием оптического кабеля.

10Base-T. Спецификация IEEE 802.3i для сетей Ethernet с использованием неэкранированного кабеля на основе скрученных пар ("витая пара").

100Base-T. Спецификация IEEE 802.3us для сетей Ethernet со скоростью передачи 100 Мбит/сек на основе неэкранированного кабеля на основе скрученных пар ("витая пара").

100Base-TX. Часть спецификации IEEE 802.3u Ethernet для скорости 100 Мбит/с с использованием 2-пар неэкранированного медного кабеля категории 5.

100Base-FX. Часть спецификации IEEE 802.3u Ethernet для скорости 100 Мбит/с с использованием оптических кабелей и стандарта FDDI TP-PMD для PMD (физическая среда).

10Gbase-ER Оптический интерфейс 10G Ethernet, обеспечивающий передачу сигналов со скоростью 10 Гбит/с по одномодовому кабелю протяженностью около 40 км при длине волны оптического излучения 1550 нм.

10Gbase-LR. Оптический интерфейс 10G Ethernet, обеспечивающий передачу сигналов со скоростью 10 Гбит/с по одномодовому кабелю протяженностью более 10 км при длине волны оптического излучения 1310 нм.

10Gbase-SR. Оптический интерфейс 10G Ethernet, обеспечивающий передачу сигналов со скоростью 10 Гбит/с по многомодовому кабелю протяженностью до 300 метров при длине волны оптического излучения 850 нм.

10GEPON. (англ. 10 Гигабит EPON). Технология пассивных оптических сетей. Представляет собой расширение стандарта 802.3ah, EFM. Между коммутационным узлом и домашней сетью развертывается распределительная сеть, по которой через оптическое волокно подается 10 Гбит/с для 32 домохозяйств, до 20 км.

A

Access method. (Метод доступа). Набор правил, обеспечивающих арбитраж доступа к среде передачи. Примерами методов доступа являются CSMA/CD (Ethernet) и передача маркера (Token Ring).

Access Point. (Точка доступа). Обычно используется для обозначения беспроводной точки доступа.

ACSE. (англ.Application Common Service Elements). Общие элементы прикладного сервиса. См. так же SASE.

Address (Адрес). Уникальный идентификатор, присваиваемый сети или сетевому устройству для того, чтобы другие сети и устройства могли распознать его при обмене информацией.

Address mask. См. Маска подсети.

Address resolution (Разрешение адреса). Используется для преобразования адресов сетевого уровня (Network Layer) в обусловленные средой (media-specific) адреса. См. также ARP.

AirPlusXtremeG. Серия беспроводного оборудования компании D-Link

Agent (Агент). Применительно к SNMP термин агент означает управляющую систему.
В модели клиент-сервер - часть системы, выполняющая подготовку информации и обмен ею между клиентской и серверной частью.

Aggregate link (Агрегированный канал). Это объединение нескольких физических каналов в одну логическую магистраль.

AMI (англ. Alternate Mark Inversion). Метод биполярного кодирования с альтернативной инверсией.

ANSI (англ. American National Standards Institute). Американский национальный институт стандартов.

AP. См. Access Point.

Application Layer (Уровень приложений). Верхний уровень модели OSI, обеспечивающий такие коммуникационные услуги, как электронная почта и перенос файлов.

ARCnet (англ. Attached Resource Computer NETwork). Первая технология для создания ЛВС микрокомпьютеров.

ARP (англ. Address Resolution Protocol - протокол разрешения адресов). Протокол Internet, используемый для динамического преобразования адресов Internet в физические (аппаратные) адреса устройств локальной сети. В общем случае ARP требует передачи широковещательных сообщений всем узлам, на которое отвечает узел с соответствующим запросу IP-адресом.

ARPANET. Компьютерная сеть, послужившая прообразом для современной сети Интернет.

ASCII (англ. American Standard Code for Information Interchange). Семибитная кодировка для представления десятичных цифр, знаков препинания, латинских и специальных символов.

ATM (англ. Asynchronous Transfer Mode - асинхронный способ передачи данных). сетевая технология, основанная на передаче данных в виде ячеек (cell) фиксированного размера 53 байта, из которых 5 байтов используется под заголовок.

AUI (англ. attachment unit interface) - 15-ти штырьковый разъём для соединения порта сетевой платы устройства и контроллера Ethernet.

Autonegotiation. Автоопределение скорости и режима соединения между двумя Ethernet устройствами.

AWG (англ. American Wire Gauge System). Американская система оценки диаметра медных кабелей.

B

Bandwidth. См. Полоса пропускания

BER (англ. bit error rate). В сетях обозначает отношение количества ошибок к общему количеству переданных бит.

BGP (англ. Border Gateway Protocol). Протокол, обеспечивающий динамическую маршрутизацию в сети Интернет.

BNC-коннектор (англ. Bayonet Neill Concelman). Разъем, использующийся для подключения тонкого коаксиального кабеля.

Bridge (Мост)**.** Устройство, соединяющее две или несколько физических сетей и передающее пакеты из одной сети в другую. Мосты работают на канальном уровне OSI модели.

Broadcast. Система доставки пакетов, при которой копия каждого пакета передается всем узлам, подключенным к сети. Примером широковещательной сети является Ethernet.

Broadcast-шторм. Нарушение в работе ЛВС, вызванное лавинообразным распространением широковещательных пакетов. Приводит к перегрузке линий связи и увеличению нагрузки на все подключенные к ЛВС устройства.

Bus topology (Шинная топология). Топология сети, при которой в качестве среды передачи используется единый кабель (он может состоять из последовательно соединенных отрезков), к которому подключаются все сетевые устройства.

C

CAN (англ. campus area network, corporate area network). Сети кампусов, под которыми первоначально подразумевались университетские городки. В современных сетях применяется для обозначения распределенных СПД, размещенных на ограниченной территории (в том числе сети предприятий и коммерческих компаний).

CDDI (англ. Copper Distributed Data Interface). Вариант стандарта FDDI используя медный кабель.

Cenelec (франц. Comité Européen de Normalisation Electrotechnique). Европейский комитет электротехнической стандартизации.

Channel. См. Канал связи.

Chassis (Шасси). Специальная конструкция для установки модулей и других компонент, образующих вместе единое устройство. Шасси обеспечивает питание и соединяющую модули магистраль.

CIDR (англ. Classless Inter-Domain Routing) Технология бесклассовой междоменной маршрутизации. Регламентируется в RFC 1519.

CLI (англ. Command Line Interface- интерфейс командной строки). Позволяет пользователю взаимодействовать с операционной системой путем ввода текстовых команд.

Client (Клиент). Узел или программное обеспечение (внешнее устройство), которое запрашивает у сервера некоторые сервисы.

Collision. См. Коллизия.

CoS (англ. Class of Service - класс обслуживания). Характеристика, позволяющая определить, как протокол верхнего уровня использует протокол нижнего уровня для обработки его сообщений. Другое название ToS.

CRC (англ. cyclic redundancy check). Циклическая проверка четности с избыточностью, контрольная сумма.

Crossover (перекрестное соединение). Соединение (внешнее или внутреннее) передатчика на одном конце коммуникационного канала с приемником на другом его конце.

CSMA/CA (англ. Carrier Sense Multiple Access/Collision Avoidance - множественный доступ к среде с распознаванием несущей и избеганием коллизий). Метод доступа к среде передачи, применяемый в беспроводных сетях IEEE 802.11.

CSMA/CD (англ. Carrier Sense Multiple Access/Collision Detection - множественный доступ к среде с обнаружением конфликтов и распознаванием несущей). Метод доступа к среде передачи, применяемый в Ethernet и IEEE 802.3.

Cut-through packet switching (Сквозная коммутация пакетов). Способ коммутации, при котором данные проходят через коммутатор таким образом, что ведущий край пакета покидает коммутатор на выходном порте еще до того, как закончится прием пакета на входном порте. Устройство со сквозной коммутацией пакетов считывает, обрабатывает и передает пакеты сразу после определения адреса приемника и выходного порта. Этот способ также называется оперативной коммутацией пакетов.

CWDM (англ. Coarse WDM - «грубое» спектральное мультиплексирование). Технология мультиплексирования, базирующаяся на использовании оптических каналов, отстоящих друг от друга на расстоянии не менее 200 ГГц.

D

DA (англ. Destination Address). Адрес получателя (MAC или IP).

Data Link Layer (Канальный уровень). Уровень 2 в модели OSI, который обеспечивает надежную передачу данных по физическому соединению. Канальный уровень отвечает за физическую адресацию, сетевую топологию, дисциплину линии связи, уведомления об ошибках, упорядоченную доставку кадров и управление потоком. IEEE делит этот уровень на два подуровня: MAC и LLC.

DECnet. Стек протоколов, разработанный корпорацией DEC.

DECT (англ. Digital Enhanced Cordless Telecommunications). Стандарт цифровой беспроводной связи, обычно применяемый для беспроводных телефонов.

DHCP (англ. Dynamic Host Configuration Protocol - протокол динамической конфигурации узла). Обеспечивает механизм динамического распределения и повторного использования освобождаемых IP-адресов.

Diffserv (англ. Differentiated Services). Простой метод классификации, управления и предоставления качества обслуживания в современных IP сетях. Использует для своей работы поле DSCP. Регламентируется RFC 2475, 3260.

DIX. Сокращение по начальным буквам названий компаний DEC, Intel и Xerox, разработавшим первую версию стандарта Ethernet.

DNS (англ. Domain Name System). Служба преобразования доменного имени в IP-адрес. Является важной частью сети Интернет.

Domain name (Доменное имя). Символьное имя, служащее для идентификации областей административной автономии в сети Интернет. См. также DNS

DSCP (англ. Differentiated Services Code Point). Поле в заголовке IP пакета, используемое для классификации (приоритезации) передаваемой информации.

DSF (англ. Dispersion Shifted Single Mode Fiber). Одномодовое волокно со смещённой дисперсией.

DSL (англ. Digital Subscriber Line). Цифровая абонентская линия. Так же см. xDSL.

DSSS (англ. direct-sequence spread spectrum). Метод расширения спектра методом прямой последовательности. Модуляция, используемая в стандарте IEEE 802.11.

DTM (англ. Dynamic synchronous transfer mode**).** Технология построения оптических сетей, стандартизированная спецификацией ETSI ES 201 803-1.

DWDM (англ. Dense WDM). «Плотное» спектральное мультиплексирование. Технология мультиплексирования, базирующаяся на использовании оптических каналов, отстоящих друг от друга на расстоянии не менее 100 ГГц.

E

E1 Цифровой канал передачи данных, соответствующий первичному уровню европейского стандарта иерархии PDH.

EasySmart. См. Smart

EBCDIC (англ. Extended Binary Coded Decimal Interchange Code). Расширенная двоично-десятичная восьмибитная кодировка, разработанная корпорацией IBM для использования на мэйнфреймах собственного производства.

EDGE (англ. Enhanced Data rates for GSM Evolution). Технология увеличения скорости передачи данных в мобильных сетях.

EIA (англ. Electronics Industries Alliance). Альянс отраслей электронной промышленности США.

EMI (англ. Electromagnetic interference - электромагнитная интерференция). Взаимное наложение электромагнитных сигналов, из-за которых может нарушиться целостность сигналов и увеличиться частота ошибок в каналах передачи данных.

Enterprise (Предприятие). Применяется для обозначения крупных сетей масштабов предприятия.

Ethernet. Стандарт организации локальных сетей (ЛВС), описанный в спецификациях IEEE и других организаций. IEEE 802.3.

Ethernet address (Адрес Ethernet). 48-битовое значение, являющееся уникальным идентификатором устройства (порта Ethernet) в сети. Обычно записывается 12 шестнадцатеричными цифрами.

ETTH (англ. Ethernet to the Home - Ethernet до дома (квартиры)). Цель решения ETTH заключается в передаче данных, речи и видео по простой и недорогой сети Ethernet. Уникальным преимуществом данного решения является то, что использование Ethernet с оптическим волокном в качестве среды передачи данных позволяет обеспечить доступ к сети непосредственно из помещений клиентов услуг на высоких скоростях.

EV-DO (англ. Evolution-Data Optimized). Телекоммуникационный стандарт передачи данных в сетях мобильной связи 3-го поколения. Так же см. 3G.

ExpressCard. Интерфейс подключения внешних устройств к мобильным ПК через шину PCI-Express. В современных мобильных ПК заменил устаревший интерфейс PC-card.

F

FastEthernet. Группа сетевых протоколов, обеспечивающих передачу данных на скорости 100Мбит/с. Регламентируется стандартом IEEE 802.3.

Fault management (Контроль сбоев). Одна из пяти определенных ISO областей управления сетями. Основной задачей этой области сетевого управления является детектирование, изоляция и корректировка сбойных фрагментов сети.

Fault tolerance (Устойчивость к сбоям). Способность программы или системы корректно работать при возникновении сбоев. Устойчивые к сбоям системы создаются для обеспечения работы при отключении питания, повреждении дисков, серьезных ошибках пользователей и т.п.

FC. Тип оптического разъема. Иногда обозначается как FC/PC

FDDI (англ. Fiber Distributed Data Interface). Технология построения сети на двух оптических кольцах, работающих одновременно и обеспечивающих скорость работы каждое по 100Мбит/с.

Fibre Channel. Высокоскоростная технология, обычно использующаяся для подключения сетевых дисковых хранилищ в корпоративных сетях.

Fiber optic cable. Оптический кабель. Кабель, содержащий одно или несколько оптических волокон и предназначенный для передачи данных.

FIDOnet. Международная некоммерческая компьютерная сеть, популярная в 1990-х годах. Практически полностью вытеснена сетью Интернет.

Filtering (Фильтрация). Процесс проверки пакетов данных в сети и определения адресатов для принятия решения о дальнейшей пересылке (данная ЛВС, удаленная ЛВС) или отбрасывании пакета. Фильтрация пакетов выполняется мостами, коммутаторами и маршрутизаторами.

Flooding (Лавинная передача). Способ передачи трафика, используемый в коммутаторах и мостах, при котором полученный интерфейсом трафик пересылается всем другим интерфейсам этого устройства.

Flow control (Управление потоком). Методы, используемые для контроля за передачей данных между двумя точками сети и позволяющие избегать потери данных в результате переполнения приемных буферов.

FQDN (англ. fully qualified domain name). Полное доменное имя. Содержит составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой: www.dlink.ru

Frame. См. Кадр.

FTP (англ. File Transfer Protocol). Стандартный протокол копирования файлов между узлами через сети TCP/IP. Регламентируется RFC 959.

Full duplex. См. Полнодуплексный режим.

G

GBIC (англ. gigabit interface converter - сменный гигабитный конвертер). Стандартный интерфейс с «горячей заменой», обеспечивает подключение гигабитных модулей с различными физическими интерфейсами передачи данных. Так же см. SFP.

GEPON (англ. Gigabit Ethernet PON). Технология пассивных оптических сетей. Регламентируется IEEE 802.3ah.

GigabitEthernet. Группа сетевых протоколов, обеспечивающих передачу данных на скорости 1Гбит/с. Регламентируется IEEE 802.3.

GPON (англ. Gigabit PON). Технология пассивных оптических сетей. Регламентируется ITU-T G.984.

GreenEthernet. Энергосберегающая технология компании D-Link. Появилась раньше, чем аналогичный энергосберегающий стандарт IEEE 802.3az.

GUI (англ. Graphical User Interface - графический интерфейс пользователя). Метод взаимодействия между пользователем и компьютером, при котором пользователь может вызывать различные функции, указывая на графические элементы (кнопки) вместо ввода команд с клавиатуры.

H

Half Duplex. См. Полудуплексный режим.

HDTV (англ. high-definition television - телевидение высокой четкости). По сравнению с обычным телевидением имеет лучшие параметры видео - разрешение видеокадра до 1920×1080, скорость до 60 кадров/сек.

Hello-пакет. Пакеты данных, использующиеся в различных протоколах для обмена сообщениями.

Host. Компьютер или сервер, подключенный к локальной или глобальной сети Интернет.

I

IANA (англ. Internet Assigned Numbers Authority). Организация, занимающаяся распределением IP адресов в Интернет.

ICMP (англ. Internet Control Message Protocol). Один из протоколов стека TCP/IP, использующийся для передачи сообщений об ошибках и некоторых иных сервисных функций. Регламентируется RFC 792.

IEEE (англ. Institute of Electrical and Electronic Engineers - Институт инженеров по электротехнике и радиоэлектронике). Профессиональная организация, основанная в 1963 году для координации разработки компьютерных и коммуникационных стандартов. Членами IEEE являются ANSI и ISO.

IEEE 802 (Комитет IEEE 802). Один из комитетов IEEE, ответственный за разработку стандартов для локальных и городских сетей. Наибольшее распространение получили стандарты Ethernet, Token Ring, Wireless LAN.

IEEE 802.3. Спецификация IEEE для локальных сетей CSMA/CD.

IGMP (англ. Internet Group Management Protocol - межсетевой протокол управления группами). Протокол, используемый IP-узлами для уведомления смежных широковещательных маршрутизаторов об их участии в широковещательных группах. Регламентируется RFC 3376.

IGMP Snooping. Процесс прослушивания данных протокола IGMP, позволяющий оптимизировать передачу многоадресного трафика в сети.

IMT-2000 (англ. International Mobile Telecommunications 2000). Группа стандартов мобильной связи и передачи данных, так называемого 3-го поколения.

Intserv (англ. integrated services). Метод классификации, управления и предоставления гарантированного качества обслуживания в современных IP сетях. Использует для своей работы протокол RSVP. Регламентируется RFC 1633.

IPSec (англ. Internet Protocol Security). Группа протоколов для создания VPN-туннеля, обеспечивающего защиту передаваемых по протоколу IP данных

IPTV. Цифровое интерактивное телевидение в сетях передачи данных по протоколу IP.

IP (англ. Internet Protocol). Часть стека протоколов TCP/IP, определенного в RFC 791 . Описывает программную маршрутизацию пакетов и адресацию устройств. Стандарт используется для передачи через сеть базовых блоков данных

и дейтаграмм IP. Обеспечивает передачу пакетов без организации соединений и гарантии доставки.

IPv4. Четвёртая версия IP протокола, наиболее массово применяемая на момент написания книги.

IPv6. Шестая версия IP протокола, заменяющая устаревшую версию IPv4.

IPX/SPX. Стек протоколов, используемый в сетях Novell NetWare.

IP-адрес. Сетевой адрес хоста в компьютерной сети, построенной по протоколу IP.

IP-телефон. Телефон, в качестве транспортной среды передачи использующий сеть на базе протокола IP.

IP-телефония. См. VoIP.

ISO (International Organization for Standardization). Международная организация по стандартизации

ISO/OSI (Open Systems Interconnection Reference Model). Эталонная модель взаимодействия открытых систем, разработанная организацией ISO.

IT (англ. Information technology). Информационные технологии.

ITU (International Telecommunication Union). Международный союз электросвязи.

J

Jumbo-фрейм. Сверхдлинные Ethernet-кадры, позволяющие увеличить производительность передачи данных в сети и снизить нагрузку на центральный процессор за счет уменьшения служебной информации в теле пакетов (сокращения количества заголовков).

L

L2F (англ. Layer 2 Forwarding Protocol). Протокол туннелирования канального уровня для создания виртуальных частных сетей связи через Интернет. Регламентируется RFC 2341.

L2 switch. Коммутатор второго уровня, обрабатывающий кадры на втором уровне модели ISO/OSI, используя MAC адреса в теле пакетов.

L2TP (англ. Layer 2 Tunneling Protocol). Сетевой протокол туннелирования канального уровня, сочетающий в себе протоколы L2F и PPTP. Регламентируется RFC 3931.

L3 switch. Коммутатор третьего уровня, обрабатывающий кадры не только на втором уровне (см. L2 switch), но и на третьем уровне модели ISO/OSI, как правило, используя IP-адреса в теле пакетов. Часто применяется название «маршрутизирующий коммутатор».

LAN (англ. Local Area Network). См. ЛВС.

LC. Тип оптического разъема, замещающий в сетевом оборудовании более крупные разъемы SC. Именно этот тип разъема применяется в SFP модулях.

LLC (англ. Logical Link Control). Подуровень управления логическим соединением. Высший из двух подуровней канального уровня, определенный IEEE. Управляет обработкой ошибок, потоками, кадрированием, а также адресацией MAC-подуровня. Наиболее распространенным LLC-протоколом является IEEE 802.2.

LSZH (англ. Low Smoke Zero Halogen). Маркировка кабелей, для изготовления оболочки которых используются полимеры, не поддерживают горения и не выделяющие при нагреве ядовитые галогены.

LTE (англ. Long Term Evolution). Новейший стандарт сотовой связи, который должен прийти на замену сетей 3G.

M

MAC (англ. Media Access Control - управление доступом к передающей среде). Низший из двух подуровней канального уровня, определенный IEEE. MAC-подуровень управляет доступом к совместно используемым носителям. См. так же LLC.

MAC address (MAC-адрес). Стандартный адрес сетевого адаптера на канальном уровне в сетях Ethernet.

Mainframe. Высокопроизводительный компьютер со значительным объёмом оперативной и внешней памяти, предназначенный для организации централизованных хранилищ данных большой ёмкости и выполнения интенсивных вычислительных работ.

MAN (англ. metropolitan area network). Крупная сеть, покрывающая город или крупный кампус. Обычно объединяет несколько ЛВС через высокоскоростную магистраль.

MDI (англ. medium dependent interface). Ethernet-порт абонентского устройства, например, сетевой карты ПК.

MDI-X (medium dependent interface with Crossover). Ethernet-интерфейс с перекрёстным подключением. Используется в Ethernet-коммутаторах.

Metro Ethernet. См. MAN

MIB (англ. Management Information Base - база управляющей информации). База данных, где хранится информация для управления сетью, которая используется и поддерживается протоколом сетевого управления SNMP.

MII (англ. Media Independent Interface - независящий от среды передачи интерфейс). Представляет собой стандартизованный интерфейс для подключения MAC-блока сети Ethernet (канальный уровень) к блоку PHY (физический уровень).

MIMO (англ. Multiple Input Multiple Output). Технология использования сразу нескольких приёмо-передатчиков. Позволяет улучшить характеристики канала связи.

MiniGBIC. См. SFP.

MLT-3 (англ. Multi-Level Transmit). Метод кодирования сигнала, использующий три уровня напряжения сигнала.

MMF (англ. Multi-mode optical fiber). Многомодовый оптический кабель.

MPLS (англ. Multiprotocol Label Switching - мультипротокольная коммутация по меткам). Метод передачи данных, эмулирующий различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов. Регламентируется RFC 3031.

MTRJ (англ. Mechanical Transfer Registered Jack**).** Тип оптического разъема, внешне напоминающего разъем 8P8C (RJ-45). В одном разъеме сразу объединены две оптические жилы.

MTU (англ. Maximum Transmission Unit - модуль передачи максимального размера). Максимальный размер (в байтах) пакета данных, который можно передать через данный интерфейс.

Multicast (Многоадресная рассылка). Режим копирования одиночных пакетов и их передачи заданному подмножеству сетевых адресов. Эти адреса задаются в поле адреса получателя.

Multicast address (Групповой адрес). Общий адрес, который относится к некоторой группе нескольких сетевых устройств.

Multicast group (Многоадресная группа). Динамически определенная группа IP-узлов, идентифицируемая одним групповым IP-адресом.

MUX. См. Мультиплексор.

N

NAT (англ. Network Address Translation - преобразование сетевых адресов). Метод в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.

NetBEUI (англ. NetBIOS Extended User Interface). Реализация протокола NetBIOS корпорацией Microsoft.

NetBIOS (англ. Network Basic Input/Output System). API, используемый программами в ЛВС.

Netware. См. Novell Netware

Network (Сеть).
1. Соединение группы узлов (компьютеров или других устройств).
2. Группа точек, узлов или станций, соединенных коммуникационными каналами и набор оборудования, обеспечивающего соединение станций и передачу между ними информации.

Network Address (Сетевой адрес). Адрес сетевого уровня, который относится к логическому, а не к физическому сетевому устройству.

Network Layer (Сетевой уровень). Уровень 3 модели OSI, отвечающий за маршрутизацию, переключение и доступ к подсетям через всю среду OSI.

NEXT (англ. Near End Crosstalk). Интерференция между парами в кабеле, измеряемая со стороны передатчика.

NFS (англ. Network File System). Протокол, позволяющий клиенту обращаться к файлам по сети так, как будто они расположены локально. Регламентируется RFC 1094, 1813, 3530.

NIC (англ. Network Interface Controller). Сетевая плата, также известная как сетевая карта, сетевой адаптер, Ethernet-адаптер — периферийное устройство, позволяющее компьютеру взаимодействовать с другими устройствами сети.

Node (Узел). Точка присоединения к сети, устройство, подключенное к сети.

Novell Netware. Сетевая операционная система компании Novell.

NRZ (англ. Non Return to Zero). Потенциальный код без возвращения к нулю.

NRZI (англ. Non Return to Zero with ones Inverted). Потенциальный кодом с инверсией при единице.

Nway. См. Autonegotiation.

NZDSF (англ. NZDSF - Non-Zero Dispersion Shifted Single Mode Fiber). Одномодовое волокно с ненулевой смещённой дисперсией.

NVRAM (англ. NonVolatile RAM - энергонезависимое ОЗУ). Оперативное запоминающее устройство, содержимое которого сохраняется при отключении питания.

O

OC-192 (англ. Optical Carrier transmission rates). Стандартизированная скорость в оптических сетях SONET, равная 9.95 Гбит/с. Так же существуют скорости OC-48 (скорость 2.48Гбит/с), OC-768 (39.8Гбит/с), и ряд других.

OSI. См. ISO/OSI.

OSPF (англ. Open Shortest Path First). Протокол динамической маршрутизации для IP-сетей. Регламентируется RFC 2328, 5340.

OTN (англ. Optical Transport Network). Набор оптических сетевых элементов, связываемых оптоволоконными линиями, способными обеспечить функции транспорта, мультиплексирования, коммутации, управления, контроля и живучести оптических каналов.

P

Packet (Пакет**).** Группа байт, включающая данные и служебные поля, представленные в соответствующих форматах, и передаваемая целиком.

PAM (англ. Pulse Amplitude Modulation). См. ИКМ.

PCMCIA. См. PC Card.

PC Card. Устаревший интерфейс подключения внешних устройств к мобильным ПК через шину PCI. В современных мобильных ПК заменяется интерфейсом ExpressCard.

PCS (англ. Physical Coding Sublayer). Подуровень физического кодирования в семействе протоколов Ethernet.

PDU (англ. Protocol Data Unit - модуль данных протокола). Термин OSI для пакетов данных.

PHY. См. Physical Layer.

Physical Layer (Физический уровень). Уровень 1 модели OSI. Определяет электрические, механические, процедурные и функциональные спецификации для создания, поддержки и разрыва физического соединения между конечными системами.

Ping (англ. Packet INternet Groper - проверка доступности адресата). Инструмент, используемый для проверки доступности адресата в IP-сетях.

PKI (англ. PKI - Public Key Infrastructure). Технология аутентификации с помощью открытых ключей.

PMA (англ. Physical Medium Attachment). Один из подуровней физического уровня в Ethernet. Обеспечивает преобразование кодовых групп в последовательный сигнал (serialize) и обратно (deserialize).

PMD (англ. Physical Media Dependent). Один из подуровней физического уровня в Ethernet. Отвечает за передачу последовательности битов в физическую среду через MDI.

PoE (англ. Power over Ethernet). Технология, позволяющая передавать удалённому устройству вместе с данными электрическую энергию через стандартную витую пару в сети Ethernet.
Регламентируется IEEE 802.3af.

PON (англ. passive optical network - пассивные оптические сети). См. GPON и GEPON.

POP3 (англ. Post Office Protocol Version 3). Протокол приема электронной почты с почтового сервера, применяется в сетях IP. Регламентируется RFC 1939, См. так же SMTP.

PPP (англ. Point-to-Point Protocol). Протокол канального уровня. Применяется для организации связи точка-точка между двумя хостами. Регламентируется RFC 1661.

PPPoA (англ. PPP over ATM). Реализация протокола PPP для сетей ATM. Регламентируется RFC 2364.

PPPoE (англ. PPP over Ethernet). Реализация протокола PPP для сетей Ethernet. Регламентируется RFC 2516.

PPTP (англ. Point-to-Point Tunneling Protocol). Протокол для создания VPN-туннеля, обеспечивающего защиту передаваемых по протоколу TCP данных. Регламентируется RFC 2631.

PVC (поливинилхлорид). Не горючий пластик, применяющийся в производстве кабеля.

PVC (англ. Permanent Virtual Circuit). Постоянный виртуальный канал (в ATM).

Proxy ARP (англ. Proxy Address Resolution Protocol). Агент протокола разрешения адресов. Вариант протокола ARP, в котором промежуточное устройство (например, маршрутизатор) посылает ответ ARP от имени конечного узла запрашивающему хосту.

Q

QoS (англ. Quality of Service - качество обслуживания). Предоставление приоритезации различным приложениям, пользователям или потокам трафика, или гарантия определенного уровня производительности потока данных.

R

RADIUS (англ. Remote Authentication Dial-In User Service - служба аутентификации удаленных пользователей). Обеспечивает аутентификацию, проверку полномочий и другие операции при доступе в сеть удаленных пользователей по коммутируемым линиям. Регламентируется RFC 2865, 2866.

Redundancy (Избыточность). Дублирование устройств, сервисов и соединений. В случае неисправности позволяет избыточным устройствам, службам и соединениям выполнять функции неисправных.

Redundant system (Избыточная система). Компьютер, маршрутизатор, коммутатор или другая система, которая содержит два или более экземпляра наиболее важных подсистем, таких как дисководы, центральные процессоры или источники питания.

Reliability (Надежность). Соотношение ожидаемых и полученных по каналу вспомогательных элементов сетевых служб. Чем выше это соотношение, тем надежнее линия.

RIP (англ. Routing Information Protocol). Протокол динамической маршрутизации для IP сетей. Регламентируется RFC 1058, 2453.

RIPNg. Протокол RIP для протокола IPv6. Регламентируется RFC 2080.

RISC-архитектура (англ. Restricted (reduced) instruction set computer) - архитектура процессора, в которой быстродействие увеличивается за счёт упрощения инструкций, что делает их декодирование проще, а время выполнения - меньше.

RJ-45. См. 8P8C.

RMON (англ. Remote MONitoring - удаленный мониторинг). Спецификация MIB-агента, которая определяет функции удаленного мониторинга сетевых устройств. Спецификация RMON предоставляет многочисленные возможности для мониторинга, определения неисправностей и отчетности. Регламентируется RFC 1271.

RoHS (англ. Restriction of Hazardous Substances) — действующая на территории Европейского Союза директива, ограничивающая содержание вредных веществ в телекоммуникационном оборудовании, среди прочего.

Router (Маршрутизатор). Устройство сетевого уровня, отвечающее за принятие решений о выборе одного из нескольких путей передачи сетевого трафика. Маршрутизаторы отправляют пакеты из одной сети в другую на основе информации сетевого уровня.

RS-232. Стандарт EIA для 25-контактного последовательного интерфейса, используемого для соединения ПК или терминалов (DTE) с коммуникационным оборудованием (DCE) типа модемов.

Rx (англ. receive). Используется для обозначения приемника или приемных линий интерфейса.

S

SA (англ. Source Address). Адрес отправителя (MAC или IP).

SafeGuard. В коммутаторах D-Link функция защиты процессора от перегрузки.

SASE (англ. Specific Application Service Elements). Специальные элементы прикладного сервиса. См. так же ACSE.

SC. Тип оптического разъема.

SDH (англ. Synchronous Digital Hierarchy). Стандартизированный мультиплексирующий протокол для передачи множественных потоков данных через оптические или электрические (для низких скоростей) интерфейсы. В некоторыми исключениями протокол SDH можно воспринимать как усовершенствованный протокол SONET.

SDLC (англ. Synchronous Data Link Control). Протокол канального уровня, разработанный IBM.

Segment. См. Сегмент.

Session Layer (Сеансовый уровень). Уровень 5 модели OSI, обеспечивающий способы ведения управляющего диалога между системами.

SFP (англ. small form-factor pluggable). Компактный сменный трансивер, часто называемый mini-GBIC. Стандартный интерфейс с «горячей заменой», обеспечивает подключение как гигабитных, так и стомегабитных модулей с оптическими интерфейсами передачи данных. Благодаря меньшим размерам, по сравнению с GBIC, позволяет получить большую плотность портов на одно устройство.

SHA (англ. Sender hardware address). В протоколе ARP - физический адрес отправителя. логический адрес отправителя (Sender protocol address, SPA).

SLIP (англ. Serial Line Internet Protocol (SLIP). Протокол канального уровня для инкапсуляции IP протокола при работе через последовательный порт или модем. Регламентируется RFC 1055.

Smart. В продуктовой линейке D-Link обозначает настраиваемые коммутаторы.

SMB (англ. small and medium businesses - малый и средний бизнес). Применяется для обозначения сетей относительно небольших организаций предприятия.

SMF (англ. Single Mode Fiber). Одномодовый оптический кабель.

SMTP (англ. Simple Mail Transfer Protocol). Простой протокол передачи электронной почты, применяется в сетях IP. Регламентируется RFC 5321 См. так же POP3.

Sniffer. Программа или программно-аппаратный комплекс для анализа сетевого трафика.

SNA (англ. System Network Architecture). Сетевая архитектура, разработанная компанией IBM и взятая за основу при создании эталонной модели ISO/OSI.

SNMP (англ. Simple Network Management Protocol - простой протокол управления сетью). Протокол, используемый почти исключительно в сетях TCP/IP для контроля и управления сетевыми устройствами, конфигурациями, производительностью и безопасностью, а также сбора статистической информации.

SOHO (англ. Small Office, Home Office - малый и домашний офис). Сетевые комплексы и технологии доступа для офисов, не имеющих прямого подключения к крупным корпоративным сетям.

SONET (англ. Synchronous Optical Networking). Стандартизированный мультиплексирующий протокол для передачи множественных потоков данных через оптические или электрические (для низких скоростей) интерфейсы. Так же см. SDH.

SSAP (англ. Source Service Access Point). Адрес точки входа сервиса источника на подуровне LLC в Ethernet-кадре.

SSL (англ. Secure Socket Layer). Протокол шифрования данных на транспортном уровне. См. TLS.

SPA (англ. Sender protocol address). В протоколе ARP – логический адрес отправителя.

ST. Тип оптического разъема.

Store and forward packet switching (коммутация пакетов с промежуточным хранением). Методика коммутации пакетов, согласно которой кадры полностью обрабатываются перед их отправкой через соответствующий порт. Обработка включает расчет CRC и проверку адреса приемника.

STM-64 (англ. Synchronous Transport Module). Стандартизированная скорость в оптических сетях SDH, равная 9.95 Гбит/с. Так же существуют скорости STM-1 (скорость 155 Мбит/с), STM-4 (622 Мбит/с), и ряд других.

Switch. См. Коммутатор.

Switched LAN. См. Коммутируемая сеть.

T

T1. Цифровой канал передачи данных, соответствующий первичному уровню американского стандарта иерархии PDH.

Tag. Идентификационная информация, в том числе и номер.

TCP (англ. Transmission Control Protocol - протокол управления передачей). Ориентированный на соединение протокол транспортного уровня, обеспечивающий надежную дуплексную передачу данных. TCP входит в набор протоколов TCP/IP.

TCP/IP (англ. Transmission Control Protocol/Internet Protocol - протокол управления передачей/ Интернет –протокол). Общее название набора протоколов, разработанных министерством обороны США в 1970-е гг. для всемирного сетевого комплекса.

TDM (англ. Time Division Multiplexing), техника мультиплексирования с разделением времени.

TDMA (англ. Time division multiple access). Множественный доступ с разделением по времени. Способ использования радиочастот, когда в одном частотном интервале находятся несколько передающих абонентов и разные абоненты используют разные временные слоты (интервалы) для передачи.

Telnet. Стандартный протокол виртуального терминала из набора протоколов TCP/IP. Протокол Telnet используется для удаленного терминального соединения, что дает возможность пользователям подключаться к удаленным системам и использовать их ресурсы, как если бы они работали через обычный терминал. Регламентируется RFC 137.

TFTP (англ. Trivial File Transfer Protocol - простейший протокол передачи файлов. Упрощенная версия протокола FTP, который позволяет компьютерам обмениваться файлами по сети. Регламентируется RFC 1350.

Throughput (Пропускная способность). Объем информации, поступающей и, возможно, проходящей через определенный участок сети в определенный момент времени.

TIA (англ. Telecommunications Industry Association). Ассоциация телекоммуникационной промышленности США — ассоциация изготовителей средств связи, разрабатывающая стандарты на кабельные системы.

TLS (англ. Transport Layer Security). Протокол шифрования данных на транспортном уровне. Является дальнейшим развитием протокола SSL. Регламентируется RFC 5246.

Token Bus (Маркерная шина). Протокол, описывающий метод построения сети таким образом, как будто компьютеры связаны в кольцо. Физическая топология при этом – «шина». Регламентируется IEEE 802.4.

Token Ring (Маркерное кольцо). Протокол, описывающий метод построения сети таким образом, как будто компьютеры связаны в кольцо. Физическая топология при этом не ограничена и может быть как «кольцом», так и «звездой», но логическая - всегда «кольцо». Регламентируется IEEE 802.5.

TPA (англ. Target protocol address). В протоколе ARP – логический адрес получателя.

Traffic segmentation (Сегментация трафика). Функция, используемая в коммутаторах для разграничения доменов на уровне 2.

Transport Layer (Транспортный уровень). Уровень 4 модели ISO/OSI, отвечающий за надежную передачу данных между конечными системами.

Trunk (Магистраль). Физическое и логическое соединение между двумя коммутаторами, по которому передается сетевой трафик. Основная магистраль состоит из нескольких магистралей.

В коммутаторах D-Link так же обозначает Link Aggregation.

TTL (англ. Time to live). Максимальное время «жизни» пакета в сетях IP. Может измеряться как в секундах, так и в количестве переходов.

Tx (англ. transmit) Используется для обозначения передатчика или передающих линий интерфейса.

U

UDP (англ. User Datagram Protocol - протокол дейтаграмм пользователя). Протокол транспортного уровня, не требующий подтверждения соединения. Входит в стек TCP/IP. UDP обеспечивает обмен дейтаграммами без подтверждения и гарантий доставки.

UL (англ. Underwriters Labs). Независимая лаборатория, проводящая сертификацию по безопасности.

Unicast (одноадресная передача). Пакет данных, доставляемый единственному адресату.

Unit (юнит). Единица измерения высоты телекоммуникационного оборудования, равная 44,45 мм (1,75 дюйма). Обозначается как 1U, 42U и т.д.

Unix. Общее название семейства сетевых операционных систем.

USB (англ. Universal Serial Bus - универсальная последовательная шина). Последовательный интерфейс передачи данных для периферийных устройств в вычислительной технике.

V

VLAN (англ. Virtual LAN - виртуальная локальная сеть). Группа устройств, принадлежащих одной или нескольким локальным сетям и сконфигурированных таким образом (при помощи программного обеспечения), что обмен данными между ними происходит так, как будто они подключены к одному кабелю, хотя на самом деле находятся в разных сегментах локальной сети. VLAN основаны на логическом соединении.

VLSM (англ. Variable Length Subnet Mask). В протоколе IP - переменная длина маски подсети в бесклассовой адресации.

VoIP (англ. Voice over IP – голос через IP). Система связи, обеспечивающая передачу речевого сигнала по любым IP-сетям. См. так же IP-телефон.

VPN (англ. Virtual Private Network - виртуальная частная сеть). Обобщённое название технологий, позволяющих обеспечить сетевое логическое соединение поверх другой сети, обычно называемое «VPN-туннель».

W

WAN (англ. Wide Area Network) - компьютерная сеть, охватывающая большие территории и включающая в себя большое число компьютеров.

WDM (англ. Wavelength-division multiplexing). Мультиплексирование с разделением по длине волны. Технология одновременной передачи нескольких информационных каналов по одному оптическому волокну на разных несущих частотах. Так же см. CWDM и DWDM.

WebSmart. См. Smart.

WECA. См WiFi Alliance.

WEP (англ. Wired Equivalent Privacy). Устаревший протокол обеспечения безопасности сетей Wi-Fi. См. WPA.

WHDI (англ. Wireless Home Digital Interface). Стандарт беспроводной передачи HD-видео с любого источника на устройство видеовывода (например, телевизор).

Wi-Fi, IEEE 802.11 — набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2,4; 3,6 и 5 ГГц. Фактически являющийся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance.

WiFi Alliance. Объединение крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi.

WiGig (англ. Wireless Gigabit Alliance). Организация, разрабатывающая решения для мультигигабитной беспроводной связи на небольшом расстоянии в диапазоне частот 60 ГГц.

WiMax (англ. Worldwide Interoperability for Microwave Access). Телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN.

Windows. Общее название семейства сетевых операционных систем.

Wireless PAN (англ. Wireless Personal Area Network). Беспроводные персональные сети, предназначенные для связи сетевых устройств на малом расстоянии. Регламентируется IEEE 802.15.

WPA (англ. Wi-Fi Protected Access). Протокол обеспечения безопасности сетей Wi-Fi. Устраняет все недостатки протокола WEP.

WWW (англ. World Wide Web - всемирная паутина. Распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к Интернету.

X

X.25. Устаревшее семейство протоколов канального уровня, применявшееся в WAN-сетях на основе коммутируемых или выделенных линиях.

xDSL. Семейство технологий, использующих телефонные провода для передачи цифровых данных.

XFP (англ. 10 Gigabit small form-factor pluggable). Компактный сменный трансивер. Стандартный интерфейс с «горячей заменой», обеспечивает подключение на скорости 10Гбит/с модулей с оптическими интерфейсами передачи данных. Так же см. SFP.

XOR. Логическая функция «исключающее ИЛИ».

xStack. Название серии управляемых коммутаторов D-Link.

А

АМ. Амплитудная модуляция.

Анализатор трафика. См. Sniffer.

АЦП. Аналого-цифровой преобразователь.

АЧХ. Амплитудно-частотная характеристика.

Б

Байт. Единица хранения и обработки цифровой информации, состоящая из 8 бит.

«Белый» адрес. В основном применяется при описании NAT. Обозначает внешний IP-адрес.

Бит. наименьшая базовая единица измерения количества информации.

Бод. Количество изменений информационного параметра несущего периодического сигнала в секунду.

В

ВЛС. Воздушные линии связи.

ВОЛС. Волоконно-оптические линии связи.

Всемирная паутина. См. WWW.

Вт. В системе СИ единица измерения мощности.

Г

ГВС. См. WAN.

Д

дБ. См. Децибел.

Дейтаграмма. Единица данных протокола UDP.

Децибел. Логарифмическая единица уровней, затуханий и усилений.

Домен. Единиц административной автономии в сети Интернет.

З

Затухание. Относительное уменьшение амплитуды или мощности сигнала при передаче по линии сигнала определенной частоты.

И

ИАМ. Импульсно-амплитудная модуляция.

ИКМ. Импулъсно-кодовая модуляция.

Интернет. Всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных. Является транспортной сетью для «Всемирной паутины» (WWW).

Интерфейс. Совокупность средств, методов и правил взаимодействия между элементами системы. Применительно в компьютерным сетям – точка соединения сетевых устройств.

Интранет. Внутренняя частная сеть организации, построенная на тех же самых принципах, что и глобальная сеть Интернет.

ИТ. Информационные технологии.

К

Кабель. Изделие, состоящее из проводников (металлических или оптических), слоев экрана и изоляции.

Кадр. Единица передачи данных на канальном уровне модели ISO/OSI.

Кампус. Университетский городок. **См. CAN**

Канал связи. Система технических средств и среда распространения сигналов для передачи сообщений от источника к получателю и обратно.

Коллизия. Возникает в сети Ethernet, когда два узла одновременно ведут передачу. Передаваемые ими по физическому носителю кадры «сталкиваются» и разрушаются.

Коммутатор. Сетевое устройство, которое фильтрует, пересылает и направляет кадры в зависимости от их адреса приемника. Коммутатор работает на канальном уровне модели ISO/OSI.

Коммутатор 2-го уровня. См. L2 switch.

Коммутатор 3-го уровня. См. L3 switch.

Коммутируемая сеть. Локальная сеть, построенная на коммутаторах.

Компьютер. Электронная вычислительная машина.

Концентратор. Устаревшее сетевое устройство, предназначенное для объединения нескольких устройств Ethernet в общий сегмент сети. Концентратор работает на физическом уровне модели ISO/OSI.

КПК. Карманный персональный компьютер.

Кросс-овер. См. Crossover.

Л

ЛВС. Высокоскоростная компьютерная сеть, покрывающая относительно небольшую территорию или группу зданий. В отличии от глобальной вычислительной сети, ЛВС имеет меньшие географические размеры и большую скорость работы.

Линия связи. Совокупность физических цепей и (или) линейных трактов систем передачи, имеющих общие линейные сооружения, устройства их обслуживания и одну и ту же среду распространения. В простейшем случае проводная линия связи - физическая цепь, образуемая парой металлических проводников.

М

MAC-адрес. См. MAC address.

Маршрутизация. В сетях связи - процесс определения маршрута следования информации.

Маршрутизирующий коммутатор. См. L3 switch.

Маска подсети. В протоколе IP битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая - к адресу самого узла в этой сети.

Модель DOD (англ. Department of Defense, Министерство обороны США) - модель сетевого взаимодействия, практической реализацией которой является стек протоколов TCP/IP.

МСЭ. См. ITU.

Мультиплексор. Комбинационное устройство, обеспечивающее передачу в желаемом порядке цифровой информации, поступающей по нескольким входам на один выход. Может быть реализован как аппаратно так и программно.

Мэйнфрейм. См. Mainframe.

О

ОС. Операционная система.

Открытая система. Аппаратура и/или программное обеспечение, которое обеспечивает переносимость и совместимость, а часто и их вместе с другими компьютерными системами.

П

Пакет. Сообщения сетевого уровня модели ISO/OSI.

Патч-корд. Коммутационный кабель.

ПК. Персональный компьютер.

ПО. Программное обеспечение.

Полнодуплексный режим. Способность канала в каждый момент времени одновременно передавать и принимать информацию.

Полоса пропускания. Диапазон между самой высокой и самой низкой частотой, доступной для передачи сетевых сигналов. Диапазон частот измеряется в герцах (Гц).

Полудуплексный режим. Способность канала в каждый момент времени только передавать или принимать информацию. Прием и передача, таким образом, должны выполняться поочередно.

Помехи. Электрические возмущения, возникающие в самой аппаратуре или попадающие в нее извне.

Последняя миля. Канал, соединяющий конечное (клиентское) оборудование с узлом доступа оператора связи. Иногда называется «первая миля».

Преамбула. В системах связи используется для того, чтобы дать время и возможность схемам приемопередатчиков прийти в устойчивую синхронизацию с принимаемыми тактовыми сигналами.

Р

РосНИИРОС. Российский научно-исследовательский институт развития общественных сетей, одной из целью которого является развитие базовых элементов инфраструктуры российского сегмента сети Интернет.

РСПД. Распределенная сеть передачи данных.

С

Сегмент.
1. Секция сети, ограниченная мостами, маршрутизаторами или коммутаторами.
2. В LAN с шинной топологией – непрерывная электрическая цепь, часто соединенная с другими сегментами при помощи повторителей.
3. Термин, используемый в спецификации TCP для описания одиночного модуля транспортного уровня.

Сервер. Компьютер (или специальное компьютерное оборудование), выделенный и/или специализированный для выполнения определенных сервисных функций. Так же - программное обеспечение, принимающее запросы от клиентов.

«Серый» адрес. В основном, применяется при описании NAT. Обозначает внутренний IP-адрес.

Сетевая карта. См. NIC.

Сетевая модель ISO/OSI. См. ISO/OSI.

Сетевая топология. Способ описания конфигурации сети, схема расположения и соединения сетевых устройств.

Сетевой адаптер. См. NIC.

Сетевой администратор. Человек, ответственный за работу локальной сети или её части.

Сеть связи. Совокупность технических средств, обеспечивающих передачу и распределение сообщений.

Симплексный режим. Способность канала передавать информацию только в одном направлении. Прием и передача, таким образом, должны выполняться на разных каналах.

Системный администратор. Сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения, а также обеспечение информационной безопасности в организации. Так же см. Сетевой администратор.

СКС. Структурированная кабельная система.

Сниффер. См. Sniffer.

Сообщение. Единица данных, которой оперирует прикладной уровень модели ISO.

СПД. Сеть передачи данных.

Спектральное уплотнение каналов. См. WDM.

Спецификация. В вычислительной технике - формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик.

Стек OSI. См. ISO/OSI

СУБД. Система управления базой данных.

Т

Транзакция. В информатике - группа последовательных операций, которая представляет собой логическую единицу работы с данными.

Тег. См. Tag.

Ф

Фрейм. См. Кадр.

Х

Хаб. См. Концентратор.

Хост. См. Host.

Ц

ЦАП. Цифро-аналоговый преобразователь.

Ч

ЧМ. Частотная модуляция.

Ш

Широковещание. См. Broadcast.

Широковещательный шторм. См. Broadcast-шторм.

Э

ЭВМ. Электронно-вычислительная машина, компьютер.

Литература:

1. Сайт D-Link. http://www.dlink.ru;
2. Документация, материалы презентаций и учебных курсов компании D-Link;
3. Компьютерные сети. Принципы, технологии, протоколы. Изд. третье/ В. Г. Олифер, Н. А. Олифер. - СПб.: Питер, 2006. - 958 с.: (Гл. 1-7).
4. Основы сетевых технологий : учеб. пособие для нач. проф. образования / С.В.Киселев, И.Л.Киселев. — М. : Издательский центр «Академия», 2008. — 64 с.;
5. Основы сетевых технологий: Учеб пособие. А.В Горячев, Н.Е. Новакова, А. В. Нисковский, С.В. Полехин., СПб.: Изд-во СПбГЭТУ«ЛЭТИ», 2000. 64 с.
6. Вычислительные машины, сети и телекоммуникационные системы: Учебно-методический комплекс. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. – М.: Изд. центр ЕАОИ. 2009. – 292 с.
7. Системы передачи информации. Курс лекций. С.В.Кунегин. М.,; в/ч 33965, 1997, - 317 с;
8. Учебно - Информационный Портал, основные технологии протоколы и стандарты связи. http://www.connect-portal.info ;
9. Свободная универсальная интернет-энциклопедия Википедия, http://ru.wikipedia.org ;
10. Сайт IETF (доступ к документам RFC) http://tools.ietf.org/html/ ;
11. Сайт IEEE (доступ к стандартам группы 802) http://standards.ieee.org/about/get/index.html .