МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВНОЕ УПРАВЛЕНИЕ ВНЕВЕДОМСТВЕННОЙ ОХРАНЫ

Утверждено
Заместителем начальника
ГУВО МВД России
полковником полиции
А.В. Грищенко
3 декабря 2013 г.

Построение и техническое обслуживание локально-вычислительной сети в пределах пункта централизованной охраны

РЕКОМЕНДАЦИИ

Р 78.36.038-2013

2013

Рекомендации разработаны сотрудниками ФКУ НИЦ "Охрана" ГУВО МВД России А.В. Голубевым, Н.В. Николаевым, О.И. Скалозубовым, А.В. Торопом, А. И. Кротовым, под руководством А. Г. Зайцева.

«Построение и техническое обслуживание локально-вычислительной сети в пределах пункта централизованной охраны» Рекомендации (Р 78.36.038-2013). – М.: НИЦ «Охрана», 2013. – 205 с.

Рекомендации предназначены для инженерно-технических работников вневедомственной охраны и электромонтеров охранно-пожарной сигнализации.

© Научно-исследовательский центр "Охрана" ГУВО МВД России, 2013

СОДЕРЖАНИЕ

1. **Термины и определения** 7
2. **Перечень сокращений** 14
3. **Введение** 19
4. **Концепция построения, назначение и типы сетей** 27
4.1 Коммуникационное оборудование вычислительных сетей 27
4.2 Среды передачи информации 30
4.2.1 Кабели на основе витых пар 30
4.2.2 Коаксиальные кабели 36
4.2.3 Оптоволоконные кабели 39
4.2.4 Бескабельные каналы связи 43
5. **Сетевое оборудование и программные средства** . 45
5.1 Уровни сетевой архитектуры 45
5.1.1 Аппаратура ЛВС 45
5.1.2 Сетевые программные средства 52
5.2 Стандартные локальные сети. Сети Ethernet и Fast Ethernet 61
6. **Типовой вариант аппаратно-программной платформы ЛВС** 67
7. **Проектирование ЛВС Ethernet на ПЦО** 75
7.1 Выбор размера сети и ее структуры 75
7.2 Выбор оборудования 79
7.3 Размещение 82
7.4 Электропитание и защитное заземление 83
7.5 Грозозащита линий локальной вычислительной сети 86
7.6 Пути и методы защиты информации в системах обработки данных 89

7.6.1 Пути и методы защиты информации
в ЛВС ПЦО 89
7.6.2 Основные угрозы ЛВС ПЦО
и меры по борьбе с ними 89
7.6.3 Пути и средства защиты информации 90
7.6.4 Вредоносные программы и борьба с ними 93
7.6.5 Использование межсетевого экрана 95
7.6.6 Применение технологии трансляции
сетевых адресов 97
7.7 Пример проектирования сети ПЦО
на 10 рабочих мест. 100
8. Техническое обслуживание и устранение неисправностей ЛВС ПЦО 104
8.1 Техническое обслуживание 104
8.2 Нормы трудозатрат по техническому
обслуживанию и ремонту ЛВС ПЦО 108
8.3 Устранение неисправностей ЛВС ПЦО 110
8.3.1 Аппаратура для поиска неисправностей
в ЛВС и тестирования ЛВС ПЦО 110
8.3.2 Программные средства для поиска
неисправностей в сети 116
8.3.3 Поиск и устранение сбоев
в волоконно-оптической линии связи 131
8.3.4 Программные средства для поиска
неисправностей в ЛВС ПЦО 137

Приложение А. Стандартные сегменты Ethernet и Fast Ethernet 149
А.1 Аппаратура 10BASE5 149
А.2 Аппаратура 10BASE2 153
А.3 Аппаратура 10BASE-T 156
А.4 Аппаратура 10BASE-FL 161

А.5 Аппаратура 100BASE-TX 165
А.6 Аппаратура 100BASE-T4 169
А.7 Аппаратура 100BASE-FX 172

Приложение Б. Прокладывание локальной сети .. 174
Б.1 Прокладывание локальной сети 10Base2 174
Б.2 Монтаж разъемов BNC 174
Б.3 Общая схема подключений 179
Б.4 Установка Т-коннекторов 180
Б.5 Установка терминаторов 181
Б.6 Переходы прямые 182
Б.7 Прокладывание локальной сети 10BaseT 183
Б.8 Общая схема подключений 183
Б.9 Монтаж разъемов RJ-45 на кабеле Path cord ... 187
Б.10 Обжимной инструмент 188
Б.11 Защитные колпачки 188
Б.12 Разъем RJ-45 189
Б.13 Последовательность монтажа разъема 191
Б.14 Монтаж сетевых розеток 197
Б.15 Монтаж разъема RJ-45 если
нет обжимного инструмента 199
Б.16 Прямое соединение двух компьютеров по
схеме «точка—точка» 202

Литература 204

1 Термины и определения.

Crosstalk — взаимное влияние кабелей и проводов друг на друга, перекрестные наводки.

Ethernet — наиболее распространенная в мире локальная сеть, предложенная фирмой Xerox (топология - шина, метод доступа CSMA/CD, скорость передачи - 10 Мбит/с). Удовлетворяет стандарту IEEE 802.3.

Fast Ethernet — высокоскоростная разновидность сети Ethernet, обеспечивающая скорость передачи 100 Мбит/с. Удовлетворяет доработанному стандарту IEEE 802.3u (стандарт утвержден в 1995 году).

Frame - кадр, пакет, единица передаваемой по сети информации.

Gigabit Ethernet - разрабатываемая сверхвысокоскоростная версия сети Ethernet, обеспечивающая скорость передачи 1 Гбит/с.

Plenum - тип кабеля в тефлоновой оболочке, более устойчивый к воздействиям окружающей среды, чем обычный кабель (non-plenum); при горении не выделяет токсичных газов.

RG-11 — распространенный тип толстого коаксиального кабеля сети Ethernet с волновым сопротивлением 50 Ом.

RG-58 A/U - распространенный тип тонкого коаксиального кабеля сети Ethernet с волновым сопротивлением, равным 50 Ом.

RJ-45 — тип разъема для присоединения кабеля на основе витых пар (8 контактов).

TCP/IP - набор протоколов нижних уровней для связи в гетерогенной среде, применяемый в сети Internet.

Витая пара — среда передачи информации , состоящая из двух перекрученных между собой электрических проводов, характеризующаяся наибольшей простотой монтажа и низкой стоимостью.

Глобальные сети (Wide Area Network, WAN) – это сети, предназначенные для объединения отдельных компьютеров и локальных сетей, расположенных на значительном удалении (сотни и тысячи километров) друг от друга. Поскольку организация специализированных высококачественных каналов связи большой протяженности является достаточно дорогой, то в глобальных сетях нередко используются уже существующие и изначально не предназначенные для построения компьютерных сетей линии (например, телефонные или телеграфные). В связи с этим скорость передачи данных в таких сетях существенно ниже, чем в локальных.

Затухание сигнала - ослабление передаваемого сигнала при его прохождении по сети, доля мощности сигнала, потерянная при прохождении по кабелю. Измеряется в децибелах (дБ).

Звезда (star) — вид топологии локальной сети, в котором к одному центральному абоненту (концентратору) подключаются несколько периферийных абонентов; при этом все управление сетью и (или) передачу всей информации в ней осуществляет центральный абонент.

Импеданс линии – сопротивление лини переменному току заданной частоты. Величина сопротивления линии (кабеля и соединителей) должна быть постоянна по всей линии в диапазоне рассматриваемых частот. Сигнал, отраженный от точек с аномальным импедансом, будет накладываться на основной сигнал

и искажать его. Для кабеля из витых пар импеданс обычно составляет 100 или 120 Ом. Для линий Категории 5 импеданс нормируется для диапазона частот 1-100 МГц и должен составлять 100 Ом ± 15%

Источник бесперебойного питания - устройство, обеспечивающее электроснабжение потребителей (компьютеров, концентраторов, принтеров и т.д.) при сбоях в электросети.

Кадр - базовый элемент передаваемых данных в сети. Часто то же самое, что и пакет.

Канал связи - система технических устройств и линий связи (см. Линия связи), обеспечивающая передачу информации между абонентами. Соотношение между понятиями "канал" и "линия" описывается следующим образом: канал связи может включать в себя несколько разнородных линий связи, а одна линия связи может использоваться несколькими каналами.

Клиент — абонент, не отдающий своего ресурса в сеть, но имеющий доступ к ресурсам сети. Иногда клиенты называются также рабочими станциями в противоположность серверу.

Коаксиальный кабель — среда передачи информации, электрический кабель, состоящий из центрального проводника и металлической оплетки, разделенные диэлектриком.

Коллизия - ситуация, при которой в сеть передаются несколько пакетов одновременно, что вызывает искажение информации. Называется также конфликтом или столкновением.

Кольцо (ring) - вид топологии локальной сети, в котором все абоненты последовательно передают информацию друг другу по цепочке, замкнутой в кольцо.

Концентратор (hub) - устройство, служащее для объединения нескольких сегментов единой сети и не преобразующее передаваемую информацию.

Коммутатор, коммутирующий концентратор, переключатель (switching hub, switch) — концентратор, передающий на другие сегменты только те пакеты, которые адресованы им.

Компьютерная сеть (Computer Network) – это множество компьютеров, соединенных линиями связи и работающих под управлением специального программного обеспечения.

Конфликт, коллизия (collision) - ситуация, при которой в сеть передаются несколько пакетов, что вызывает искажение информации.

Локальная сеть (Local Area Network, LAN или **ЛВС** - русское название)- компьютеры или другие устройства, соединенные линиями связи для передачи информации между ними на сравнительно небольшие расстояния. Классическим примером локальных сетей является сеть одного предприятия, расположенного в одном или нескольких стоящих рядом зданиях. Небольшой размер локальных сетей позволяет использовать для их построения достаточно дорогие и высококачественные технологии, что обеспечивает высокую скорость обмена информацией между компьютерами.

Линия связи - совокупность технических устройств, и физической среды, обеспечивающих передачу сигналов от передатчика к приемнику. В реальной жизни примерами линий связи могут служить участки кабеля и усилители, обеспечивающие передачу сигналов между коммутаторами телефонной сети. На основе линий связи строятся каналы связи (см. Канал связи).

Маршрутизатор (router) — устройство (компьютер), служащее для определения маршрута, по которому наиболее целесообразно пересылать пакет.

Метод доступа — способ определения, какой из абонентов сети может захватить сеть и начать передачу своего пакета.

Модем (модулятор-демодулятор) - устройство, преобразующее цифровые данные от компьютера в аналоговые сигналы перед их передачей по абонентской телефонной линии связи и, после приёма, производящее обратное преобразование.

Модемы, разновидности по типам линии передачи — специальные типы модемов для работы в линии электропроводки (power line modems), в системах кабельного телевидения (cable modems) и в беспроводных (радио-) линиях (radio modems).

Мост (bridge) - устройство (компьютер), служащее для объединения в единую сеть нескольких сетей разных типов, а также для снижения нагрузки в сети.

Невыделенный сервер - сервер, который может выполнять помимо функций по обслуживанию сети еще и другие задачи.

Оптоволоконный кабель - среда передачи информации, представляющая собой стеклянное или пластиковое волокно в оболочке, по которому распространяется световой сигнал.

Пакет - единица информации, передаваемой по сети. Могут быть короткими (порядка десятков байт и даже единиц байт), а также длинными (порядка нескольких килобайт). Включают в себя данные (необязательно), адреса и управляющие коды.

Переключатель - то же, что коммутатор.

Повторитель, репитер (repeater) — устройство для восстановления и усиления сигналов в сети, служащее для увеличения ее длины.

Протокол - набор правил, алгоритм обмена информацией между абонентами сети.

Рабочая станция — другое название абонента сети, клиента сети (в противоположность серверу) или специального компьютера, ориентированного на работу в сети.

Ретрансляция - прием и передача информации без ее изменения, но с восстановлением уровней сигналов и их формы.

Сеанс - логическое соединение между абонентами сети для обмена информацией; включает в себя передачу нескольких пакетов.

Сегмент — часть сети, ограниченная разделяющими устройствами (репитерами, концентраторами, мостами, маршрутизаторами, шлюзами), иногда используется как синоним понятия сети.

Сервер - абонент сети, отдающий в сеть свой ресурс и имеющий или не имеющий доступа к ресурсам сети. Также сервером называют специализированный компьютер, предназначенный для работы в сети (имеет быстродействующие диски большого объема, быстрый процессор, большую память).

Сервер печати - компьютер, обеспечивающий доступ клиентам сети к совместно используемому принтеру.

Сетевая операционная система - программное обеспечение, управляющее работой сети и позволяющее поддерживать связь и совместно использовать ресурсы.

Сетевой адаптер (он же контроллер, интерфейс, сетевая карта) — электронная плата, сопрягающая аппаратуру абонента сети и линии связи сети.

Сеть на основе сервера - сеть, в которой имеется четкое разделение абонентов на клиентов и серверов, и есть хотя бы один выделенный сервер.

Среда передачи информации — электрический кабель (коаксиальный, витая пара), волоконно-оптический кабель, радиоканал, инфракрасный канал, то есть то, что используется в данной сети для связи абонентов; характеризуется стоимостью, удобством подключения, пропускной способностью (то есть предельной скоростью передачи), предельной длиной линии связи (затуханием сигнала с расстоянием на данной частоте), помехоустойчивостью, секретностью передаваемых данных (возможностью подслушивания), требуемой сложностью адаптеров абонентов, а также рядом специфических параметров, менее важных для пользователей сети.

Топология - метод соединения, структура связей абонентов сети. Основные топологии — это звезда, шина и кольцо, реже встречаются топологии цепочка и дерево; топологии различаются требуемой длиной соединительного кабеля, удобством соединения, возможностями подключения дополнительных абонентов, отказоустойчивостью, возможностями управления обменом.

Трансивер (TRANSmitter+reCEI VER) — приемопередатчик сети, служащий для умощнения сигналов или для преобразования физической природы сигналов (например, электрических сигналов в световые и наоборот).

Узел - компьютер или другое устройство, подключенное к сети, то же, что абонент.

Шина (bus) - вид топологии локальной сети, в котором все абоненты параллельно подключены к линейному отрезку кабеля, согласованного на концах.

Шифрование — способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

Шлюз (gateway) — устройство (компьютер), служащее для объединения сетей с совершенно различными протоколами обмена.

Шум — временные или фазовые искажения сигнала в сети, которые могут нарушить обмен.

2 Перечень сокращений.

10BASE2 — стандарт сегмента сети Ethernet на тонком коаксиальном кабеле.

10BASE5 — стандарт сегмента сети Ethernet на толстом коаксиальном кабеле.

10BASE-T — стандарт сегмента сети Ethernet на витой паре.

10BASE-FL - стандарт сегмента сети Ethernet на оптоволоконном кабеле.

100BASE-T4 - стандарт сегмента сети Fast Ethernet на счетверенной витой паре.

100BASE-TX - стандарт сегмента сети Fast Ethernet на сдвоенной витой паре.

100BASE-FX — стандарт сегмента сети Fast Ethernet на оптоволоконном кабеле.

1000BASE-T - стандарт сегмента сети Gigabit Ethernet на неэкранированной витой паре.

AUI (Access Unit Interface) — тип разъема и кабеля для подключения сетевого адаптера Ethernet к трансиверу (MAU) толстого коаксиального кабеля.

BFOC/2.5 — стандарт оптоволоконного байонетного ST-разъема.

BNC (Bayonet Neill Concelnan) - разъем байонетного типа, применяющийся, в частности, в сети Ethernet для соединения адаптера с тонким коаксиальным кабелем.

CD (Collision Detection) - обнаружение коллизий, столкновений пакетов.

CDDI (Copper Distributed Data Interface) — реализация сети FDDI на электрическом (медном) кабеле, то же, что TPFDDI и SDDI.

CSMA/CD (Carrier-Sense Multiple Access/Collision detection) — децентрализованный метод доступа к сети с контролем несущей (с контролем наличия передачи) и обнаружением конфликтов, применяемый, в частности, в сети Ethernet. Распространенное сокращение — МДКН/ОК.

DB9 - стандартный 9-контактный разъем, используемый в сети Token-Ring.

ECMA (European Computer Manufacturers Association) — Европейская Ассоциация производителей компьютеров, международная организация.

EIA/TIA 568 (Commercial Building Telecommunications Cabling Standard) — стандарт на кабели для локальных сетей, определяющий их основные характеристики (затухания на различных частотах, отражения, количество витков на метр длины и т.д.).

FDDI (Fiber Distributed Data Interface) — распределенный интерфейс передачи данных по оптоволоконным каналам - 100 Мбит/с).

FLP (Fast Link Pulse) — сигналы, передаваемые в промежутках между пакетами в сети Fast Ethernet в режиме автодиалога (автоматического согласования скоростей передачи).

FOMAU (Fiber Optic MAU) — оптоволоконные трансиверы сети Ethernet.

FTP (File Transfer Protocol) - протокол передачи файлов, используемый в сети Internet.

IEEE (Institute of Electrical and Electronic Engineers) - Институт инженеров по электронике и радиотехнике (ИИЭР), организация, занимающаяся, в частности, стандартизацией локальных сетей.

LAN (Local Area Network) - локальная (вычислительная) сеть, ЛВС.

LED (Light Emitted Diode) - светодиод.

MAC-адрес — уникальный 48-битный адрес сетевого адаптера, устанавливаемый производителем адаптера. Применяется в сетях Ethernet, FDDI.

MAU (Medium Attachment Unit) - трансивер сети Ethernet на толстом коаксиальном кабеле, устанавливаемый непосредственно на кабеле.

Mbps (Mb/s, Mbits per second) - мегабит в секунду (Мбит/с), единица измерения скорости передачи и пропускной способности среды передачи.

MDI (Medium Dependent Interface) - интерфейс, зависящий от среды, средства непосредственной связи со средой передачи, например, разъем.

NIC (Network Interface Card) - сетевой адаптер (контроллер), сетевая карта.

NVP (Nominal Velocity of Propagation) - скорость распространения сигнала в кабеле, выражается в долях от скорости света (С), например, NVP=0,7C.

OSI (Open System Interchange) - модель взаимодействия открытых систем (ВОС), которая выделяет семь уровней в сетевых функциях: 1 - физический, 2 - канальный, 3 - сетевой, 4 - транспортный, 5 - сеансовый, 6 - представительский, 7 - уровень приложений.

PCI (Peripheral Component Interconnect) — быстродействующая 32-чли 64-разрядная магистраль, применяющаяся в персональных компьютерах типа IBM PC.

PVC - поливинилхлоридная оболочка кабеля.

RSA (Rivest, Shamir, Adleman) - метод шифрования данных, относящийся к группе методов несимметричного шифрования.

RX, RXD (Received Data) - принимаемые данные.

SDDI (Shielded Distributed Data Interface) - реализация сети FDDI на экранированной витой паре, то же, что CDDI и TPFDDI.

SFD (Start of Frame Delimiter) - признак начала кадра.

SMTP (Simple Mail Transfer Protocol) - протокол передачи сообщений электронной почты, используемый в сети Internet.

STP (Shielded Twisted-Pair cable) - кабель на основе экранированных витых пар, сами экранированные витые пары.

TIA (Telecommunication Industry Association) - Ассоциация телекоммуникационной промышленности.

TPFDDI (TDDI) - версия сети FDDI на электрическом кабеле (витой паре) со скоростью передачи данных 100 Мбит/с, то же, что CDDI и SDDI.

TX, TXD (Transmitted Data) — передаваемые данные.

UART (Universal Asynchronous Receiver/Transmitter) - универсальный асинхронный приемопередатчик (УАПП).

UTP (Unshielded Twisted-Pair cable) - кабель на основе неэкранированных витых пар, сами неэкранированные витые пары.

USART (Universal Synchronous/Asynchronous Receiver/Transmitter) - универсальный синхронно-асинхронный приемопередатчик (УСАПП).

WAN (Wide Area Network) — глобальная (вычислительная) сеть, ГВС.

WWW (World Wide Web) - гипертекстовая мультимедийная служба в сети Internet, содержащая информацию в гипертекстовом виде.

3. Введение

Главной целью объединения компьютеров в сеть является предоставление пользователям возможности доступа к различным информационным ресурсам (например, документам, программам, базам данных и т.д.).

Во вневедомственной охране применение локальных сетей на ПЦО связано с несколькими факторами:

1. Применение компьютеров в качестве замены пультов СПИ/РСПИ. Например, пульт СПИ «Фобос» был рассчитан на работу только с 3 ретрансляторами, невозможно было увеличить количество ретрансляторов до 8, или подключить к пульту ретрансляторы других СПИ. Для работы с 8 ретрансляторами была разработана программа КСА ПЦО. АРМ «Антей» позволяет работать с 16 ретрансляторами СПИ «Фобос», а также с ретрансляторами других СПИ – например, СПИ «Фобос-А», КЦН «Альтаир» и др.

2. Увеличение количества охраняемых объектов привело к увеличению необходимого количества рабочих мест дежурных ПЦО. При увеличении количества компьютеров на ПЦО удобно объединять их в локальную сеть, организовать доступ к одному принтерус разных рабочих мест для экономии стоимости, иметь один общий сервер базы данных

3. Появившееся разнообразие производимых СПИ и АРМ-ов также привело к увеличению необходимого количества рабочих мест дежурных ПЦО. АРМ-ы различных СПИ пока что ещё не допускают установки на один компьютер, что ведет к увеличе-

нию количества компьютеров, которые можно только через локальную сеть объединить вместе с компьютерами дежурного офицера, инженера ПЦО, службы ремонта, администратора АРМ.

4. Появившиеся в продаже новые сетевые устройства, например модемы Zyxel Prestige 791R, позволяют интегрировать локальные сети ПЦО в городские сети УВО.

5. Маршрутизаторы, например Zyxel P660, позволяют подключать к локальной сети ПЦО сети Internet и GPON для работы с устройствами оконечными по цифровым каналам TCP/IP, подключать сети GPRS для работы с устройствами оконечными по каналам сотовой связи GSM.

Под локальными понимаются такие сети, которые имеют небольшие, локальные размеры, соединяют близко расположенные компьютеры.

Главное отличие локальной сети от сети Internet или WAN - высокая скорость обмена и низкий уровень ошибок передачи. Поэтому локальные сети обязательно используют специально прокладываемые качественные линии связи.

Принципиальное значение имеет и такая характеристика сети, как возможность работы с большими нагрузками, то есть с большой интенсивностью обмена (или, как еще говорят, с большим трафиком). В соответствии с таблицей 5.1 требования разработчиков АРМ-ов к сетевым картам – от 10 Mb/c (для АРМ «Приток-А», «Струна-5», «Иртыш-3Р», «Протон») до 1000 Mb/c (для АРМ «Ахтуба»). Если механизм управления обменом, используемый в сети, не слишком эффективен, то компьютеры могут чрезмерно

долго ждать своей очереди на передачу, и даже если передача будет производиться затем на высочайшей скорости и полностью безошибочно, то для пользователя сети это все равно обернется неприемлемой задержкой доступа ко всем сетевым ресурсам.

Любой механизм управления обменом может гарантированно работать только тогда, когда заранее известно, сколько компьютеров (абонентов, узлов) может быть подключено к сети. По локальной сети может передаваться самая разная цифровая информация: данные, изображения, телефонные разговоры, электронные письма и т.д. Чаще всего локальные сети используются для разделения (совместного использования) таких ресурсов, как дисковое пространство, принтеры и выход в глобальную сеть. По ЛВС ПЦО передается информация, необходимая для функционирования программ АРМ: информация о состоянии охраняемых объектов, команды управления взятием под охрану и снятием с охраны, команды управления базой данных, и т. д.

При организации локальных сетей ПЦО прорабатываются вопросы:

- материальных затрат на покупку сетевого оборудования и сетевого программного обеспечения, на прокладку соединительных кабелей;

- материальных затрат на обучение персонала;

- необходимости наличия администратора сети - специалиста, который контролирует работу сети, управляет доступом к ресурсам, устраняет неисправности;

- размещения компьютеров, так как при этом могут понадобиться материальные затраты на перекладку соединительных кабелей;

- материальных затрат на защиту компьютеров от вирусов.

Сервером называется абонент (узел) сети, который предоставляет свои ресурсы другим абонентам, но сам не использует ресурсы других абонентов. Серверов в сети может быть несколько.

Выделенный сервер - это сервер, занимающийся только сетевыми задачами.

Специфический тип сервера - это сетевой принтер.

Клиентом называется абонент сети, который только использует сетевые ресурсы, но сам свои ресурсы в сеть не отдает. Компьютер-клиент также часто называют рабочей станцией. Каждый компьютер может быть одновременно как клиентом, так и сервером.

Под сервером и клиентом часто понимают также не сами компьютеры, а работающие на них программные приложения. В этом случае то приложение, которое только отдает ресурс в сеть, является сервером, а то приложение, которое только пользуется сетевыми ресурсами, является клиентом.

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи. Понятие топологии относится к локальным сетям, в которых структуру связей можно легко проследить.

Топология определяет требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Существует три основных топологии сети. "Общая шина" и "кольцо" - устаревшие топологии. В настоящее время широко используется топология "звезда".

Звезда — топология компьютерной сети, в которой все компьютеры сети присоединены к центральному узлу (обычно коммутатор), образуя физический сегмент сети. Подобный сегмент сети может функционировать как отдельно, так и в составе сложной сетевой топологии (как правило, «дерево»). Весь обмен информацией идет исключительно через центральный компьютер, на который таким способом возлагается очень большая нагрузка, поэтому ничем другим, кроме сети, он заниматься не может. Как правило, именно центральный компьютер является самым мощным, и именно на него возлагаются все функции по управлению обменом. Никакие конфликты в сети с топологией звезда в принципе невозможны, потому что управление полностью централизовано (рис. 3.1);

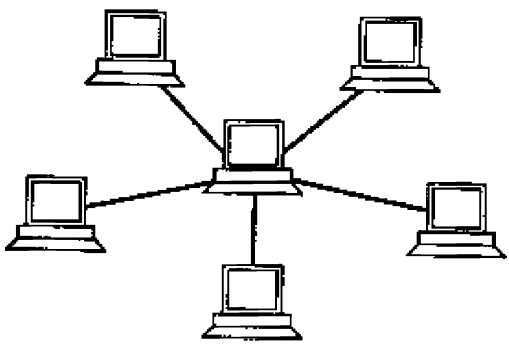


Рис. 3.1. Сетевая топология «звезда»

В «звезде» на каждой линии связи находятся только два абонента: центральный и один из периферийных. Чаще всего для их соединения используется две линии связи, каждая из которых передает информацию только в одном направлении. Таким образом, на каждой линии связи имеется только один приемник и один передатчик.

Серьезный недостаток топологии «звезда» состоит в жестком ограничении количества абонентов. Обычно центральный абонент может обслуживать не более 8-16 периферийных абонентов. Если в этих пределах подключение новых абонентов довольно просто, то при их превышении оно просто невозможно.

«Звезда», показанная на рис. 3.1, носит название активной, или истинной «звездой» (в центре сети содержится компьютер, который выступает в роли сервера.).

Существует также топология, называемая пассивной «звездой», которая только внешне похожа на звезду (рис. 3.2). В настоящее время она распространена гораздо больше, чем активная звезда. Достаточно сказать, что она используется в самой популярной на сегодняшний день сети Ethernet.

В центре сети с данной топологией содержится не компьютер, а концентратор или коммутатор (хаб (hub)). Сигналы, поступающие от любого компьютера, он пересылает в другие линии связи. Все пользователи в сети равноправны. Схема прокладки кабелей подобна истинной или активной звезде, фактически мы имеем дело с шинной топологией, так как информация от каждого компьютера одновременно передается ко всем остальным компьютерам, а центрального абонента не существует. Естественно, пассивная звезда

получается дороже обычной шины, так как в этом случае обязательно требуется еще и концентратор. Однако она предоставляет целый ряд дополнительных возможностей, связанных с преимуществами звезды. Именно поэтому в последнее время пассивная звезда все больше вытесняет истинную шину, которая считается малоперспективной топологией.

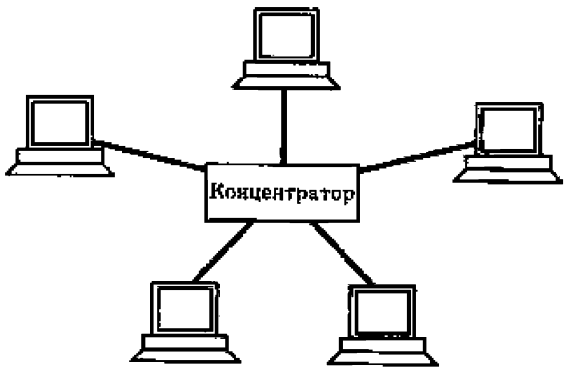


Рис. 3.2. Топология «пассивная звезда»

Можно выделить также промежуточный тип топологии между активной и пассивной звездой. В этом случае концентратор не только ретранслирует поступающие на него сигналы, но и производит управление обменом, однако сам в обмене не участвует.

Большое достоинство звезды (как активной, так и пассивной) состоит в том, что все точки подключения собраны в одном месте. Это позволяет легко контро-

лировать работу сети, локализовать неисправности сети путем простого отключения от центра тех или иных абонентов (что невозможно, например, в случае шины), а также ограничивать доступ посторонних лиц к жизненно важным для сети точкам подключения. К каждому периферийному абоненту в случае «звезды» может подходить как один кабель (по которому идет передача в обоих направлениях), так и два кабеля (каждый из них передает в одном направлении), причем вторая ситуация встречается чаще.

Общим недостатком для всех топологий типа «звезда» является значительно больший, чем при других топологиях, расход кабеля и выход из строя центрального концентратора обернётся неработоспособностью сети (или сегмента сети) в целом.

Топология не является основным фактором при выборе типа сети. Гораздо важнее, например, уровень стандартизации сети, скорость обмена, количество абонентов, стоимость оборудования, выбранное программное обеспечение.

4 Концепция построения, назначение и типы сетей.

4.1 Коммуникационное оборудование вычислительных сетей

Сетевой адаптер (сетевая карта) - это устройство двунаправленного обмена данными между ПК и средой передачи данных вычислительной сети. Кроме организации обмена данными между ПК и вычислительной сетью, сетевой адаптер выполняет буферизацию (временное хранение данных) и функцию сопряжения компьютера с сетевым кабелем.

В зависимости от применяемой технологии вычислительных сетей Ethernet, Fast Ethernet или Gigabit Ethernet, сетевые карты обеспечивают скорость передачи данных: 10, 100 или 1000 Мбит/с.

В качестве кабелей соединяющих отдельные ПК и коммуникационное оборудование в вычислительных сетях применяются: витая пара, коаксиальный кабель, оптический кабель, свойства которых изложены в пункте 4.2 настоящих Рекомендаций.

В качестве промежуточного коммуникационного оборудования применяются: трансиверы, повторители (repeaters), концентраторы (hubs), коммутаторы (switches), мосты (bridges), маршрутизаторы (routers) и шлюзы (gateways).

Промежуточное коммуникационное оборудования вычислительных сетей используется для усиления и преобразования сигналов, для объединения ПК в физические сегменты, для разделения вычислительных сетей на подсети (логические сегменты) с целью увеличения производительности сети, а также для объединения подсетей (сегментов) и сетей в единую вычислительную сеть.

Повторители обеспечивают усиление и восстановление сигналов в вычислительных сетях с целью увеличения их длины. Концентраторы и коммутаторы служат для объединения нескольких компьютеров в требуемую конфигурацию локальной вычислительной сети.

Концентраторы являются средством физической структуризации вычислительной сети, так как разбивают сеть на сегменты. Коммутаторы предназначены для логической структуризации вычислительной сети, так как разделяют общую среду передачи данных на логические сегменты и тем самым устраняют столкновения.

Для соединения подсетей (логических сегментов) и различных вычислительных сетей между собой в качестве межсетевого интерфейса применяются коммутаторы, мосты, маршрутизаторы и шлюзы.

Трансиверы или приемопередатчики – это аппаратные устройства, служащие для двунаправленной передачи между адаптером и сетевым кабелем или двумя сегментами кабеля. Основной функцией трансивера является усиление сигналов. Трансиверы применяются и в качестве конверторов для преобразование электрических сигналов в другие виды сигналов (оптические или радиосигналы) с целью использования других сред передачи информации.

Концентраторы – это аппаратные устройства множественного доступа, которые объединяют в одной точке отдельные физические отрезки кабеля, образуют общую среду передачи данных или физические сегменты сети.

Коммутаторы - это программно – аппаратные устройства, которые делят общую среду передачи

данных на логические сегменты. Логический сегмент образуется путем объединения нескольких физических сегментов с помощью концентраторов. Каждый логический сегмент подключается к отдельному порту коммутатора.

Мосты – это программно – аппаратные устройства, которые обеспечивают соединение нескольких локальных сетей между собой или несколько частей одной и той же сети, работающих с разными протоколами. Мосты предназначены для логической структуризации сети или для соединения в основном идентичных сетей, имеющих некоторые физические различия. Мост изолирует трафик одной части сети от трафика другой части, повышая общую производительность передачи данных.

Маршрутизаторы - это коммуникационное оборудование, которое обеспечивает выбор маршрута передачи данных между несколькими сетями, имеющими различную архитектуру или протоколы. Маршрутизаторы применяют только для связи однородных сетей и в разветвленных сетях, имеющих несколько параллельных маршрутов. Маршрутизаторами и программными модулями сетевой операционной системы реализуются функции сетевого уровня.

Шлюзы – это коммуникационное оборудование (например, компьютер), служащее для объединения разнородных сетей с различными протоколами обмена. Шлюзы полностью преобразовывают весь поток данных, включая коды, форматы, методы управления и т.д.

Коммуникационное оборудование: мосты, маршрутизаторы и шлюзы в локальной вычислительной сети - это, как правило, выделенные компьютеры со специальным программным обеспечением.

4.2 Среды передачи информации

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети.

Информация в локальных сетях чаще всего передается в последовательном коде, то есть бит за битом.

Промышленностью выпускается огромное количество типов кабелей. Все выпускаемые кабели можно разделить на три большие группы:

- кабели на основе витых пар проводов (twisted pair), которые делятся на экранированные (shielded twisted pair, STP) и неэкранированные (unshielded twisted pair, UTP);
- коаксиальные кабели (coaxial cable);
- оптоволоконные кабели (fiber optic).

При выборе типа кабеля надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

4.2.1 Кабели на основе витых пар

Витые пары проводов используются в самых дешевых и на сегодняшний день, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки.

Обычно в кабель входит четыре витые пары.

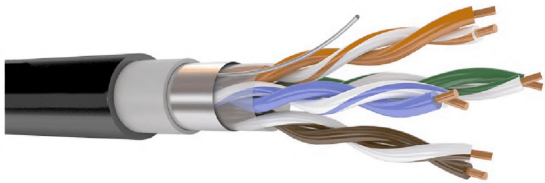


Рис. 4.2.1.1. Кабель с витыми парами

Виды кабеля, применяемого в сетях:

В зависимости от наличия защиты — электрически заземлённой медной оплётки или алюминиевой фольги вокруг скрученных пар, определяют разновидности данной технологии:

- неэкранированная витая пара (англ. UTP — Unshielded twisted pair) — без защитного экрана;
- фольгированная витая пара (англ. FTP — Foiled twisted pair), также известна как F/UTP) — присутствует один общий внешний экран в виде фольги;
- экранированная витая пара (англ. STP — Shielded twisted pair) — присутствует защита в виде экрана для каждой пары и общий внешний экран в виде сетки;
- фольгированная экранированная витая пара (англ. S/FTP — Screened Foiled twisted pair) — внешний экран из медной оплетки и каждая пара в фольгированной оплетке;

• незащищенная экранированная витая пара (англ. U/STP — Unshielded Screened twisted pair) — без внешнего экрана и каждая пара в фольгированной оплетке;

• защищенная экранированная витая пара (SF/UTP — или с англ. Screened Foiled Unshielded twisted pair).Отличие от других типов витых пар заключается в наличии двойного внешнего экрана, сделанного из медной оплётки, а также фольги

Экранирование обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних и т. д. Экран по всей длине соединён с неизолированным дренажным проводом, который объединяет экран в случае разделения на секции при излишнем изгибе или растяжении кабеля.

В зависимости от структуры проводников — кабель применяется одно- и многопроволочный. В первом случае каждый провод (жила) состоит из одной медной проволоки, а во втором — из нескольких скрученных проволок.

Однопроволочный кабель не предполагает прямых контактов с подключаемой периферией. То есть, как правило, его применяют для прокладки в коробах, стенах и т. д. с последующим терминированием розетками. Связано это с тем, что медные жилы довольно толсты и при частых изгибах быстро ломаются. Однако для «врезания» в разъёмы панелей розеток такие жилы подходят как нельзя лучше.

В свою очередь многопроволочный кабель плохо переносит «врезание» в разъёмы панелей розеток (тонкие жилы разрезаются), но замечательно ведет себя при изгибах и скручивании. Кроме того, многопрово-

лочный провод обладает большим затуханием сигнала. Поэтому многопроволочный кабель используют в основном для изготовления патчкордов (англ. patchcord), соединяющих периферию с розетками.

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также слабой защищенностью от подслушивания с целью, например, промышленного шпионажа. Перехват передаваемой информации возможен как с помощью контактного метода (посредством двух иголочек, воткнутых в кабель), так и с помощью бесконтактного метода, сводящегося к радиоперехвату излучаемых кабелем электромагнитных полей. Для устранения этих недостатков применяется экранирование.

В случае экранированной витой пары STP, каждая из витых пар помещается в металлическую оплетку-экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга (crosstalk - перекрестные наводки).

Основные достоинства неэкранированных витых пар - простота монтажа разъемов на концах кабеля, а также простота ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей. В настоящее время витая пара используется для передачи информации на скоростях до 100 Мбит/с, и ведутся работы по повышению скорости передачи до 1000 Мбит/с.

Согласно стандарту EIA/TIA 568, существуют пять категорий кабелей на основе неэкранированной витой пары (UTP), но практически используются:

- кабель категории 3 — это кабель для передачи данных в полосе часто до 16 МГц, состоящий из витых

пар с девятью витками проводов на метр длины. Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Это самый простой тип кабелей, рекомендованный стандартом для локальных сетей.

- кабель категории 5 - самый совершенный кабель в настоящее время, рассчитанный на передачу данных в полосе частот до 100 МГц. Состоит из витых пар, имеющих не менее 27 витков на метр длины (8 витков на фут). Кабель тестируется на все параметры и имеет волновое сопротивление 100 Ом. Рекомендуется применять его в современных высокоскоростных сетях типа Fast Ethernet и TPFDDI.

Параметры кабеля:

Полное волновое сопротивление наиболее совершенных кабелей категорий 3, 4 и 5 должно составлять 100 Ом ± 15% в частотном диапазоне от частоты 1 МГц до максимальной частоты кабеля. Волновое сопротивление экранированной витой пары STP должно быть по стандарту равно 150 Ом ± 15%. Для согласования импедансов кабеля и оборудования в случае их несовпадения применяют согласующие трансформаторы.

Максимальное затухание сигнала, передаваемого по кабелю, на разных частотах. Величины затухания на верхних частотах для всех кабелей очень значительны, что предъявляет высокие требования к приемникам сигнала.

Затухание перекрестной наводки на ближнем конце. Оно характеризует влияние разных проводов в кабеле друг на друга. Более качественные кабели обеспечивают меньшую величину перекрестной наводки.

Максимально допустимая величина рабочей емкости каждой из витых пар кабелей категории 4 и 5. Она должна составлять не более 17 нФ на 305 метров (1000 футов) при частоте сигнала 1 кГц и температуре окружающей среды 20°С.

Скорость распространения сигнала в кабеле, то есть задержка распространения сигнала в кабеле в расчете на единицу длины. Типичная величина задержки большинства современных кабелей составляет около 5 нс/м.

Для присоединения витых пар используются разъемы RJ-45 .Разъемы RJ-45 имеют восемь контактов. Присоединяются разъемы к кабелю с помощью специальных обжимных инструментов. При этом золоченые игольчатые контакты разъема прокалывают изоляцию каждого провода, входят между его жилами и обеспечивают надежное и качественное соединение. При установке разъемов допускается расплетение витой пары кабеля на длину не более одного сантиметра.

Каждый из проводов, входящих в кабель витых пар, как правило, имеет свой цвет изоляции, что существенно облегчает монтаж разъемов, особенно в том случае, когда концы кабеля находятся в разных комнатах, и контроль с помощью приборов затруднен.

Чаще всего витые пары используются для передачи данных в одном направлении, то есть в топологиях типа «звезда» или «кольцо». Топология «шина» обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Кабели выпускаются с двумя типами внешних оболочек:

- кабель в поливинилхлоридной (ПВХ) оболочке. Он дешевле и предназначен для работы кабеля в сравнительно комфортных условиях эксплуатации;

- кабель в тефлоновой оболочке. Он дороже и предназначен для более жестких условий эксплуатации.

4.2.2 Коаксиальные кабели

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку (рис.4.2.2.1).

Рис. 4.2.2.1. Коаксиальный кабель

Коаксиальный кабель до недавнего времени был распространен наиболее широко, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), а также более высокими, чем в случае витой пары, допустимыми скоростями передачи

данных (до 500 Мбит/с) и большими допустимыми расстояниями передачи (до километра и выше). К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют реже, чем витую пару.

Основное применение коаксиальный кабель находит в сетях с топологией типа «шина». При этом на концах кабеля обязательно должны устанавливаться терминаторы для предотвращения внутренних отражений сигнала, причем один (и только один!) из терминаторов должен быть заземлен. Без заземления металлическая оплетка не защищает сеть от внешних электромагнитных помех и не снижает излучение передаваемой по сети информации во внешнюю среду. Но при заземлении оплетки в двух или более точках из строя может выйти не только сетевое оборудование, но и компьютеры, подключенные к сети (подробнее об этом - в специальном разделе этой главы). Терминаторы должны быть обязательно согласованы с кабелем, то есть их сопротивление должно быть равно волновому сопротивлению кабеля.

Реже коаксиальные кабели применяются в сетях с топологией «звезда» и «пассивная звезда».

Параметры коаксиального кабеля:

Волновое сопротивление кабеля указывается в сопроводительной документации. Чаще всего в локальных сетях применяются 50-омные и 93-омные кабели.

Тип коаксиального кабеля. Существует два основных типа коаксиального кабеля:

- тонкий (thin) кабель, имеющий диаметр около 0,5 см, более гибкий;

- толстый (thick) кабель, имеющий диаметр около 1 см, значительно более жесткий. Он представляет собой классический вариант коаксиального кабеля, который уже почти полностью вытеснен более современным тонким кабелем.

Тонкий кабель используется для передачи на меньшие расстояния, чем толстый, так как в нем сигнал затухает сильнее. Зато с тонким кабелем гораздо удобнее работать: его можно оперативно проложить к каждому компьютеру, а толстый требует жесткой фиксации на стене помещения. Подключение к тонкому кабелю (с помощью разъемов BNC байонетного типа) проще и не требует дополнительного оборудования, а для подключения к толстому кабелю надо использовать специальные довольно дорогие устройства, прокалывающие его оболочки и устанавливающие контакт как с центральной жилой, так и с экраном. Толстый кабель примерно вдвое дороже, чем тонкий. Поэтому тонкий кабель применяется гораздо чаще.

Тип его внешней оболочки. Применяются как non-plenum (PVC), так и plenum кабели.

Величина задержки распространения сигнала в коаксиальном кабеле для тонкого кабеля около 5 нс/м, а для толстого — около 4,5 нс/м.

Наличие двойного экрана (один экран расположен внутри другого и отделен от него дополнительным слоем изоляции). Такие кабели имеют лучшую помехозащищенность и защиту от прослушивания.

4.2.3 Оптоволоконные кабели

Оптоволоконный кабель — это кабель, информация по которому передается световым сигналом. Главный его элемент - это прозрачное стекловолокно, по которому свет проходит на расстояния до десятков километров с незначительным ослаблением.

Структура оптоволоконного кабеля похожа на структуру коаксиального электрического кабеля (рис. 4.2.3.1), только вместо центрального медного провода здесь используется тонкое (диаметром порядка 1-10 мкм) стекловолокно, а вместо внутренней изоляции - стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна из-за полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля применяется для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

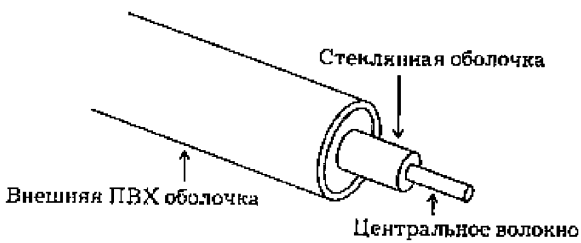


Рис. 4.2.3.1. Структура оптоволоконного кабеля

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам этот сигнал принципиально не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как это требует нарушения целостности кабеля. Теоретически возможная полоса пропускания такого кабеля достигает величины 1012 Гц, что несравнимо выше, чем у любых электрических кабелей. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля. Однако в данном случае необходимо применение специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

Типичная величина затухания сигнала в оптоволоконных кабелях на частотах, используемых в локальных сетях, составляет около 5 дБ/км, что примерно соответствует показателям электрических кабелей на низких частотах. Но в случае оптоволоконного кабеля при росте частоты передаваемого сигнала затухание увеличивается очень незначительно, и на больших частотах (особенно свыше 200 МГц) его затухание меньше, чем у электрического кабеля.

Кабель обеспечивает идеальную гальваническую развязку компьютеров сети.

Недостатки оптоволоконного кабеля:

Высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно.

Любое разветвление оптоволоконного кабеля сильно ослабляет световой сигнал.

Оптоволоконный кабель механически менее прочен, чем электрический, и менее гибкий (типичная величина допустимого радиуса изгиба составляет около 10—20 см).

Чувствителен:

- к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть (увеличивается затухание сигнала),
- к резким перепадам температуры, в результате которых стекловолокно может треснуть.
- к механическим воздействиям (удары, ультразвук) — так называемый микрофонный эффект. Для его уменьшения используют мягкие звукопоглощающие оболочки.

Применяют оптоволоконный кабель только в сетях с топологией «звезда» и «кольцо». Кабель обеспечивает идеальную гальваническую развязку компьютеров сети.

Существуют два различных типа оптоволоконных кабелей:

- многомодовый, или мультимодовый, кабель, более дешевый, но менее качественный;

- одномодовый кабель, более дорогой, но имеющий лучшие характеристики.

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего все они достигают приемника одновременно, и форма сигнала не искаженна. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Такие приемопередатчики пока еще сравнительно дороги и не слишком долговечны.

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки - 125 мкм. Для передачи используется обычный светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков. Длина волны света в многомодовом кабеле равна 0,85 мкм. Допустимая длина кабеля достигает 2-5 км. В настоящее время многомодовый кабель - основной тип оптоволоконного кабеля, так как он дешевле и доступнее.

Задержка распространения сигнала в оптоволоконном кабеле не сильно отличается от задержки в электрических кабелях и составляет около 4-5 нс/м.

4.2.4 Бескабельные каналы связи

В компьютерных сетях используются бескабельные каналы, которым не требуется прокладка проводов и устранять повреждения кабеля (рис. 4.2.4.1). Компьютеры сети в этом случае легко перемещать в пределах комнаты или здания.

Радиоканал использует передачу информации по радиоволнам. В локальных сетях радиоканал не получил широкого распространения из-за довольно высокой стоимости передающих и приемных устройств, низкой помехозащищенности, полного отсутствия секретности передаваемой информации и низкой надежности связи. Используют радиоканал для связи двух и более локальных сетей, находящихся далеко друг от друга, в единую сеть.

Стандартные типы радиопередачи информации:

- Передача в узком спектре (или одночастотная передача) рассчитана на охват площади до 46500 м^2. Радиосигнал в данном случае не проникает через металлические и железобетонные преграды. Связь в данном случае относительно медленная (около 4,8 Мбит/с).

- Передача в рассеянном спектре - использование некоторой полосы частот, разделенной на каналы. Все абоненты сети через определенный временной интервал синхронно переходят на следующий канал. Для повышения секретности используется специальное кодирование информации. Скорость передачи при этом невысока - не более 2 Мбит/с, расстояние между абонентами - не более 3,2 км на открытом пространстве и не более 120 м внутри здания.

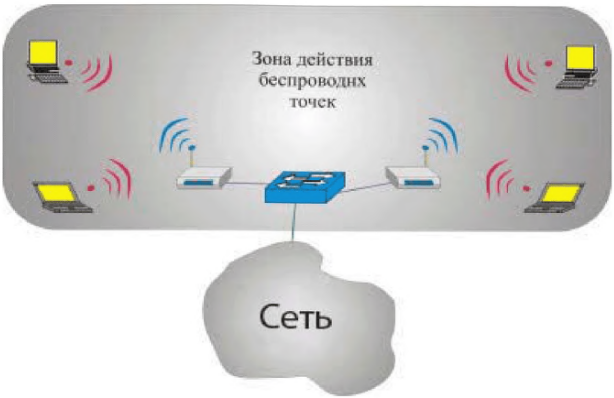


Рис. 4.2.4.1. Бескабельные каналы

Сотовые сети, строящиеся по тем же принципам, что и сотовые телефонные сети (они используют равномерно распределенные по площади ретрансляторы).

Инфракрасный канал, который использует для связи инфракрасное излучение. Он нечувствителен к электромагнитным помехам. Инфракрасный канал чувствителен к другим источники теплового (инфракрасного) излучения и пыли.

Скорость передачи информации по инфракрасному каналу не превышает 5-10 Мбит/с. Секретность передаваемой информации низкая. Требуются сравнительно дорогие приемники и передатчики. Применяются инфракрасные каналы довольно редко.

5. Сетевое оборудование и программные средства.

5.1 Уровни сетевой архитектуры.

5.1.1 Аппаратура ЛВС.

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами. К аппаратуре локальных сетей относятся:

- кабели для передачи информации;
- разъемы для присоединения кабелей;
- согласующие терминаторы;
- сетевые адаптеры;
- репитеры;
- трансиверы;
- концентраторы;
- мосты;
- маршрутизаторы;
- шлюзы.

Сетевые адаптеры - это основная часть аппаратуры локальной сети, без которой сеть невозможна. Адаптеры снабжены собственным процессором и памятью. Сетевые карты можно разделить на два типа:

- адаптеры для клиентских компьютеров;
- адаптеры для серверов.

Назначение сетевого адаптера - сопряжение компьютера с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Они

выполняют функции нижних уровней модели OSI. Сетевые адаптеры выполняются в виде платы, вставляемой в слоты расширения системной шины компьютера (PCI или PCI-E). Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети (рис. 5.1.1.1.).

Все функции сетевого адаптера делятся на магистральные и сетевые. К магистральным относятся те функции, которые осуществляют обмен адаптера с системной шиной компьютера. Сетевые функции обеспечивают общение адаптера с сетью.

Рис. 5.1.1.1. Платы сетевых адаптеров PCI и PCI-E.

Для нормальной работы платы адаптера в составе компьютера необходимо правильно установить ее основные параметры:

- базовый адрес порта ввода/вывода;
- базовые адреса буферной и загрузочной памяти.

Эти параметры могут устанавливаться на плате адаптера с помощью перемычек (джамперов) или переключателей, но могут задаваться и программно с помощью специальной программы инициализации адаптера, поставляемой вместе с платой. При выборе всех параметров (адресов и номеров прерываний) необходимо, чтобы они отличались от тех, которые заняты другими устройствами компьютера (как системными, так и дополнительно подключенными). Современные сетевые адаптеры часто поддерживают режим Plug-and-Play, то есть не нуждаются в настройке параметров со стороны пользователя, настройка в них осуществляется автоматически при включении питания компьютера.

Основные функции сетевых адаптеров:

- гальваническая развязка компьютера и кабеля локальной сети;
- преобразование логических сигналов в сетевые и обратно;
- кодирование и декодирование сетевых сигналов;
- опознание принимаемых пакетов;
- преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
- буферирование передаваемой и принимаемой информации в буферной памяти адаптера;

- организация доступа к сети в соответствии с принятым методом управления обменом;

- подсчет контрольной суммы пакетов при передаче и приеме.

Трансиверы, или приемопередатчики, служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

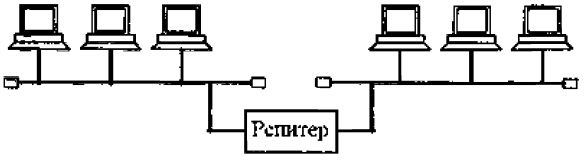


Рис. 5.1.1.2. Соединение репитером двух сегментов сети

Репитеры, или повторители (repeater), выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их вид, а только восстанавливают ослабленные сигналы, приводя их форму к исходному виду. Цель такой ретрансляции сигналов состоит в увеличении длины сети (рис. 5.1.1.2.). Однако часто репитеры выполняют и некоторые другие функции, например гальваническую развязку соединяемых сегментов. Репитеры и трансиверы не производят никакой информационной обработки проходящих через них сигналов.

Концентраторы (hub) служат для объединения в единую сеть нескольких сегментов сети. Концентраторы можно разделить на пассивные и активные.

Пассивные, или репитерные, концентраторы представляют собой собранные в едином конструктиве несколько репитеров. Они выполняют те же функции, что и репитеры (рис. 4.1.2.3.). Преимущество подобных концентраторов по сравнению с отдельными репитерами только в том, что все точки подключения собраны в одном месте, что упрощает реконфигурацию сети, контроль за ней и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

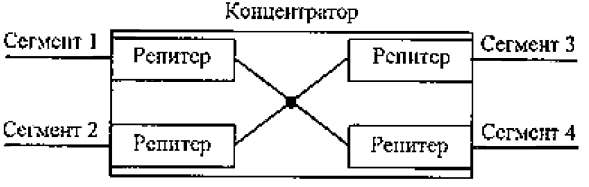


Рис. 5.1.1.3. Структура репитерного концентратора

Активные концентраторы преобразовывают информацию и протоколы обмена (коммутирующие или переключающие концентраторы (switching hub), коммутаторы.) Они передают из одного сегмента сети в другой сегмент не все пакеты, а только те, которые действительно адресованы компьютерам из другого сегмента. Сам пакет коммутатором не принимается. Это приводит к снижению интенсивности обмена в сети вследствие разделения нагрузки, так как каждый сегмент работает только со своими пакетами.

Мосты (bridge), маршрутизаторы (router) и шлюзы (gateway) служат для объединения в единую сеть нескольких разнородных сетей с разными протоколами обмена нижнего уровня, в частности, с разными форматами пакетов, разными методами кодирования, разной скоростью передачи и т.д. В результате их применения сложная и неоднородная сеть, содержащая в себе самые разные сегменты, с точки зрения пользователя выглядит обычной сетью - то есть обеспечивается «прозрачность» сети для протоколов высокого уровня. Реализуются они на базе компьютеров, подключенных к сети с помощью сетевых адаптеров. Это специализированные абоненты (узлы) сети.

Мосты - наиболее простые устройства, служащие для объединения сетей с разными стандартами обмена, или нескольких сегментов одной и той же сети (рис. 5.1.1.4.). В последнем случае мост служит только для разделения нагрузок сегментов, повышая тем самым производительность сети в целом. Мосты принимают поступающие пакеты целиком и в случае необходимости производят их простейшую обработку.

Маршрутизаторы выполняют более сложную функцию, чем мосты. Их главная задача - выбор для каждого пакета оптимального маршрута для избегания чрезмерной нагрузки отдельных участков сети и обхода поврежденных участков. Они применяются в сложных разветвленных сетях, имеющих несколько маршрутов между отдельными абонентами. Маршрутизаторы не преобразуют протоколы нижних уровней, поэтому они соединяют только сегменты одноименных сетей. Существуют также **гибридные маршрутизаторы** (brouter), представляющие собой гибрид моста и мар-

шрутизатора. Они выделяют пакеты, которым нужна маршрутизация, и обрабатывают их как маршрутизаторы, а для остальных пакетов служат обычными мостами.

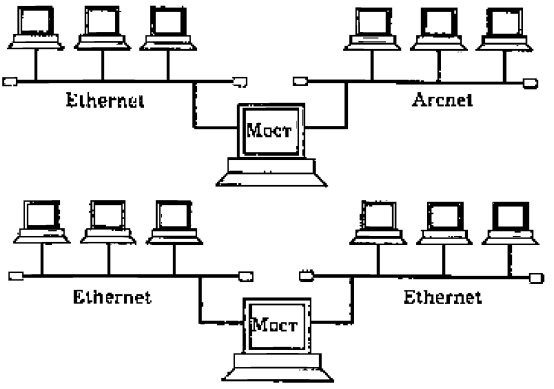


Рис. 5.1.1.4. Включение моста

Шлюзы - это устройства для соединения совершенно различных сетей с сильно отличающимися протоколами, например для соединения локальных сетей с большими компьютерами или с глобальными сетями. Это самые дорогие и редко применяемые сетевые устройства.

Если обратиться к модели OSI, то можно считать, что репитеры и репитерные концентраторы связывают сети или сегменты на первом уровне, мосты - на втором уровне, маршрутизаторы - на третьем уровне, а шлюзы - на более высоких уровнях (на 4, 5, 6 и

7). Соответственно, репитеры выполняют функции (не все, а только некоторые) первого уровня, мосты реализуют функции второго уровня (на первом уровне и частично на втором у них работают сетевые адаптеры), маршрутизаторы - третьего уровня, а шлюзы должны выполнять функции всех уровней.

5.1.2 Сетевые программные средства

Функции верхних уровней эталонной модели OSI выполняют сетевые программные средства. Для установки сети достаточно иметь набор сетевого оборудования, его драйверы и сетевое программное обеспечение. От выбора программного обеспечения зависит: допустимый размер сети, удобство использования и контроля сети, режимы доступа к ресурсам, производительность сети в разных режимах и т.д.

Типы сетей.

- Одноранговые сети, то есть сети, состоящие из равноправных компьютеров.

- Сети на основе серверов, в которых существуют только выделенные (dedicated) серверы, занимающиеся исключительно сетевыми функциями. Выделенный сервер может быть единственным или их может быть несколько.

Каждому типу сети соответствует свои программные средства.

Одноранговые сети (рис. 5.1.2.1) и соответствующие программные средства используются при необходимости объединения небольшого количества компьютеров (до 10-20). Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя вполне возможно назначение какого-то

компьютера только сервером, а какого-то - только клиентом. В одноранговой сети любой сервер может быть невыделенным (non-dedicated), то есть может не только обслуживать сеть, но и работать как автономный компьютер. В одноранговой сети могут быть и выделенные серверы, только обслуживающие сеть.

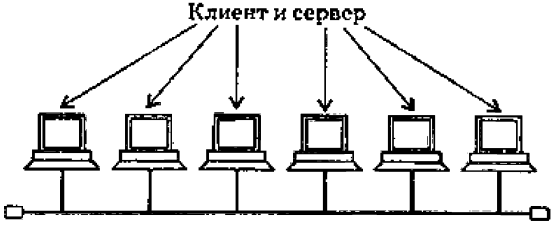


Рис. 5.1.2.1 Одноранговая сеть

Именно в данном случае наиболее правильно говорить о распределенных дисковых ресурсах, о виртуальном компьютере, а также о суммировании объемов дисков всех компьютеров сети. Если все компьютеры являются серверами, то любой файл, созданный на одном компьютере, сразу же становится доступным всем остальным компьютерам, его не надо передавать на централизованный сервер.

Достоинством одноранговых сетей является их высокая гибкость: в этом случае сеть может использоваться очень активно, а может и не использоваться совсем в зависимости от конкретной задачи. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки сети. В одноранговых сетях допускается определение различных

прав пользователей по доступу к сетевым ресурсам, но система разграничения прав не слишком развита. Также недостатком одноранговых сетей является слабая система контроля за сетью, протоколирования работы сети. Выход из строя любого компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, так как трудно обеспечить высокую скорость процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но решают и другие задачи.

Распространенные одноранговые сетевые программные средства:

- Windows XP (Microsoft);
- Windows Vista (Microsoft);
- Windows 7 (Microsoft).

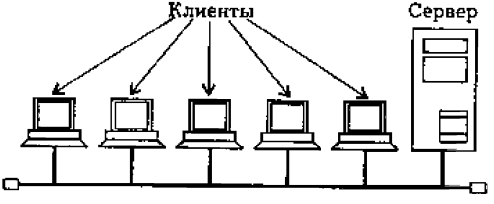


Рис. 5.1.2.2. Сеть на основе сервера

Сети на основе сервера применяются в тех случаях, когда в сеть должно быть объединено много пользователей. В этом случае быстродействия одноранговой сети может не хватить. Поэтому в сеть включается специализированный компьютер - сервер, который обслуживает только сеть и не решает никаких других задач (рис. 5.1.5.3). Такой сервер называется выделенным. Серверы специально оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления защитой файлов и каталогов. При больших размерах сети мощности одного сервера может оказаться недостаточно, и тогда в сеть включают несколько серверов. Серверы могут выполнять и некоторые другие задачи: сетевая печать, выход в глобальную сеть, связь с другой локальной сетью, обслуживание электронной почты и т.д. Количество пользователей сети на основе сервера может достигать нескольких тысяч. Одноранговой сетью такого размера просто невозможно было бы управлять.

В сети на основе сервера существует четкое разделение компьютеров на клиентов (или рабочие станции) и серверы. Клиенты не могут работать как серверы, а серверы - как клиенты и как автономные компьютеры. Все сетевые дисковые ресурсы располагаются только на сервере, а клиенты обращаются только к серверу. Пересылка информации от одного клиента к другому возможна только через сервер, например через файл, доступный всем клиентам. Реализуется некоторая «логическая звезда» с сервером в центре, хотя физическая топология сети может быть любой.

Достоинством сети на основе сервера является надежность, если сервер надежен. В противном случае любой отказ сервера приводит к полному параличу сети в отличие от ситуации с одноранговой сетью, где отказ одного из компьютеров не приводит к полному отказу все сети. Бесспорное достоинство сети на основе сервера - высокая скорость обмена, так как сервер всегда оснащается быстрым процессором (или даже несколькими процессорами), оперативной памятью большого объема и быстрыми жесткими дисками. Так как все ресурсы сети собраны в одном месте, возможно применение гораздо более мощных средств управления доступом, защиты данных, протоколирования обмена, чем в одноранговых сетях.

К недостаткам сети на основе сервера относятся ее громоздкость в случае небольшого количества компьютеров, зависимость всех компьютеров-клиентов от сервера, более высокая стоимость сети вследствие использования дорогого сервера. Но, говоря о стоимости, надо также учитывать, что при одном и том же объеме сетевых дисков большой диск сервера получается дешевле, чем много дисков меньшего объема, входящих в состав всех компьютеров одноранговой сети.

Распространенные сетевые программные средства на основе сервера:

- Windows XP (Microsoft);
- Windows Server 2003 (Microsoft);
- Windows Server 2008 (Microsoft);
- Linux.

На файл-сервере в данном случае устанавливается сетевая операционная система Эта сетевая ОС специально оптимизирована для эффективного вы-

полнения специфических операций по организации сетевого обмена

Для администрирования сети (то есть управления распределением ресурсов, контроля права доступа, за защитой данных, за файловой системой, резервированием файлов и т.д.) в случае сети на основе сервера необходимо выделять специального человека, имеющего соответствующую квалификацию. Централизованное администрирование облегчает обслуживание сети и позволяет оперативно решать все вопросы. Особенно это важно для надежной защиты данных от несанкционированного доступа. В случае же одноранговой сети можно обойтись и без специалиста-администратора, правда, все пользователи сети должны при этом иметь хоть какое-то представление об администрировании.

Требования производителей к операционной системе, техническим характеристикам рабочих станций и серверов для построения ЛВС ПЦО при работе с СПИ/РСПИ, применяемыми в подразделениях вневедомственной охраны приведены в таблице 5.1. Следует отметить, что в соответствии с требованиями производителей, сетевой протокол в ЛВС систем и радиосистем, указанных в таблице, обязательно должен быть TCP/IP.

Таблица 5.1

	СПИ							**РСПИ**			
	Приток-А	**Ахтуба**	**Альтаир**	**Юпитер**	**Атлас-20,**	**Заря**	**Радиосеть**	**Струна-5**	**Аргон, Аргон-Стрелец**	**Иртыш-ЗР**	**Протон**
Поддержка операционных систем (ОС)											
Рабочие станции											
- Windows 2000	+		+	+	+	+	+	+	+		
- Windows XP	+	+	+	+	+	+	+	+	+	+	+
- Windows Vista					+				+		
- Windows 7	+		+			+	+				
Сервер											
- Windows XP		Win XP Pro SP2	+					+		+	+
- Windows Server 2000, 2003, 2008.	+		+	+	+	+	+		+		+
- Linux						мар-шрути-затор					

	СПИ							РСПИ			
	Приток-А	**Ахтуба**	**Альтаир**	**Юпитер**	**Атлас-20,**	**Заря**	**Радио-сеть**	**Струна-5**	**Аргон, Аргон-Стрелец**	**Иртыш-ЗР**	**Протон**
Минимальные требования к рабочим станциям											
- процессор	Pentium 4 2400	Intel P4	Pentium II 300 МГц;	Celeron 1200 и выше	Intel P4	Penti-unII 300 МГц	Intel P4 3.00 GHz	Pentiun 133 МГц	Intel P4	Penti-unII 300 МГц	Intel P 1200
- оперативная память	1Гб	1Gb	128 Мб	512 Mb	256Mb	128Mb	1GB	128Мб	256Mb	512 Mb	256 Mb
- жесткий диск	80 Гб	40 Гб	1Gb	20 Gb	20 Gb	2Gb	40 Gb	1GB	20 Gb	1Gb	80Gb
- видеокарта	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64Mb	SVGA 64
- наличие звуковой карты, колонок	+			+			+			+	+
- наличие сетевой карты	10/100 Mb/c	100/1000 Mb/c	100Mb/c	100 Mb/c	100 Mb/c	100 Mb/c	100 Mb/c	10/100 Mb/c	100 Mb/c	10/100 Mb/c	10/100 Mb/c
- наличие LPT-порта(для ключа)		HASP-ключ									
- наличие USB – портов			Питание модем				USB-ключ				+

	СПИ							РСПИ			
	Приток-А	**Ахтуба**	**Альтаир**	**Юпитер**	**Атлас-20,**	**Заря**	**Радио-сеть**	**Струна-5**	**Аргон, Аргон-Стрелец**	**Иртыш-ЗР**	**Протон**
Минимальные требования к серверам											
- процессор	Pentium Xeon 2.4	Intel P4	Intel P2	Celeron 1200 и выше	Intel P4	Penti-unII 300 МГц		Pen-tium 133 МГц	Intel P4	Penti unII 300 МГц	Intel P 4 2400
- оперативная память	2Гб	1Gb	1Gb	1Gb	256 Mb	256Mb		256Mb	256 Mb	1Gb	2Gb
- жесткий диск	300Гб	80Gb	100Gb	40Gb	40Gb	4Gb		2Gb	40Gb	2Gb	100Gb
- поддержка RAID											
- наличие сетевой карты	1000 Mb/c	100/1000 Mb/c	100Mb/c	100Mb/c	100Mb/c	100Mb/c		100 Mb/c	100Mb/c	100 Mb/c	100 Mb/c
- наличие CD (DVD) – привода	+	+	+	+	+	+	+	+	+	+	+
- наличие LPT-порта		HASP-ключ									
- наличие USB - портов	+	+	USB - ключ			USB - ключ					
- наличие UPS	2200VA	600VA	600VA	+	+	+	+	+		+	+

5.2 Стандартные локальные сети. Сети Ethernet и Fast Ethernet

За время, прошедшее с появления первых локальных сетей, было разработано несколько сотен самых разных сетевых технологий, однако заметное распространение получили всего несколько сетей, что связано прежде всего с поддержкой этих сетей известными фирмами и с высоким уровнем стандартизации принципов их организации. Далеко не всегда стандартные сети имеют рекордные характеристики, обеспечивают наиболее оптимальные режимы обмена, но большие объемы выпуска их аппаратуры и, следовательно, ее невысокая стоимость обеспечивают им огромные преимущества. Немаловажно и то, что производители программных средств также в первую очередь ориентируются на самые распространенные сети. Поэтому пользователь, выбирающий стандартные сети, имеет полную гарантию совместимости аппаратуры и программ.

В настоящее время тенденция уменьшения количества типов используемых сетей все усиливается. Дело в том, что увеличение скорости передачи в локальных сетях до 100 и даже до 1000 Мбит/с. требует применения самых передовых технологий, проведения серьезных и дорогих научных исследований. Естественно, это могут позволить себе только крупнейшие фирмы, которые, конечно же, поддерживают свои стандартные сети и их более совершенные разновидности. Поэтому в ближайшем будущем вряд ли стоит ожидать принятия принципиально новых стандартов.

Наибольшее распространение среди стандартных сетей получила сеть Ethernet. Впервые она появи-

лась в 1972 году (разработчиком выступила известная фирма Xerox). Сеть оказалась довольно удачной, и вследствие этого ее в 1980 году поддержали такие крупнейшие фирмы, как DEC и Intel (объединение этих фирм, поддерживающих Ethernet, назвали DIX по первым буквам их названий). Стараниями этих фирм в 1985 году сеть Ethernet стала международным стандартом, ее приняли крупнейшие международные организации по стандартам: комитет 802 IEEE (Institute of Electrical and Electronic Engineers) и ECMA (European Computer Manufacturers Association).

Стандарт получил название IEEE 802.3 .Он определяет множественный доступ к моноканалу типа «шина» с обнаружением конфликтов и контролем передачи, то есть с уже упоминавшимся методом доступа CSMA/CD. Вообще-то надо сказать, что этому стандарту удовлетворяют и некоторые другие сети, так как он не очень сильно детализирован. В результате сети стандарта IEEE 802.3 нередко несовместимы между собой как по конструктивным, так и по электрическим характеристикам. Основные характеристики стандарта IEEE 802.3: топология - шина, среда передачи - коаксиальный кабель, скорость передачи - 10 Мбит/сек.

Сеть Ethernet сейчас наиболее популярна в мире. Этому в немалой степени способствовало то, что с самого начала все характеристики, параметры, протоколы сети были открыты для всех, в результате чего огромное число производителей во всем мире стали выпускать аппаратуру Ethernet, полностью совместимую между собой.

В классической сети Ethernet применяется 50-омный коаксиальный кабель двух видов (толстый и тонкий). Однако в последнее время (с начала 90-х годов) все большее распространение получает версия Ethernet, использующая в качестве среды передачи витые пары. Определен также стандарт для применения в сети оптоволоконного кабеля. В стандарты были внесены соответствующие добавления. В 1995 году появился стандарт на более быструю версию Ethernet, работающую на скорости 100 Мбит/с (так называемый Fast Ethernet, стандарт IEEE 802.3u), использующую в качестве среды передачи витую пару или оптоволоконный кабель. Появилась и версия на скорость 1000 Мбит/с (Gigabit Ethernet, стандарт IEEE 802.3z).

Помимо стандартной топологии «шина» применяются также топологии типа «пассивная звезда» и «пассивное дерево». При этом предполагается использование репитеров и пассивных (репитерных) концентраторов, соединяющих между собой различные части (сегменты) сети (рис. 5.2.1).

В сети Fast Ethernet не предусмотрена физическая топология «шина», используется только «пассивная звезда» или «пассивное дерево». К тому же в Fast Ethernet гораздо более жесткие требования к предельной длине сети. Ведь при увеличении в 10 раз скорости передачи и сохранении формата пакета его минимальная длина становится в десять раз короче (5,12 мкс против 51,2 мкс в Ethernet). Допустимая величина двойного времени прохождения сигнала по сети уменьшается в 10 раз.

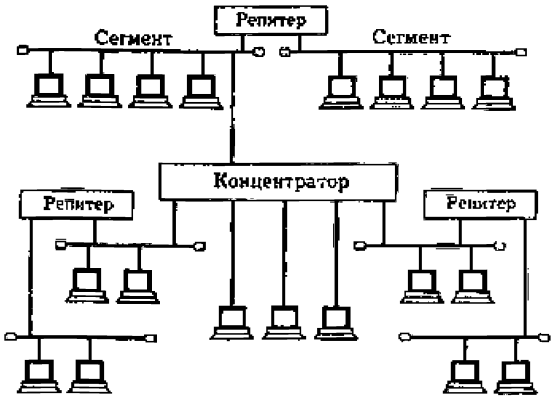


Рис. 5.2.1. Топология сети Ethernet

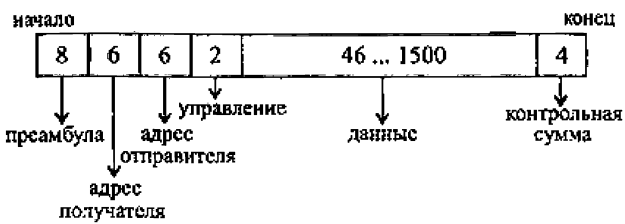


Рис. 5.2.2. Структура пакета сети Ethernet, (цифры показывают количество байт)

Доступ к сети Ethernet осуществляется по случайному методу CSMA/CD, обеспечивающему полное равноправие абонентов. В сети используются пакеты переменной длины со структурой, представленной на

рис. 5.2.2. Длина кадра Ethernet должна быть не менее 512 битовых интервалов, или 51,2 мкс. Предусмотрена индивидуальная, групповая и широковещательная адресация.

В пакет Ethernet входят следующие поля:

- Преамбула состоит из 8 байт, первые семь из которых представляют собой код 10101010, а последний восьмой - код 10101011. В стандарте IEEE 802.3 этот последний байт называется признаком начала кадра (SFD - Start of Frame Delimiter) и образует отдельное поле пакета.

- Адрес получателя (приемника) и адрес отправителя (передатчика) включают по 6 байт. Эти адресные поля обрабатываются аппаратурой абонентов.

- Поле управления (L/T - Length/Type) содержит информацию о длине поля данных. Поле управления обрабатывается программно.

- Поле данных должно включать в себя от 46 до 1500 байт данных.

- Поле контрольной суммы (FCS — Frame Check Sequence) содержит 32-разрядную циклическую контрольную сумму пакета и служит для проверки правильности передачи пакета.

Минимальная длина кадра (пакета без преамбулы) составляет 64 байта (512 бит). Эта величина определяет максимально допустимую двойную задержку распространения сигнала по сети в 512 битовых интервалов (51,2 мкс для Ethernet, 5,12 мкс для Fast Ethernet). Стандарт предполагает, что преамбула может уменьшаться при прохождении пакета через различные сетевые устройства, поэтому она не учитывается. Максимальная длина кадра равна 1518 байтам (12144 бита,

то есть 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet). Это важно для выбора размера буферной памяти сетевого оборудования и для оценки общей загруженности сети.

Для сети Ethernet, работающей на скорости 10 Мбит/с, стандарт определяет четыре основных типа среды передачи информации:

- 10BASE5 (толстый коаксиальный кабель);
- 10BASE2 (тонкий коаксиальный кабель);
- 10BASE-T (витая пара);
- 10BASE-FL (оптоволоконный кабель).

Точно так же для сети Ethernet, работающей на скорости 100 Мбит/с (Fast Ethernet) стандарт определяет три типа среды передачи:

- 100BASE-T4 (счетверенная витая пара);
- 100BASE-TX (сдвоенная витая пара);
- 100BASE-FX (оптоволоконный кабель).

Сеть Ethernet не отличается ни рекордными характеристиками, ни оптимальными алгоритмами, она уступает по ряду параметров другим стандартным сетям. Но благодаря мощной поддержке, высочайшему уровню стандартизации, огромным объемам выпуска технических средств, Ethernet резко выделяется среди других стандартных сетей, и поэтому любую другую сетевую технологию принято сравнивать именно с Ethernet.

6. Типовой вариант аппаратно-программной платформы ЛВС

Локальные сети для работы с СПИ, применяемыми подразделениями вневедомственной охраны, строятся на ПЦО, как правило, по топологии «звезда». В качестве центрального звена в данном случае используется коммутатор или концентратор, а периферийными абонентами данной «звезды» будут являться сервер(ы) и компьютеры с установленным ПО АРМ: АРМ ДПУ, АРМ ДПЦО, АРМ Инженера и др. Основным достоинством топологии «звезда» является простота сопровождения и поиска неисправностей. Повреждение в кабеле отражаются только на устройстве (ПК), к которому подключен кабель. Такие изолированные неисправности намного легче обнаружить и устранить, чем в шинной топологии. Единственным недостатком физической топологии «звезда» является несколько больший расход кабеля и трудозатраты на его прокладку. По мнению ИТ-специалистов топология ЛВС типа «звезда» - наиболее популярная топология в современных локальных сетях.

Локальную сеть ПЦО целесообразно создавать при количестве охраняемых объектов свыше 500. В данном случае на ПЦО организуется одноранговая ЛВС на базе ПЭВМ под управлением соответствующей ОС, рекомендуемой производителем СПИ. При этом используется, как правило, следующее оборудование: сетевой коммутатор Ethernet на 8-16 портов 10/100/1000 Мбит/с, сетевые платы в ПЭВМ. На ПЭВМ устанавливается программное обеспечение СПИ: АРМ ДПУ, АРМ ДПЦО и АРМ Инженера или

иные схожие по функциям АРМ, имеющиеся в составе СПИ. В случае использования сетей передачи данных по каналам VPN от СПИ, установленных на территориально удаленных или оснащенных цифровыми каналами связи АТС применяется каналообразующее оборудование стандартов ADSL/SHDSL, а также преобразователи интерфейсов RS-232/Ethernet. Для обмена информацией с объектовыми устройствами, работающими по каналу GSM/GPRS, на ЛВС используется рекомендованные производителем СПИ специализированные GSM/GPRS модемы. Линии передачи ЛВС, как правило, прокладываются кабелем неэкранированная «витая пара» UTP Cat 5-E.

На рис. 6.1 представлена типовая схема организации одноранговой ЛВС на ПЦО для работы СПИ. Следует отметить, что для СПИ «Радиосеть» одноранговая сеть является основной технологией для построения локальной сети на ПЦО.

При увеличении количества охраняемых объектов (ориентировочно свыше 1000 объектов) для повышения надежности системы централизованной охраны, повышения быстродействия и удобства работы с СПИ в состав локальной сети ПЦО целесообразно включить сервер, на котором, как правило, ведется единая база данных охраняемых объектов, размещаются архивы, отчеты и другая служебная информация. На рис. 6.2 представлена примерная структурная схема локальной сети ПЦО, в составе которой имеется сервер БД.

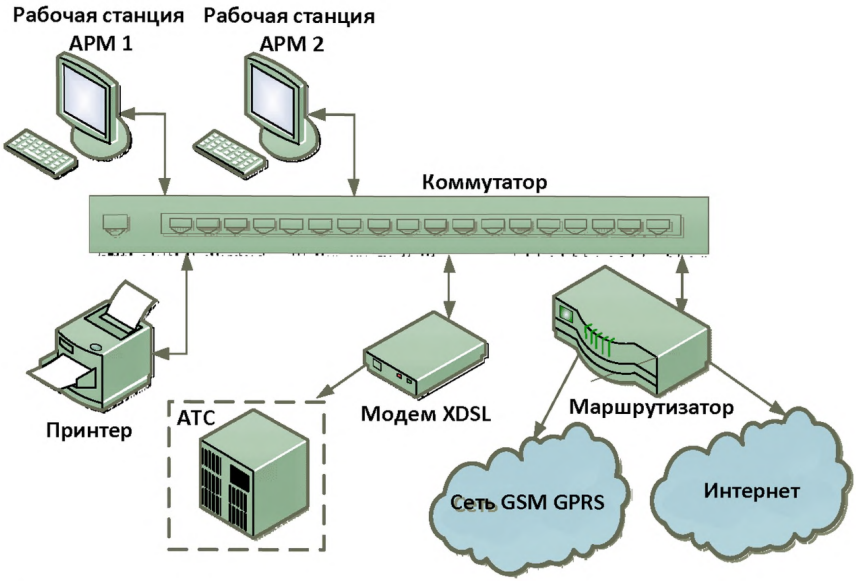


Рис. 6.1 Примерная схема организации одноранговой ЛВС на ПЦО

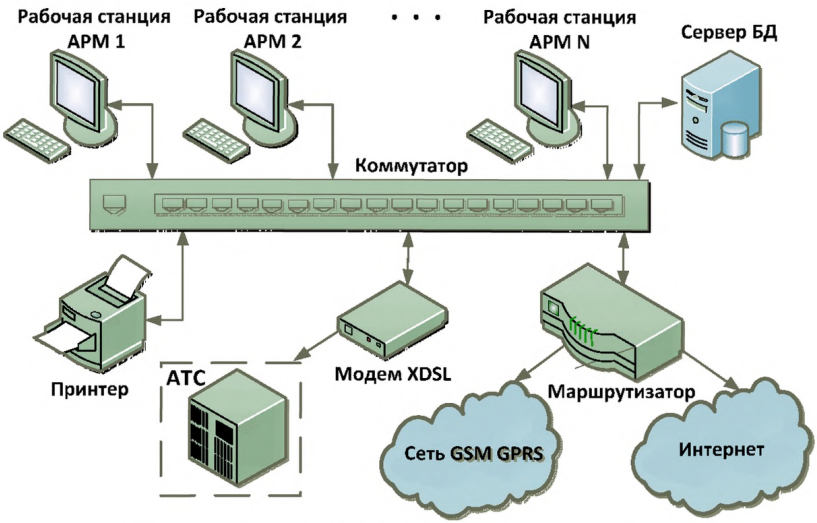


Рис. 6.2 Примерная схема организации на ПЦО локальной сети с сервером БД

В случае дальнейшего роста количества охраняемых объектов для обеспечения надежной и стабильной работы ЛВС ПЦО, для устойчивой работы локальной сети и для защиты от возможных сбоев в работе основного сервера необходимо иметь резервный сервер, на котором в реальном режиме будет осуществляться копирование основной базы данных и другой необходимой служебной информации.

Следует отметить, что в ряде СПИ, в частности в СПИ «Приток-А» и «Ахтуба», предприятия-производители систем рекомендуют при организации ЛВС иметь два сервера – основной и резервный. На рис. 6.3 представлена примерная структурная схема ЛВС ПЦО с двумя серверами, а также сервером подключения (требуется для СПИ «Приток-А»), через который осуществляется обмен информации с объектовым оборудованием, работающим по каналам открытого Интернета.

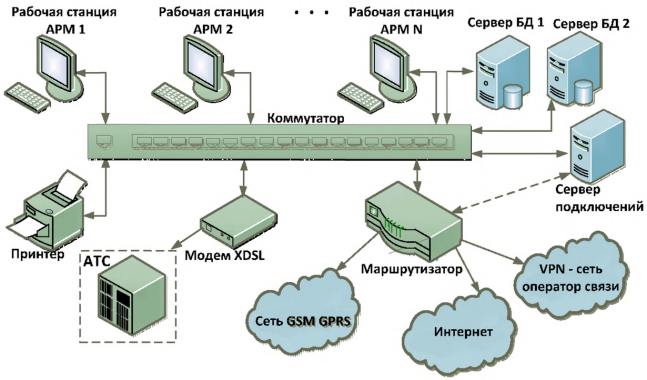


Рис. 6.3 Примерная схема организации на ПЦО локальной сети с основным и резервным сервером БД и сервером подключений (для СПИ «Приток-А»)

В табл. 6.1 приведен перечень СПИ, применяемых подразделениями вневедомственной охраны для централизованной охраны объектов, квартир и МХИГ, с указанием топологии локальной сети, организуемой на ПЦО.

Таблица 6.1

Наименование СПИ	**Приток-А**	**Ахтуба**	**Альтаир**	**Юпитер**	**Атлас-20,**	**Заря**	**Радиосеть**
Скорость обмена данными в ЛВС	1000 Мбит/с в шине серверов; 100 Мбит/с между АРМами	100/ 1000 Мбит/с	100 Мбит/с	100 Мбит/с	100 Мбит/с	100 Мбит/с	100 Мбит/с
Среда передачи данных в ЛВС	кабель - неэкранированная «витая пара» UTP Cat 5-E						
Топология ЛВС	«звезда»/ распределенная «звезда» («дерево»)						

При построении ЛВС на ПЦО главная задача — проектирование будущей сети, поскольку благодаря правильно выбранной структуре и топологии сети

можно значительно повысить скорость и функциональность системы и сократить расходы на ее создание и обслуживание.

Для того чтобы сформировать локальную сеть, необходимо провести серьезную подготовительную работу, изучить потребность в прокладке кабеля ЛВС, определить ее состав и структуру, выбрать топологию сети, среду и протоколы передачи данных. Располагая такой информацией, можно выбрать способы реализации ЛВС и оборудование для ее создания, рассчитать ориентировочную стоимость.

Рассмотрим ряд основных вопросов, которые необходимо решить при построении локальной сети ПЦО.

Первый из них — пропускная способность сети, или скорость обмена данными. В настоящее время каждый ПК оснащается встроенным сетевым интерфейсом, рассчитанным на скорость обмена данными до 1000 Мбит/с, существуют и коммутаторы, поддерживающие такую скорость. Строить гигабитную сеть имеет смысл только тогда, когда по ней будут передаваться действительно большие объемы информации, что вполне возможно при работе с базами данных, обработке медиаконтента (видео- и аудиофайлов), интенсивном использовании сетевых приложений. В остальных случаях достаточно 100 Мбит/с. Нужно понимать и то, что высокая скорость может понадобиться при обмене с сервером, который целесообразнее всего подключать к коммутатору высокоскоростным соединением, при этом локальные порты клиентских ПК обеспечивают более низкую скорость, чем серверные.

Второй вопрос — размещение рабочих мест и управляющих узлов, а также периферийного оборудования. Хорошо, если все компьютеры находятся в одной комнате, и равномерно распределены по площади: при подобном варианте прокладка кабелей не составит труда, и все выходы легко подсоединить к одному коммутатору на нужное количество входов. Если же рабочие места разделены на группы (комнаты), следует продумать стратегию размещения не только кабелей, но и активного сетевого оборудования: например, для пяти комнат по пять человек целесообразнее приобрести шесть коммутаторов (по одному на каждую комнату плюс один объединяющий), чем тянуть кабели к одному узлу. Возможны и другие проблемы, в частности наличие удаленных точек, которые могут находиться на значительном расстоянии от основного помещения — 200–300 м, что превышает допустимое расстояние для витой пары (до 100 м). Следовательно, в этом случае придется использовать другие виды связи с помощью дополнительного оборудования.

Важно помнить, что проектирование ЛВС базируется на принципах структурирования и именно структурированные кабельные сети позволяют решать любые задачи максимально качественно и надежно, поэтому лучше всего применять полноценные решения, включающие пассивные элементы: телекоммуникационные шкафы-стойки, патч-панели, короба и розетки. Данный подход позволит в перспективе легко масштабировать сеть до требуемых размеров, а при необходимости и переместить ее в другое помещение.

Количество коммутаторов следует предусмотреть, исходя из наиболее удобного расположения сег-

ментов сети, и не стремиться подключить «всё к одному», поскольку выход из строя этого коммутатора приведет к отказу всей сети. К примеру, для ЛВС ПЦО на 25 клиентских мест, содержащую сетевой принтер, файловый сервер, шлюз в Интернет необходимо иметь минимум 29 портов, к которым надо обязательно добавить несколько резервных точек подключения. В данном случае можно установить коммутатор на 48 портов, что видимо нецелесообразно, так как лучше установить два коммутатора по 16 или 24 портов, каскадировав их. В такой схеме отказ одного позволит сохранить работоспособность всей сети в целом, даже если придется временно отсоединить одно-два рабочих места. Большее количество коммутаторов целесообразно предусматривать, если планируется разбивка ЛВС на рабочие группы или если рабочие места находятся в разных комнатах.

7 Проектирование ЛВС Ethernet на ПЦО.

7.1 Выбор размера сети и ее структуры

При создании новой локальной сети для ПЦО желательно учитывать следующие факторы:

- Требуемый размер ЛВС.
- Основные направления и интенсивность информационных потоков.
- Технические характеристики оборудования и его стоимость.
- Возможности прокладки кабельной системы в помещениях и между ними, а также меры обеспечения целостности кабеля.
- Обеспечение обслуживания ЛВС и контроля за ее безотказностью и безопасностью.
- Требования к программным средствам по допустимому размеру ЛВС, скорости, гибкости, разграничению прав доступа, стоимости, возможностям контроля за обменом информацией, и т.д.
- Необходимость подключения к глобальным сетям или к другим локальным сетям.

Первым этапом проектирования ЛВС ПЦО должен быть определен её размер и структура. Под размером ЛВС в данном случае понимается минимальное количество объединяемых в сеть компьютеров, и расстояния между ними с учетом дальнейшего роста количества компьютеров в ЛВС на 20-50%.

Если на ПЦО будет эксплуатироваться СПИ только одного производителя, то топология ЛВС ПЦО будет соответствовать топологии ЛВС СПИ, рекомендованной производителем (Рис. 7.1.1). Если на ПЦО будет эксплуатироваться несколько СПИ, то топология ЛВС ПЦО будет смешанной (Рис. 7.1.2).

Обычно при проектировании ЛВС точно неизвестно количество подключаемого оборудования - известны, лишь, типы эксплуатируемых СПИ. Однако среди всего разнообразия СПИ можно выделить обязательное сетевое оборудование, входящее в состав любого СПИ: принтер (МФУ), ПК АРМа инженера (администратор), ПК АРМа дежурного офицера (АРМ ДПЦО). Также неизвестны перспективы развития каждого конкретного СПИ: состав СПИ может изменяться со временем, СПИ может быть модернизирована , увеличено количество её АРМ ДПУ или вообще демонтирована. ЛВС ПЦО необходимо строить так, чтобы все изменения в количественном составе сетевого оборудования ЛВС ПЦО не влияли или минимально отражались на работоспособности остального сетевого оборудования. Поэтому ЛВС ПЦО рекомендуется строить по схеме «звезда», объединяя не оборудование в целом, а локальные сети СПИ применяемых на ПЦО. Именно по такой схеме расширение конкретной СПИ, демонтаж её оборудования, временное исключение её из ЛВС ПЦО (на время ремонта) или включение новой СПИ в состав ЛВС ПЦО, минимизирует влияние на работоспособность и взаимодействие остального оборудования ЛВС ПЦО. Перед проектированием необходимо изучить руководство по эксплуатации каждой СПИ, изучить состав сетевого оборудования, схему организации ЛВС каждой СПИ, рекомендуемую производителем. Если схема ЛВС СПИ не представлена производителем, то её необходимо начертить самостоятельно - как правило, ЛВС СПИ строится по схеме: набор серверов, подключённых к коммутатору, к которому в свою очередь подключены АРМы различного назначения и принтер.

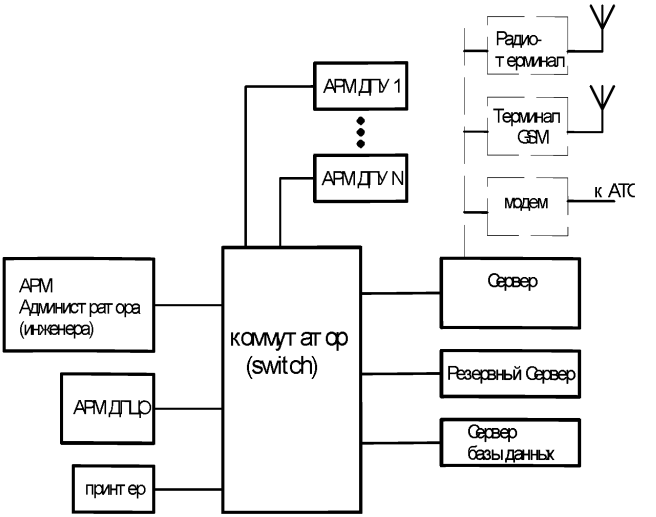


Рис. 7.1.1. Структура ЛВС СПИ.

После анализа схемы ЛВС каждой СПИ определяются сходные программно –аппаратные средства входящие в состав каждой СПИ, что экономит оборудование и пространство рабочего места. Как правило, это оборудование доступа к поставщикам услуг сети «Интернет» (провайдер), принтер.

Затем проектируется общая схема ЛВС ПЦО, в которую включается дополнительное сетевое оборудование, например, коммутатор, связывающий составные части ЛВС ПЦО между собой, сервер ЛВС ПЦО, Видео-сервер и т.д.

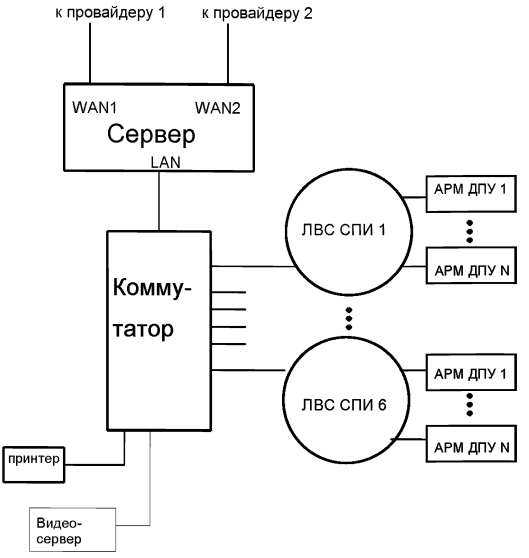


Рис. 7.1.2. Структура ЛВС ПЦО.

Согласно руководствам по эксплуатации СПИ определяется диапазон IP-адресов для каждой ЛВС СПИ: наименьшие номера адресов должны присваиваться постоянному оборудованию: принтеру, АРМ ДПЦО, АРМ Администратора, серверам ЛВС СПИ. Имена всех ПК входящих ЛВС ПЦО должны быть уникальными и области IP-адресов ЛВС СПИ, по возможности не должны, пересекаться друг с другом.

7.2 Выбор оборудования

При выборе эксплуатируемого на ПЦО оборудования необходимо руководствоваться его унификацией, учитывая при этом соотношение цена/качество.

Компьютеры

Компьютеры необходимо выбирать в соответствии с требованиями к техническим характеристикам рабочих станций и серверов для построения ЛВС ПЦО при работе с СПИ/РСПИ, применяемыми в подразделениях вневедомственной охраны, приведенными в таблице 5.1. ПК, например, АРМ различного назначения можно выбрать одного типа, т.к. требования аппаратные к ним примерно одинаковы. К серверам предъявляемые требования несколько другие: они могут быть выполнены не только в обычном конструктивном исполнении, но и в корпусе для крепления в 19" стойку. Также более высокие требования предъявляются к производительности, объёму памяти и количеству коммуникационных портов и слотов. Поэтому унификации серверов может и не получиться.

Сервер ПЦО резервирование обеспечивает доступ к сети «Интернет», Интернет-соединения, связь ЛВС ПЦО с ведомственной сетью (при ее наличии), защиту ЛВС ПЦО от различных сетевых атак и «вирусов. Сервер ПЦО может быть организован на платформе обычного ПК. Современные ПК выпускаются уже со встроенной гигабитной сетевой картой, и, для реализации доступа и резервирования сети «Интернет», в компьютер сервера ПЦО необходимо установить две сетевые карты с сетевой скоростью 100BASE-TX, к которым подключается оборудование

поставщиков интернет-услуг (провайдеров). Если же требуется беспроводное резервирование, то к USB-порту подключается рекомендуемый провайдером 3G/4G-модем. Вместо компьютера сервера ПЦО может быть применён аппаратный межсетевой экран с двумя WAN-портами: в такое устройство уже включены антивирусная защита и защита от сетевых атак. Преимуществом серверов перед аппаратными межсетевыми экранами является своевременное обновление программного обеспечения по защите от различного вида сетевых атак и «вирусов», возможность смены производителя такого ПО, удобный подсчёт трафика и анализ сетевых атак.

Коммутаторы

Сетевой коммутатор - устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. В настоящее время выпускается очень много видов коммутаторов с многообразными характеристиками, поэтому выбор коммутатора достаточно затруднён. Можно выделить несколько рекомендаций по выбору коммутатора:

- все коммутаторы в ЛВС должны быть одного производителя;
- наличие портов 10/100BASE-TX;
- при наличии в ЛВС видео-сервера, IP-телефонии коммутатор должен обладать портами 10/100/1000BASE-TX;
- если необходима маршрутизация в ЛВС, то лучше применить коммутатор с функцией маршрутизации;

- по возможности, неуправляемые коммутаторы.

Также при выборе коммутатора рекомендуется руководствоваться принципом унификации: если в ЛВС СПИ достаточно 5-портового коммутатора, а в другой ЛВС СПИ необходим коммутатор с восемью портами, то лучше применить два 8-портовых коммутатора.

В ЛВС ПЦО достаточно 16-портового коммутатора при топологии ЛВС приведённой на Рисунке 7.1.1.

Оборудование доступа в сеть «Интернет»

Как правило, провайдеры рекомендуют своим абонентам применять оборудование доступа в Интернет, которое они сами же и сертифицировали, или даже просто не оставляют вариантов выбора. Так, абонентское оборудование сети GPON практически незаменимо, т.к. оно работает совместно с серверным оборудованием только своего производителя. Поэтому следует применять оборудование доступа в Интернет рекомендованное провайдером, который гарантирует устойчивую связь именно с этим оборудованием.

Принтер

Принтер (МФУ) на ПЦО следует использовать без подключения к какому-либо компьютеру, т.е. принтер должен быть включен в ЛВС ПЦО. Такое решение позволяет поместить принтер в любом месте помещения ПЦО, и, он останется доступным в независимости от неисправности какого-либо компьютера. Поэтому принтер, в первую очередь, должен обладать свойством подключения в ЛВС.

7.3 Размещение

После создания схемы ЛВС ПЦО и выбора оборудования приступают к размещению ЛВС ПЦО на плане помещения ПЦО, т.е. решается вопрос: «Что и где должно находиться?». На этом этапе необходимо знать количественные данные сетевого оборудования и перспективы развития, эксплуатируемых на ПЦО СПИ. Основные требования к размещению оборудования следующие: площадь каждого АРМ должна составлять не менее 6 кв. метров, а расстояние между мониторами – не менее двух метров.

Коммутаторы ЛВС СПИ следует размещать равноудалённо от компьютеров АРМ ДПУ, т. к. наибольшее количество сетевых соединений приходится именно на компьютеры этих рабочих мест. Такое размещение позволяет сократить общую длину сетевых соединений и использовать стандартные кабели. Также это относится и к коммутатору ЛВС ПЦО.

Для минимизации длины прокладываемых кабелей, рекомендуется компоновать всё сетевое оборудование каждой отдельной СПИ в одном месте.

Требуемая длина линий связи сети играет большую роль в проектировании сети, чем количество компьютеров. При большом расстоянии линий связи сети может понадобиться дополнительное оборудование. С увеличением расстояния резко возрастает зависимость линий связи от внешних электромагнитных помех и уменьшается скорость передачи информации по сети. При выборе расстояний нужно закладывать примерно 10% запас для учета различных непредвиденных обстоятельств.

Рекомендуется применять готовые, покупные кабели (патч-корды: RJ 45, вилка - RJ 45, вилка) категории

5е и выше с уже заделанными разъёмами, поскольку промышленно изготовленные кабели обеспечивают более надёжную опрессовку контактов и герметичность разъёма, чем изготовление кабеля ручным способом.

Фабрично патч-корды с вилками RJ-45 изготавливаются несколькими стандартными длинами: 0.5м, 1м, 1.5 м, 2м, 3м, 5м, 7м,10м. Шнуры меньшей и большей длины распространены меньше и обычно производятся на заказ, но в продаже есть и длины 15м и 20м.

7.4 Электропитание и защитное заземление.

Оборудование ЛВС подключается к питающей электросети ПЦО через источники бесперебойного питания.

Все розетки сети 220 Вольт должны быть с заземлением, поскольку, в большинстве случаев компьютерное оборудование не имеет отдельных клемм заземления.

Допустимая мощность нагрузки подключаемой к электрической сети ПЦО должна быть выше совокупной мощности потребляемой оборудованием ЛВС ПЦО.

При подключении активного сетевого оборудования к электропитанию необходимо руководствоваться требованиями документа «Правила устройства электроустановок (ПУЭ). Седьмое издание. Дата введения 01.01.03.»

Сечение токопроводящих жил для подключения активного сетевого оборудования необходимо выбирать исходя из таблицы 1.3.4 ПЭУ.

Защита от поражения электрическим током должна соответствовать требованиям раздела 1.7 ПУЭ.

В сетях, защищаемых от перегрузок, проводники следует выбирать по расчетному току, при этом

должно быть обеспечено условие, чтобы по отношению к длительно допустимым токовым нагрузкам аппараты защиты имели кратность не более:

- 80% для номинального тока плавкой вставки или тока уставки автоматического выключателя, имеющего только максимальный мгновенно действующий расцепитель (отсечку), - для проводников с поливинилхлоридной, резиновой и аналогичной по тепловым характеристикам изоляцией; для проводников, прокладываемых в невзрывоопасных производственных помещениях промышленных предприятий, допускается 100%;

- 100% для номинального тока плавкой вставки или тока уставки автоматического выключателя, имеющего только максимальный мгновенно действующий расцепитель (отсечку), - для кабелей с бумажной изоляцией;

- 100% для номинального тока расцепителя автоматического выключателя с нерегулируемой обратно зависящей от тока характеристикой (независимо от наличия или отсутствия отсечки) - для проводников всех марок;

- 100% для тока трогания расцепителя автоматического выключателя с регулируемой обратно зависящей от тока характеристикой - для проводников с поливинилхлоридной, резиновой и аналогичной по тепловым характеристикам изоляцией;

- 125% для тока трогания расцепителя автоматического выключателя с регулируемой обратно зависящей от тока характеристикой - для кабелей с бумажной изоляцией и изоляцией из вулканизированного полиэтилена.

Таблица 7.1.4.1 Допустимый ток для проводов и шнуров с резиновой и поливинилхлоридной изоляцией с медными жилами

Сечение токопроводящей жилы, мм^2	Ток, А, для проводов, проложенных					
	открыто	в одной трубе				
		двух одножильных	трех одножильных	четырех одножильных	одного двухжильного	одного трехжильного
0,5	11	-	-	-	-	-
0,75	15	-	-	-	-	-
1	17	16	15	14	15	14
1,2	20	18	16	15	16	14,5
1,5	23	19	17	16	18	15
2	26	24	22	20	23	19
2,5	30	27	25	25	25	21
3	34	32	28	26	28	24
4	41	38	35	30	32	27
5	46	42	39	34	37	31
6	50	46	42	40	40	34
8	62	54	51	46	48	43
10	80	70	60	50	55	50
16	100	85	80	75	80	70
25	140	115	100	90	100	85
35	170	135	125	115	125	100
50	215	185	170	150	160	135
70	270	225	210	185	195	175
95	330	275	255	225	245	215
120	385	315	290	260	295	250
150	440	360	330	-	-	-
185	510	-	-	-	-	-
240	605	-	-	-	-	-
300	695	-	-	-	-	-
400	830	-	-	-	-	-

7.5 Грозозащита линий локальной вычислительной сети.

Устройства грозозащиты линий локальных вычислительных сетей необходимы для защиты от грозы, статического электричества, помех от работы электрических цепей, для снижения амплитуды наведенных помех, защиты оборудования от импульсной электромагнитной наводки, которая может возникать при замыкании силовых кабелей или от близлежащих линий связи; защиты от прямого попадания и от вторичных воздействий молнии, а также снятия статического заряда.

Устройства защиты должны устанавливаться между линией связи, подверженной опасному воздействию электричества, и защищаемым оборудованием. На одно защищаемое устройство устанавливается одно устройство защиты. Перед установкой устройства защиты необходимо произвести его внешний осмотр с целью выявления механических повреждений корпуса и соединительных элементов. Установка устройства должна производиться в сухом помещении. После установки устройства его необходимо в первую очередь надёжным образом подключить к защитному заземлению. Соединение с защитным заземлением должно выполняться проводом возможно большего сечения и быть по возможности коротким. Запрещается использовать устройство защиты без защитного заземления.

Рисунок 7.5.1. Внешний вид устройства грозозащиты Ethernet "I-Pro-Standart" (RJ-45).

Устройство грозозащиты сетей Ethernet "I-Pro-Standart" (рис. 7.5.1) обеспечивает защиту оборудования при всех типовых ситуациях (грозы, статика, молнии, сухой снег, ветер, помехи от работы электрических цепей и т.д.)

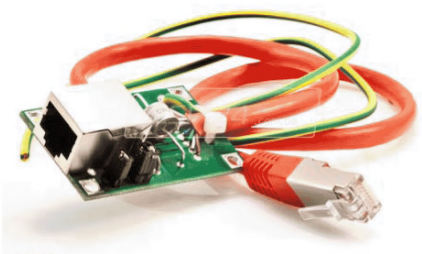


Рисунок 7.5.2. Внешний вид устройства грозозащиты Ethernet mcWit 100.

Грозозащита mcWit 100 (рис. 7.5.2) предназначена для снижения амплитуды наведенных помех, защиты оборудования от импульсной электромагнитной наводки, которая может возникать при замыкании силовых кабелей или от близлежащих линий связи; защиты от вторичных воздействий молнии, а также снятия статического заряда. Предназначена для 100 мегабитных сетей.

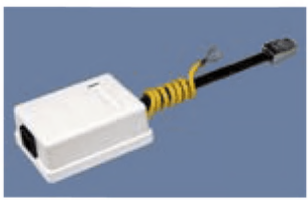


Рисунок 7.5.3. Внешний вид устройства грозозащиты Ethernet "УГЗ-1".

Устройства защиты "УГЗ-1" (рис. 7.5.3) предназначены для защиты телекоммуникационного и абонентского оборудования от повреждения высоковольтными импульсами напряжения, возникающими в физических линиях связи под воздействием грозовых разрядов, и от протекания больших токов при возникновении электрического контакта проводов линий связи с проводами силовых линий электропередач.

7.6 Пути и методы защиты информации в системах обработки данных

7.6.1 Пути и методы защиты информации в ЛВС ПЦО

Защита информации – это комплекс мероприятий, проводимых с целью предотвращения ее утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п. Поскольку утрата информации может происходить по сугубо техническим, объективным и неумышленным причинам, под это определение подпадают также и мероприятия, связанные с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и т.д.

7.6.2 Основные угрозы ЛВС ПЦО и меры по борьбе с ними

ЛВС ПЦО должна быть защищена от:

- возможного заражения информации вредоносными программными средствами;
- вторжений из внешней сети (Интернет, Ethernet, сеть мобильного оператора и др.);
- потери накопленной информации, ввиду выхода из строя жестких дисков сервера или других возможных причин (случайное или преднамеренное действие персонала, пожар и др.).

При работе ЛВС ПЦО с ретрансляторами по абонентским телефонным (выделенным) линиям существует практически одна угроза аппаратно-программному комплексу ЛВС в части возможности заражения установленного на компьютерах ЛВС про-

граммного обеспечения вредоносными программными средствами (ВПС). В случае подключения к ПЦН оконечного оборудования, установленного на объектах, квартирах и МХИГ с использованием внешних цифровых сетей (Интернет, Ethernet, сеть мобильного оператора и др.), дополнительно к угрозе заражения ВСП возникает опасность проведения в отношении ЛВС ПЦО сетевой атаки, направленной на вывод из строя аппаратно-программного комплекса СЦН и в ряде случаев - с целью совершения противоправных действий в отношении охраняемых ПЦО объектов.

7.6.3 Пути и средства защиты информации

Пути и средства обеспечения защиты информации в ЛВС ПЦО в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на следующие группы:

1. **Технические (аппаратные) средства**. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первая часть задачи решается при реализации на ПЦО защитных мероприятий согласно требованиям нормативных документов МВД России по технической укрепленности и оборудованию помещений ПЦО охранно-пожарной сигнализацией, системами контроля доступа и видеонаблюдения.

Вторая часть – это проведения мероприятий с использованием генераторов шума, сетевых фильтров, сканирующих радиоприемников, а также других уст-

ройств, "перекрывающих" потенциальные каналы утечки информации или позволяющих их обнаружить. Данные мероприятия, как правило, на ПЦО не проводятся.

2. **Программные средства** включают в себя программы для идентификации пользователей, контроля доступа к рабочим компьютерам, средства антивирусной защиты, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.

3. **Смешанные аппаратно-программные средства** реализуют те же функции, что аппаратные и программные средства в отдельности. Такие средства обеспечения безопасности могут быть реализованы как в виде специально разработанных для этого продуктов (например, межсетевые экраны), так и в виде встроенных функций операционных систем, системных приложений, компьютеров и сетевых коммуникационных устройств.

4. **Организационные средства.**

К организационным (или административным) средствам защиты информации ЛВС ПЦО относится разработка порядка работы со служебной информацией на компьютере (в т.ч. работа с USB флеш-накопителями), а также планирование и проведение соответствующего обучения и контроля за работой инженерно-технического персонала ПЦО на АРМ СПИ. При этом должны использоваться законодательные и нормативно-правовые акты, которыми регламентируются правила использования и обработки информации ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.

Для этих целей в подразделении вневедомственной охраны целесообразно разработать положение (инструкцию) по обеспечению информационной безопасности, которая, как правило, включает ответы на следующие вопросы:

- какую информацию и от кого следует защищать;
- кому и какая информация требуется для выполнения служебных обязанностей;
- какая степень защиты требуется для каждого вида информации;
- чем грозит потеря того или иного вида информации;
- как организовать работу по защите информации.

Положение описывает порядок представления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах информационной безопасности.

Поскольку система защиты информации является комплексной системой и предназначена обеспечивать безопасность всей защищаемой информации, к ней должны предъявляться следующие требования:

— она должна быть привязана к целям и задачам защиты информации для конкретного состава и структуры, в том числе ЛВС ПЦО;

— она должна быть целостной: содержать все ее составляющие, иметь структурные связи между компонентами, обеспечивающие ее согласованное функционирование;

— она должна быть всеохватывающей, учитывающей все объекты и составляющие их компоненты защиты, все обстоятельства и факторы, влияющие на безопасность информации, и все виды, методы и средства защиты;

— она должна быть достаточной для решения поставленных задач и надежной во всех элементах защиты, т. е. базироваться на принципе гарантированного результата;

— она должна быть «вмонтированной» в технологические схемы сбора, хранения, обработки, передачи и использования информации;

— она должна быть логически, технологически и экономически обоснованной;

— она должна быть реализуемой, обеспеченной всеми необходимыми ресурсами;

— она должна быть простой и удобной в эксплуатации и управлении, а также в использовании;

— она должна быть непрерывной и достаточно гибкой, способной к целенаправленному приспособлению при изменении компонентов ее составных частей, технологии обработки информации, условий защиты.

Рассмотрим ряд основных угроз в отношении ЛВС ПЦО, а также программные и аппаратные средства защиты информации, используемые с целью обеспечения информационной безопасности ЛВС ПЦО.

7.6.4 Вредоносные программы и борьба с ними

Класс вредоносных программных средств (ВПС) составляют компьютерные вирусы, троянские кони (закладки) и средства проникновения в удаленные системы через локальные и глобальные сети.

Согласно классическому определению компьютерного вируса – это программа, которая может заражать другие программы, модифицируя их посредством добавления своей, возможно измененной, копии. Ключевым понятием в определении вируса является

его способность к саморазмножению. Это единственный критерий, позволяющий отличить программы-вирусы от остальных программ. При этом «копии» вируса действительно могут структурно и функционально отличаться между собой. Вирусы постоянно расширяют свою «среду обитания» и реализуют принципиально новые алгоритмы внедрения и поведения.

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Троянские кони представляют собой программы, реализующие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

Программные закладки также содержат некоторую функцию, наносящую ущерб ПО ЛВС, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

В качестве возможных деструктивных функций, реализуемых вирусами, троянскими конями и программными закладками, следует отметить:

- уничтожение информации.
- перехват и передача информации.
- целенаправленная модификация кода программы.

Основной и по своей сути главной мерой по защите ЛВС ПЦО от ВПС являются мероприятия по установке и обязательному поддержанию в актуальном состоянии специального лицензионного антивирусного программного обеспечения, рекомендуемого предприятиями-изготовителями СПИ.

7.6.5 Использование межсетевого экрана

В стратегии защиты от несанкционированного доступа к информационным ресурсам ЛВС ПЦО особое внимание уделяется обеспечению безопасности ее границ от угроз, исходящих из внешних сетей, таких как Интернет, VPN-сеть и др. Целостность периметра локальной сети ПЦО обеспечивается использованием тех или иных базовых технологий межсетевого экранирования в точке подключения защищаемой сети к внешней неконтролируемой сети. В качестве внешней сети чаще всего выступает глобальная сеть Интернет. Систему разграничения ЛВС с различными политиками безопасности, реализующую правила информационного обмена между ними, называют межсетевым экраном (МЭ). В технической литературе также встречаются термины firewall или брандмауэр.

Межсетевой экран — это локальное (однокомпонентное) или функционально-распределенное (многокомпонентное) программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в ЛВС ПЦО и/или исходящей из нее. Основной принцип действия межсетевых экранов – проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов. Таким образом, межсетевые экраны значительно расширяют возможности сегментирования информационных сетей и контроля за циркулированием данных.

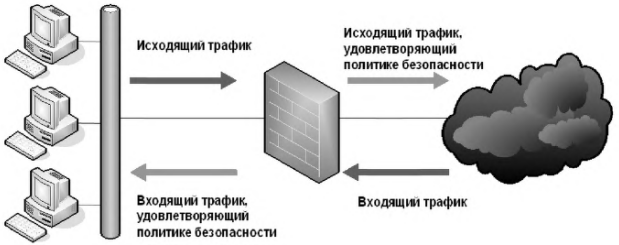


Рисунок 7.6.5. Контроль периметра сети МЭ (защищаемая сеть слева)

МЭ повышает безопасность объектов внутренней сети за счет игнорирования несанкционированных запросов из внешней среды. Это уменьшает уязвимость внутренних объектов, так как сторонний нарушитель должен преодолеть некоторый защитный барьер, в котором механизмы обеспечения безопасности сконфигурированы особо тщательно. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования. Кроме того, экранирование позволяет контролировать информационные потоки, исходящие во внешнюю среду, что способствует поддержанию во внутренней области режима конфиденциальности. Кроме функций разграничения доступа, МЭ может обеспечивать выполнение дополнительных функций безопасности (аутентификацию, контроль целостности, фильтрацию содержимого, обнаружение атак, регистрацию событий).

МЭ не является симметричным устройством, для него определены понятия «внутри» и «снаружи» (входящий и исходящий трафики). При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

7.6.6 Применение технологии трансляции сетевых адресов.

Кроме вышеупомянутых МЭ для построения системы защиты ЛВС ПЦО от внешней сети целесообразно использовать специальные устройства, обладающие механизмом трансляции сетевых адресов (NAT) — технология, которая позволяет устройству выполнять функцию прокси-сервера по сокрытию информации об узлах внутренней сети. Следует отметить, что данная технология может быть реализована почти любым маршрутизирующим устройством - маршрутизатором, межсетевым экраном, сервером доступа. Рассмотрим реализацию NAT-технологии на примере маршрутизатора.

В целях закрытия информации о внутренней сети, маршрутизатор с NAT функционирует следующим образом:

− при передаче запросов клиентов защищаемой сети во внешнюю сеть заменяет их IP-адреса на IP-адрес своего внешнего интерфейса (может использоваться и диапазон IP-адресов);

− при возврате ответов серверов клиентам производит обратную замену: свой адрес в поле получателя меняет на адрес клиента, отправившего исходный запрос (рис. 7.6.6.1).

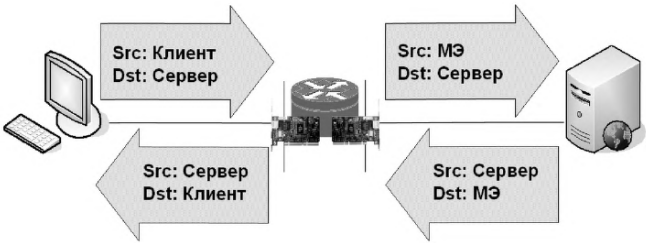


Рисунок 7.6.6.1. Технология NAT

Преимущество использования трансляции сетевых адресов состоит в том, что при подключении внутренней сети к сети Интернет технология NAT позволяет существенно увеличить адресное пространство за счет использования IP-адресов из диапазона частных сетей, не обрабатываемых маршрутизаторами Интернет.

Существует несколько методов реализации NAT. Одни трансляторы адресов осуществляют это посредством статического присваивания адресов (static address assignment), при этом адрес клиента внутренней сети связывается с фиксированным внешним IP-адресом. Другие трансляторы, функционирующие по принципу динамического присваивания адресов (dynamic address assignment), выделяют клиентам внутренней сети внешний IP-адрес по мере поступления запросов. После освобождения клиентом внешнего IP-адреса он возвращается маршрутизатором в список свободных адресов и может быть предоставлен другому клиенту.

Концепция трансляции сетевых адресов, о которой шла речь до сих пор, обычно называется базовой

трансляцией адресов (basic NAT). Ее реализация требует наличия нескольких внешних IP-адресов для обеспечения одновременной работы нескольких клиентов внутренней сети. Это означает, что число внешних IP-адресов маршрутизатора с NAT должно быть равно максимально возможному числу активных исходящих соединений. Чтобы расширить число возможных исходящих соединений и при этом не увеличивать количество отведенных маршрутизатору внешних адресов в новой форме NAT, которая называется трансляцией портов сетевых адресов (NAPT), используется замена одновременно и IP-адреса и номера порта отправителя. Таким образом, один IP-адрес можно распределить между множеством клиентов внутреннней сети просто за счет изменения номера порта отправителя. Иногда для обозначения NAPT употребляются термины «PAT» (трансляция адресов портов) и «Overloading NAT».

Технология, называемая векторизацией адресов («address vectoring») или перенаправлением портов («port mapping»), по сути, является обратной NAT и служит для обеспечения возможности доступа извне к некоторым узлам защищаемой с помощью NAT сети. МЭ с включенной функцией перенаправления портов принимает запрос на соединение от внешнего клиента и в случае допустимости поступившего запроса переадресовывает его во внутреннюю сеть на указанный в таблице перенаправления узел, причем порт назначения внутреннего узла не обязательно должен совпадать с портом назначения в запросе внешнего узла (рис. 7.6.6.2).

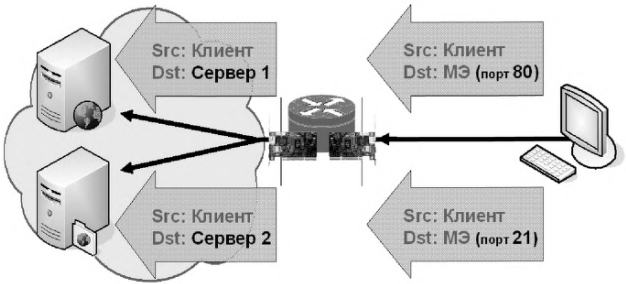


Рисунок 7.6.6.2. Технология векторизации адресов

7.7 Пример проектирования сети ПЦО на 10 рабочих мест.

На рисунке 7.7.1 приведён пример схемы ЛВС ПЦО на 10 рабочих мест при эксплуатации двух СПИ с разной топологией своих ЛВС на примере СПИ «Приток» и «Радиосеть».

СПИ «Приток» имеет топологию ЛВС на основе серверов. Все компьютеры и периферийное оборудование связи этой СПИ подключены к неуправляемому 16-канальному коммутатору (избыточные порты не показаны).

СПИ «Радиосеть» имеет одноранговую топологию ЛВС. Все компьютеры данной СПИ подключены к неуправляемому 16-канальному коммутатору (избыточные порты не показаны). 16-канальный применён из-за недостаточности резервирования 8-канального коммутатора. Периферийное оборудование связи в этой СПИ подключается непосредственно к компьютерам АРМ ДПУ, поэтому оно не показано на схеме.

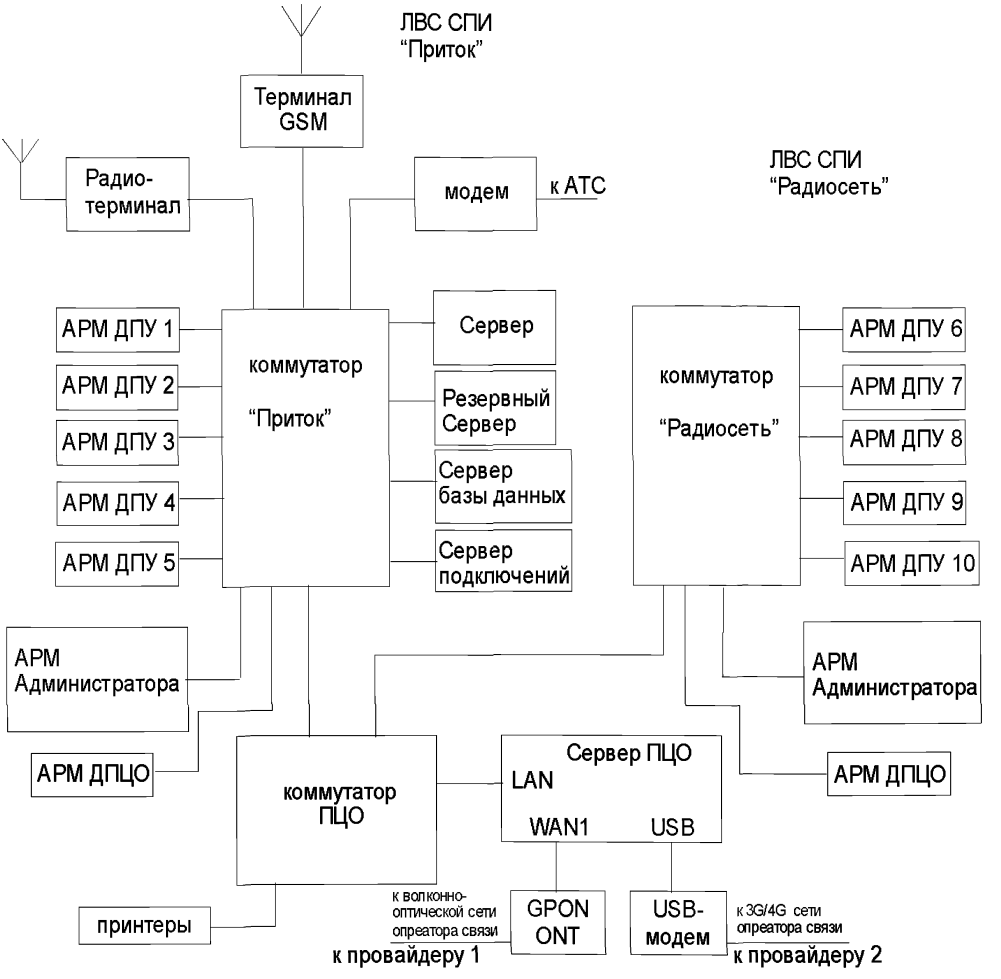


Рисунок 7.7.1. Схема ЛВС ПЦО на 10 рабочих мест

Коммутатор ПЦО с целью унификации применён в 16-канальном исполнении (избыточные порты не показаны). Он позволяет для обеих СПИ сделать общими принтер и доступ в Интернет.

Сервер ПЦО обеспечивает общий доступ в Интернет, резервирование доступа в Интернет, защиту ЛВС ПЦО от «вирусов» и сетевых атак.

Основной доступ в Интернет осуществляется по GPON технологии посредством ONT-оборудования, устанавливаемого оператором связи.

Резервирование доступа в Интернет осуществляется по беспроводной технологии посредством USB-модема.

Размещение оборудования ЛВС ПЦО на плане пультового помещения ПЦО показано на Рисунке 7.7.2.

Сервер ПЦО, периферийное оборудование связи, принтер, коммутатор ПЦО помещены между АРМ ДПУ обеих СПИ, а также и между АРМ ДПЦО и Инженера. Установка коммутатора ПЦО в центре между АРМДПУ обеих СПИ обеспечивает примерно равную удалённость от их коммутаторов, что позволяет использовать промышленно изготовленные патч-корды одинаковой длины. Установка коммутаторов СПИ в центре ряда своих АРМ ДПУ также позволяет использовать стандартные патч-корды одинаковой длины (пары патч-кордов), что сокращает номенклатуру закупаемого оборудования.

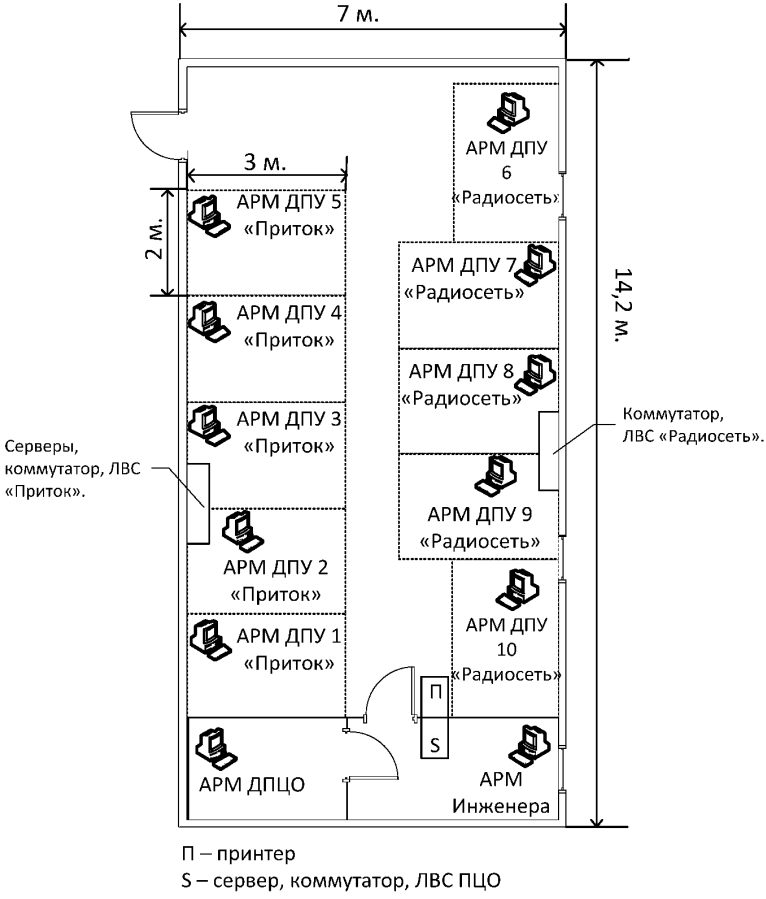


Рисунок 7.7.2. Размещение сетевого оборудования ЛВС ПЦО

8. Техническое обслуживание и устранение неисправностей ЛВС ПЦО.

8.1 Техническое обслуживание

Необходимость и возможность проведения определенных видов работ зависят от производителя, модели и конструктивных особенностей оборудования. При проведении работ необходимо тщательно изучить «Руководство по эксплуатации» на каждую модель оборудования.

Для того чтобы компоненты ЛВС работали нормально, напряжение питающей сети должно быть достаточно стабильным, а уровень помех в ней не должен превышать предельно допустимой величины.

Работы по обслуживанию программного обеспечения АРМ фиксируются в специальном журнале, хранящемся на ПЦО.

Контроль ошибок

Просмотреть лог-файлы оборудования за последний период (1неделя÷1месяц) на наличие ошибок и сбоев в работе. С помощью тестовых программ (PC Wizard , Chekit , Sisoftware Sandra, Everest) просмотреть состояние и загрузку центрального процессора, состояние физических и логических интерфейсов.

Обновление ПО

Обновление ПО оборудования позволяет устранять возможные ошибки и недостатки в работе сетевых устройств, расширять их функционал, добавлять новые возможности. Появление новых версий ПО целесообразно отслеживать на сайте производителя.

Перед установкой на АРМ новой версии ПО необходимо обеспечить копирование дистрибутива

эксплуатирующейся версии и текущей базы данных на внешний носитель с включением сопроводительного файла, содержащего номер версии копируемого автоматизированного рабочего места, даты, времени, а также должности и Ф.И.О. исполнителя работ. По окончании копирования в обязательном порядке проводится контрольная проверка целостности дистрибутива. Кроме того, через службу технической поддержки предприятия-изготовителя или иные источники информации целесообразно убедиться в совместимости обновленной версии ПО со всей номенклатурой оконечного оборудования СПИ, функционирующего на охраняемых объектах, а также возможных особенностях ее установки. Скаченное с сайта производителя ПО, целесообразно хранить в специально созданном архиве.

Обновление (замену) ПО целесообразно проводить с использованием ПК АРМ из «горячего» резерва на время переустановки.

Для оперативной замены вышедших из строя АРМ ПЦО разрабатывается пошаговый алгоритм действий.

Резервное копирование системы

Один из основных этапов профилактического обслуживания — резервное копирование системы. Эта операция позволяет восстановить работоспособность системы при фатальном аппаратном сбое. Для резервного копирования необходимо приобрести устройство хранения информации большой ёмкости (D-Link DNS-320L 2×HDD 3.5”).

База данных ПЦО копируется (архивируется) на внешний носитель либо другой компьютер не реже одного раза в месяц.

Чистка

Один из наиболее важных элементов профилактического обслуживания — регулярные и тщательные чистки. Пыль на компонентах ЛВС, влияет:

- на охлаждения компонентов ЛВС, так как является теплоизолятором;
- на возникновение утечек и коротких замыканий между электрическими цепями из-за наличия в пыли проводящих частиц;
- на окисление контактов, приводящее к нарушениям электрических соединений, из-за некоторых веществ, содержащихся в пыли.

Внешним осмотром оценить состояние корпуса оборудования, крепежа и кабелей. Подготовить средства уборки: ветошь, чистящий состав, пылесос, щетку. Отключить электропитание. С помощью щетки, ветоши и чистящего состава очистить внешние поверхности. Пылесосом удалить пыль из вентиляционных отверстий. Снять верхнюю крышку, с помощью пылесоса очистить внутренние поверхности. Закрыть крышку, восстановить крепеж. Включить электропитание. После загрузки проверить функционирование.

Установка микросхем на свои места

При профилактическом обслуживании очень важно устранить последствия термических смещений микросхем, установленные в гнездах. Поскольку компоненты ЛВС при включении и выключении нагреваются и остывают (следовательно, расширяются и сжимаются), микросхемы, установленные в гнездах, постепенно из них "выползают". Необходимо найти все микросхемы, не установленные в гнездах, и поставить их на место.

Чистка контактов разъемов

Для того, чтобы соединения между узлами и компонентами системы были надежными нужно протирать ветошью контакты разъемов. Следует обратить внимание на наличие следов коррозии на разъемах расширения компьютера, электропитания, подключения сетевых кабелей. На платах сетевых адаптеров протереть печатные разъемы, вставляемые в слоты на системной плате, и все остальные разъемы (например, установленные на внешней панели адаптера).

Серьезную угрозу для компонентов ЛВС представляют статическое электричество. Наиболее опасно оно зимой, при низкой влажности воздуха, а также в районах с сухим климатом. В этих условиях при работе с компьютером необходимо принять специальные меры предосторожности:

- ЛВС должна быть заземлена;
- помещения должны быть по возможности оборудованы увлажнителями воздуха;
- технический персонал должен производить чистку оборудования в заземленном браслете. При отсутствии браслета, оператору необходимо всякий раз перед чисткой контактов оборудования касаться заземления.

Электростатические явления вне корпуса компонентов ЛВС редко приводят к серьезным последствиям, но на шасси, клавиатуре или просто рядом с коммутатором или компьютером сильный разряд может привести к ошибкам при проверке четности (в памяти ОЗУ) или зависанию компьютера.

Контроль температуры помещения

Колебания температуры неблагоприятно сказываются на состоянии компонентов ЛВС. Для надежной ра-

боты компонентов ЛВС температура в помещении ПЦО должна быть постоянной в диапазоне: от +15 до +32°С.

8.2 Нормы трудозатрат по техническому обслуживанию оборудования ЛВС ПЦО.

Техническое обслуживание ТСО проводится на плановой основе в соответствии с требованиями нормативных правовых актов МВД России и эксплуатационной документацией заводов-изготовителей.

При производстве работ по техническому обслуживанию устройств ЛВС ПЦО следует соблюдать «Правила устройства электроустановок (ПУЭ). Седьмое издание. Дата введения 01.01.03.»", "Руководством по техническому обслуживанию установок охранно-пожарной сигнализации", "Типовыми правилами технического содержания установок пожарной автоматики ВСН 25-09.68.85".

Техническое обслуживание устройств ЛВС ПЦО проводится в объеме регламентов №1 (Р1) и №2 (Р2) в соответствии с Рекомендациями «Содержание основных работ по регламентному техническому обслуживанию проводных и радиоканальных СПИ, рекомендованных для применения в подразделениях вневедомственной охраны Р78.36.025-2012».

Объем выполненных регламентных работ устройств ЛВС ПЦО контролируется ИТР ПЦО, фиксируется в журнале электромонтера ПЦО с последующей отметкой дежурного пульта управления в контрольном листе (журнале) устройств ЛВС ПЦО.

Общий для всех устройств ЛВС ПЦО объём работ по техническому обслуживанию приведён в таблице 8.2.1.

Таблица 8.2.1

Работы	Р 1	Р 2
Проверка целостности проводки, надёжности подсоединения разъемов	+	+
Чистка поверхности коммутационного оборудования от пыли, грязи, влаги, устранение механических повреждений	+	+
Проверка исправности органов управления	+	+
Контроль ошибок		+
Обновление системного ПО		+
Резервное копирование системы		+
Установка микросхем на свои места		+

Нормы трудозатрат по техническому обслуживанию оборудования ЛВС ПЦО силами инженерно-технического состава ПЦО приведены в таблице 8.2.2.

Таблица 8.2.2

Наименование оборудования ЛВС	Норма трудозатрат (1 чел. час)	
	Р1	Р2
Согласующие терминаторы (Устройства сопряжения, блоки сопряжения, модемы, модули управления, репиторы)	0.1	1.5
Сетевые адаптеры	0.25	0.5
Трансиверы (приемопередатчики)	2.25	3.25
Концентраторы	0.1	0.25
Мосты	0.1	0.25
Маршрутизаторы	0.5	3.0
Коммутаторы	0.5	3.0
Шлюзы	0.5	3.0

Примечание:

1. В таблице представлены ориентировочные нормы трудозатрат. Цифры необходимо уточнить в соответствии с «Руководством по эксплуатации» на конкретную модель оборудования или определить с учетом трудозатрат на обслуживание аналогичного по функциональному назначению оборудования СПИ/РСПИ в соответствии с Рекомендациями «Содержание основных работ по регламентному техническому обслуживанию проводных и радиоканальных СПИ, рекомендованных для применения в подразделениях вневедомственной охраны Р78.36.025-2012».

2. При необходимости привлечения дополнительных специалистов для выполнения технического обслуживания и ремонта ЛВС ПЦО норма часов распределяется на их количество.

8.3 Устранение неисправностей ЛВС ПЦО

8.3.1 Аппаратура для поиска неисправностей и тестирования ЛВС ПЦО.

Для диагностики, поиска неисправностей кабельных систем используются:

- кабельные сканеры;
- тестеры (мультиметры);
- визуализаторы (для ВОЛС).

Кабельные сканеры позволяют определить длину кабеля, затухание, импеданс, схему разводки, уровень электрических шумов и оценить полученные результаты (Рисунок. 8.3.1.1.) Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания и т.д.) используется метод кабельного радара, или Time Domain Reflectometry (TDR). Суть эго состоит в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки отраженного сигнала. По полярности отраженного импульса определяется характер повре-

ждения кабеля (короткое замыкание или обрыв). По времени задержки отраженного сигнала – местоположение повреждения. В правильно установленном и подключенном кабеле отраженный импульс отсутствует.

Рисунок. 8.3.1.1. Внешний вид кабельного сканера Fluke DTX 1800 .

Тестеры (омметры) - наиболее простые и дешевые приборы для диагностики кабеля. Они позволяют определить целостность кабеля, однако, в отличие от кабельных сканеров, не определяют местоположение повреждения. Проверка целостности линий связи выполняется путем последовательной «прозвонки» витых пар с помощью омметра.

Визуализаторы (для ВОЛС).

Самая распространенная задача при эксплуатации — коммутационные работы, для выполнения которых выпускается целый ряд простых и недорогих приборов.

Визуализатор применяется для:

- обнаружения неисправностей на небольшой дистанции (до нескольких сотен метров): обрывов и изгибов малого радиуса в многомодовых коммутационных шнурах и кабелях, изгибов малого радиуса в одномодовых кабелях;

- контроля их целостности и идентификации кабельных окончаний;

- просветки волоконно-оптических линий (до 5 км на одномодовых и до 2 км на многомодовых).

Визуализатор производится в нескольких вариантах. Самые удобные из них — «фонарик» (Рисунок. 8.3.1.2) и «брелок» (Рисунок 8.3.1.3). Сам прибор содержит источник излучения красного цвета (длина волны около 650 нм) и элементы питания.

Рисунок 12: Фонарик, специально созданный для использования в волоконно-оптических кабельных системах.

Рисунок 8.3.1.2. Визуализатор «Фонарик»

Фонарики, специально предназначены для использования в компьютерных сетях, оснащены разными типами адаптеров: SC, ST и другие. В таких фонариках пучок света сфокусирован лучше, чем в обычных фонарях, а цвет света используется довольно яркий и красный. В них не применяются лампы накаливания, и лазеры.

Рисунок 8.3.1.3. Визуализатор «Брелок».

Детектор излучения на основе изгибного ответвителя.

Детектор излучения на основе изгибного ответвителя (Рисунок 8.3.1.4) позволяет определить наличие излучения в волокне и его направление, а также оценить его мощность без нарушения связи и выполнения коммутаций.

Рисунок 8.3.1.4. Детектор излучения на основе изгибного ответвителя

Оптическое волокно вкладывается в паз ответвителя и изгибается с определенным радиусом. Вышедшее наружу из-за нарушения условий распространения излучение фиксируется и обрабатывается. Детекторы излучения рассматриваемого вида могут иметь не только световой, но и звуковой индикатор. Некоторые модели рассчитаны на использование вместе с источником тестовых сигналов в виде модулированного некоторой частотой излучения; в них встроен детектор для определения наличия и значения частоты

модуляции. Такая пара незаменима для идентификации оптических кабелей и их окончаний.

Визуальные дефектоскопы.

Визуальные дефектоскопы (Visual Fault Locator) (Рисунок 8.3.1.5.) представляют собой источники оптического сигнала видимого диапазона 400-700 нм, которые могут использоваться для визуального обнаружения повреждений в кабелях и интерфейсах, обнаружения неоднородностей и оценки качества сварных швов. Сигнал от визуального дефектоскопа рассеивается на крупных неоднородностях в кабеле, то есть наблюдается оператором в виде светлых пятен (источников рассеяния) через пластиковую оболочку кабеля.

Такой дефектоскоп - это простой хорошо видимый источник красного света в непрерывном или импульсном режиме, подключенный в оптическую линию. Дефектоскоп используется для визуального обнаружения повреждений в кабелях и интерфейсах, выявления неоднородностей и оценки качества сварных швов.

Визуальные дефектоскопы часто используются в комплекте с оптическими рефлектометрами, диапазон действий которых ограничен границей мертвой зоны (EDZ). В этом случае визуальный дефектоскоп обеспечивает оценку качества оптического интерфейса и позволяет обнаружить неоднородности в пределах мертвой зоны.

В остальных случаях портативные визуальные дефектоскопы используются как удобный инструмент при монтаже и эксплуатации оптических кабелей.

Обычно в визуальных дефектоскопах используются полупроводниковые лазеры или гелий-неоновые лазерные источники (HeNe). Гелий-неоновые лазеры

мощнее полупроводниковых, однако требуют в 50 раз большей мощности питания и имеют большие габариты. Использование полупроводниковых лазеров позволяет создавать портативные визуальные дефектоскопы. Наиболее часто применяются визуальные дефектоскопы с центральной частотой источника 635, 650 или 670 нм. Максимальная дальность визуальных дефектоскопов - 1,75 км. Чаще всего встречаются лазеры Класса II, работающие на длине волны 650 нм и испускающие красный свет.

FLS-230A

FLS-235B

VFL-670

Рисунок 8.3.1.5. Визуальные дефектоскопы (VFL).

8.3.2 Алгоритм поиска неисправностей в ЛВС ПЦО.

Поиск неисправности в ЛВС ПЦО зависит от характеристик сбоя на ЛВС ПЦО (в дальнейшем - сети.)

Если сбой в сети затрагивает большой участок и ресурсы, используемые совместно, то необходимо последовательно удалять лишние причины, приводящие к сбою, сводя количество факторов сбоя к минимально возможному значению:

- В топологии «шины» подключиться по более короткому участку кабеля;
- Подключить к сети другой, заведомо исправный, сетевой коммутатор или хаб;
- Выключить или отсоединить от сети все рабочие станции, кроме двух. Если они нормально взаимодействуют между собой, попробуйте добавить еще одну, затем еще. Если в какой-то момент связь прерывается, проверить физические элементы канала:
- концевые разъемы на кабеле;
- сам кабель;
- задействованные порты на активном оборудовании (в хабах и коммутаторах).

Если сбой затрагивает отдельную рабочую станцию, то следует:

- поменять на ней сетевую карту;
- переустановить драйверы сетевой карты (при этом нельзя использовать то сетевое программное обеспечение или файлы настроек, которые содержатся на этой рабочей станции, их лучше удалить);
- подключить к имеющемуся кабельному сегменту диагностические устройства. Например, кабельный анализатор (тестер, работающий в частотном диапазоне).

Если с сетевым подключением все в порядке, то надо:

- проверить, не вызывает ли сбой на рабочей станции какое-то одно приложение;

- запустить с того же диска и в той же файловой системе другое приложение;

- сравнить имеющиеся настройки с настройками рядом расположенной рабочей станции, которая функционирует нормально.

- переустановить программное приложения (необходимо использовать свежую копию, а не имеющееся на станции программное обеспечение и файлы настроек).

Если от сбоя пострадал только один пользователь, то необходимо:

- проверить сетевые настройки безопасности и права доступа именно этого пользователя;

- определить изменения в настройках безопасности, повлиявшие на работу этого пользователя, а именно:

1. удалялась ли в сети учетная запись, настройки безопасности которой, служили основой для настроек этого пользователя;

2. удалялся ли этот пользователь из какой-нибудь группы в сети;

3. переносилось ли используемое приложение в сети на другой ресурс или устройство;

4. вносились ли изменения в сценарий регистрации во всей системе или в последовательность регистрации данного пользователя;

- сравнить настройки учетной записи пользователя с учетной записью кого-нибудь еще, кто может

успешно выполнять действия, вызывающие проблему у данного пользователя.

- войти в сеть с соседней рабочей станции, работающей нормально, и выполнить соответствующие действия с нее.

- войти в сеть с проблемной рабочей станции и выполнить ту же задачу на ней.

- внести изменения в соответствующие сценарии регистрации и настройки безопасности.

- заменить сетевое устройство, сетевую карту, кабель или другой компонент физической инфраструктуры

- применить средства программного исправления (patch-файлы);

- переустановить приложение или его компонент;

- вылечить файлы, зараженные вирусом;

Так как проведение вышестоящих действий может вызвать новые сбои, рекомендуется:

- записывать все произведенные ранее действия;

- сохранять копии файлов настроек.

- открыть вторую терминальную сессию на коммутаторе или маршрутизаторе, чтобы с ее помощью набирать команды, необходимые для внесения изменений в настройки, и держать их наготове, а сами изменения производить из первого окна. Это позволит зафиксировать команду, вызвавшую негативные последствия.

Ведение подробных записей позволяет:

- устранять такие же или похожие неисправности;

- готовить отчеты для руководства и пользователей по наиболее частым проблемам и сбоям в сети;

- проводить инструктаж новых пользователей или специалистов отдела ИТ.

Если сбой затрагивает аппаратную часть то:

- неисправный элемент оборудования заменить исправным;
- сбойный порт закрыть или отметить его, как неисправный;
- подключить свободный порт;

Если сбой связан с программным обеспечением то нужно:

- переустановить программное обеспечение, вызывающее проблему;
- удалить разрушенные и потенциально разрушенные файлы ;
- проверить целостность и сохранность всех необходимых файлов, в соответствии с руководством по эксплуатации на данное программное обеспечение ;
- перенастроить сбойное программное обеспечение, удалить учетную запись и завести ее заново;
- проконтролировать работу ЛВС ПЦО и выявить наличие сбоев.

Поиск неисправности в сегменте ЛВС ПЦО с помощью кабельного сканера.

Если кабельный сканер после выполнения Автотеста показал вам сбой, то необходимо:

- проверить правильность настройки Автотеста:
- тип выбранного сегмента;
- тип установленного адаптера
- тип установленного коннектора;
- обновить программное обеспечение, используемое в анализаторе;
- убедиться, что прибор был поверен, аккумуляторы полностью заряжены.

Если тест выдает пограничный результат, отмеченный звездочкой (PASS* или FAIL*), то следует просмотреть подробные результаты теста, чтобы:

- найти причину проблемы;

- устранить ее и затем получить хороший результат при повторном тестировании. Можно запустить диагностические тесты TDR или TDX и просмотреть получившиеся диаграммы – это поможет найти точку сбоя.

Если тест дал "чистый" сбой, а не пограничный результат со звездочкой (*), и при этом ошибок в схеме разводки нет, то нужно:

- воспользоваться функциями глубокой диагностики, имеющимися у кабельного тестера, чтобы выяснить, где кроется причина сбоя: в разъемах на концах, в кабеле или патч-шнурах.

- запустить тесты TDR или TDX и посмотреть диаграммы, которые могут указать место расположения сбоя.

Сбои из-за ошибок в схеме разводки (Wiremap) проводников в вилке RJ45

Ошибки в схеме разводки (обрывы, короткие замыкания и неправильный порядок проводников) определяются в системе с помощью тестов схемы разводки (Wiremap) и длины (Length). Они позволяют выявить неаккуратно заделанные компоненты, проверить непрерывность проводников и найти ошибки в расположении пар. Некоторые сбои, вызванные разделением пар (Split), обнаружить сложнее: для этого требуется тест, проверяющий величину перекрестных наводок в зависимости от расстояния. Таков, например, тест TDX. Он работает по тому же принципу, что

и тест, определяющий расстояние до точки сбоя (измерение длины и тест TDR).

Большинство ошибок в схеме разводки появляется при заделке коммутационного оборудования: либо в гнезде/вилке RJ45, либо в кроссе или на патч-панели. Ошибки на модуле или в вилке RJ45 часто можно идентифицировать визуально, просто проверив порядок цветов на соответствие схемам разводки T568A или T568B. В вилке еще следует проверить, все ли проводники введены в коннектор до упора – иначе при обжиме вилки на некоторых проводниках будет отсутствовать контакт. Проверяя, все ли проводники введены, как следует, заодно взгляните, какой тип зубцов у контактов вилки RJ45. Зубцы в вилках для одножильного кабеля (кабель с полнотелой жилой, solid) отличаются от зубцов для многожильного кабеля (stranded), вот только после обжима вилки их не так-то просто разглядеть. Посмотрите Рисунок 8.3.2.1

Рисунок 8.3.2.1 Виды зубцов в вилке RJ45 для многожильного (stranded) и одножильного (solid) кабеля.

Если использована вилка с несоответствующим типом зубцов, то контакт может получиться ненадежным, со временем он может вообще пропасть, несмотря на то, что обычно шнуры используют сразу после изготовления. Вилки RJ45 могут страдать еще и от неравномерного обжима. На Рисунке 8.3.2.2. показаны 4 результата неравномерного обжима. На верхней левой вилке нормально продавлены крайние контакты, но недостаточно дожаты центральные. На верхней правой вилке все с точностью до наоборот, центральные контакты продавлены как следует, а боковые – недостаточно.

На нижних вилках с одной стороны вилки было приложено нормальное усилие обжатия, в то время как с другой стороны давление было недостаточным, имеет место недообжим. Обычно так бывает при использовании дешевых обжимных инструментов, в которых рама сделана из пластика. Он гнется тем сильнее, чем больше приложено усилие. Может быть масса других разновидностей обжимов подобного типа. Например, все контакты могут быть продавлены одинаково, но при этом недостаточно глубоко.

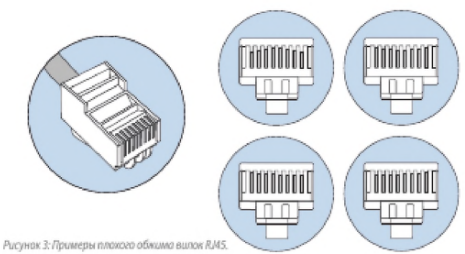


Рисунок 8.3.2.2.

Недостаточный обжим чаще всего происходит тогда, когда не до конца отрабатывает трещотка (храповик) инструмента. В этом случае инструмент позволяет извлечь из него вилку RJ45 до того, как она обжата полностью. Если инструмент поврежден, то один или несколько контактов могут быть вообще не продавлены на свои места. Иногда обжимной инструмент недостаточно прочен или его элементы разболтаны. Это приводит к появлению одной из проблем, показанных на Рисунке 8.3.2.3. Если в вилке RJ45 какие-то контакты недостаточно обжаты, то при подключении ее к гнезду RJ45 соответствующие ламели гнезда могут продавиться слишком глубоко, стать плоскими, и в будущем они просто не достанут до контактов вилки (см. Рисунок 8.3.2.3).

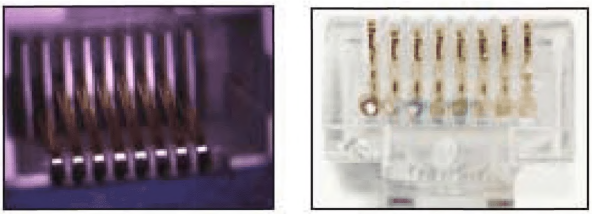


Рисунок 4: Слева показано гнездо RJ45, поврежденное недостаточно обжатой вилкой RJ45. Внешние ламели продавлены и постоянно находятся ниже остальных ламелей. Справа показана вилка RJ45, контакты которой обжаты неравномерно и могут вызывать такие повреждения.

Рисунок 8.3.2.3

Повреждение гнезда, показанное на Рисунке 8.3.2.3, иногда можно устранить, если найти подходящий предмет, тонкий и при этом достаточно прочный, чтобы выправить продавленные ламели и поставить

их вровень с остальными, неповрежденными ламелями. Пробуя выправить продавленную ламель, не спешите и не прилагайте чрезмерных усилий. Помните, что такие действия могут нарушать условия гарантий, которые производители компонентов дают на свою продукцию.

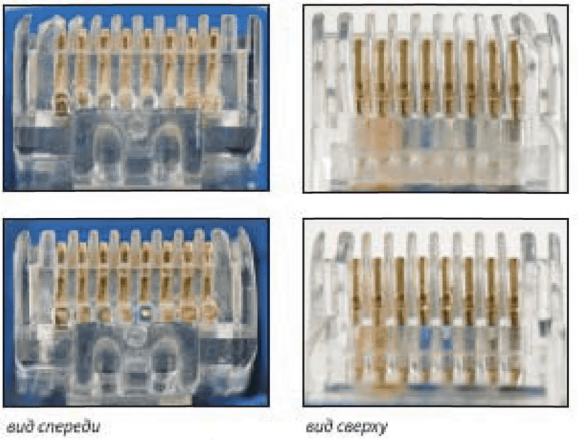


Рисунок 5: Два примера повреждений вилки RJ45, обнаруженных при поиске сбоя.

Рисунок 8.3.2.4

Осмотр пластмассовые элементов вилки RJ45, особенно между металлическими контактами, может выявить деформацию или поломку пластмассовых элементов вилки RJ45. Если они деформированы или поломаны, то пластмассовые фрагменты могут оказаться точно над контактом, и тогда в гнезде не будет соединения с соответствующей ламелью.

На Рисунке 8.3.2.4 на верхних фотографиях видны повреждения на вилках RJ45 пластмассовых разделителей между контактами. С двумя ламелями в гнезде контакта не будет, с третьей контакт маловероятен.

Нижние фотографии вилки RJ45 тоже показывают повреждение пластмассовых деталей: расстояние между разделителями для самого правого контакта слишком мало, и крайняя ламель не сможет его коснуться.

В гнезде RJ45 тоже могут быть повреждения – например, какие-то ламели могут сместиться в сторону, вплоть до возникновения короткого замыкания с соседней ламелью. Рисунок 8.3.2.5

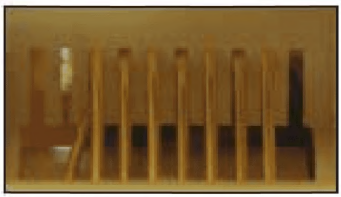


Рисунок 6: Смещение ламели внутри гнезда RJ45.

Рисунок 8.3.2.5

Сбои в сегменте ЛВС ПЦО из-за превышения длины кабеля.

В результате ошибочной установки кабельной системы могут встречаться сегменты длиной более 100 м, максимально разрешенных стандартом. Кабельный сегмент может быть просто слишком длинным из-за установленного запаса в виде нескольких петель или даже небольшой бухты. Сворачивание кабеля в бухту приводит к избыточным перекрестным наводкам, которые непременно скажутся при реализации в системе 1- и 10-гигабитных приложений.

Если длина одной или нескольких пар кабеля существенно отличается от длины остальных пар, то

необходимо проверить промежуточные патч-панели и точки межсоединения: нет ли там провисших или неправильно расшитых пар?

Большинство подобных ошибок появляется именно в промежуточных точках подключения. Значения длины у разных пар всегда должны немного различаться между собой, поскольку шаги повива у пар в кабеле специально делаются разными.

Сбои в сегменте ЛВС ПЦО из-за вносимых помех.

Вносимые помехи, больше известные, как затухание (Attenuation), как правило, зависят от длины кабеля. Потери сигнала растут пропорционально длине кабеля. При получении сбоя по затуханию надо проверить общую длину кабеля. Чрезмерная длина кабеля – самая явная причина сбоя.

Другая причина – это плохое соединение: следствие провисшего под своим весом кабеля, грязных или окислившихся контактов и других подобных факторов. Один плохой патч-шнур в сегменте может привести к сбою всего сегмента.

Чрезмерные переходные помехи, которые чаще всего называют “параметр NEXT”, зарождаются в двух местах: внутри самого кабеля (внутренние наводки) и снаружи (соответственно, внешние наводки). Переходные помехи, возникающие внутри кабеля, сказываются тем сильнее, чем меньше расстояние от передающей пары. Если пара кабеля расплетена больше, чем допускает стандарт – то есть больше 13 мм, то перекрестные наводки становятся очень большими. При возникновении сбоя по перекрестным наводкам следует:

1 Проверить качество монтажа на обоих концах сегмента. Рисунок 8.3.2.6

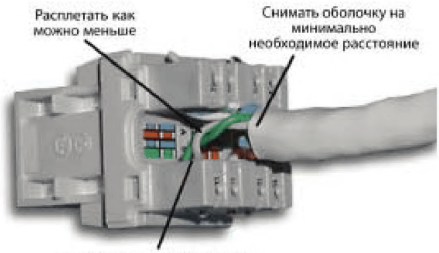


Рисунок 8: Пример правильно выполненного монтажа: пары расплетены на минимальное расстояние, необходимое для заделки.

Рисунок 8.3.2.6

Если разъем содержит расплетенные пары, то их нужно обязательно перезаделать.

2 Вытащить и перезаделать кабель в промежуточных точках подключения (в кроссах). Не следует применять в компьютерных сетях старые кроссы 66-го типа, изначально разработанные для телефонии. При тестировании они показывают плохие параметры не только по переходным помехам. Чтобы соотвествовать требованиям категории 5e, 6 и тем более 6A, следует использовать кроссы 110-го типа или кроссы с более высокими характеристиками. Эта продукция должна быть маркирована, как продукция, пригодная для систем такого уровня.

Прежде чем приступить к перезаделке компонентов для улучшения перекрестных наводок, сначала воспользуйтесь диагностическими средствами. Выполните дополнительные тесты, которые помогут найти причину возникновения перекрестных помех.

Сбои в сегменте ЛВС ПЦО вызванные шумами.

Основные типы шумов:

- Импульсный шум, который чаще всего приводит к появлению в кабеле пиков по напряжению или току.

- Случайный (белый) шум, распределенный по всему спектру частот.

- Внешние переходные помехи (наводки с одного кабеля на пары соседнего кабеля).

Импульсный шум

Из этих трех типов шумов работе сети чаще всего препятствует импульсный шум. Большинство кабельных тестеров имеют встроенные функции для тестирования импульсных шумов. Стандарт 802.3 устанавливает конкретное пороговое значение для импульсных шумов: 264 мВ. Для высокоскоростных сетевых приложений – например, для 1000BASE-T –пороговое значение ниже и составляет 40 мВ. Если таких импульсов за определенный промежуток времени мало (меньше одного импульса за 100 секунд), то приложение будет надежно работать в такой кабельной системе.

Случайный (белый) шум

Источниками импульсного и случайного шума могут быть находящиеся поблизости кабели электропитания или активное оборудование, обычно с высокой нагрузкой по току. К такому оборудованию относятся: большие электродвигатели, лифты и подъемники, фотокопировальная техника, кофе машины, вентиляционное оборудование, нагревательные приборы, электросварочные аппараты, компрессоры и многое другое. Другой, менее очевидный источник шумов – передатчики, испускающие ненаправленное излуче-

ние: телевизионное оборудование, радиопередатчики, микроволновые печи, приемо-передающие станции мобильной связи, носимые радиостанции, системы безопасности здания, авиационное электронное оборудование и любые другие устройства с передающими мощностями выше, чем у обычного мобильного телефона. Некоторые кабельные анализаторы могут рассчитать средний уровень таких шумов и вычесть их из результатов тестирования. Такой тест занимает много времени, поскольку необходимо проводить много дополнительных измерений.

Небольшой уровень шумов мало влияет на передаваемые сигналы в сети и практически не влияет на приёмный сигнал и способность приемных схем в сетевых картах и других активных устройствах определять и правильно распознавать сетевые сигналы. Но если тестер вычленяет усредненные шумы из результатов тестирования, то в реальной работающей сети такие шумы никуда не исчезают и создают серьезные препятствия сетевому трафику.

Необходимо либо найти источник шума и переместить его дальше от кабелей, либо использовать в этой зоне волоконную оптику. Найти источники шумов не так- то просто. Они работают не постоянно, то генерируя шумы, то нет. Для определения частоты и величины шумов необходимо применять спектральный анализатор. Занимаясь поисками источника, нельзя упускать из виду то, что происходит во всей зоне, где проходит кабель. Неожиданное пропадание шумов порой так же полезно для поиска, как и постоянное присутствие шума. В этом случае надо выяснить, что за оборудование использовалось. А какое было только что выключено.

Внешние переходные помехи

Внешние переходные помехи выделены в отдельный тип шума, поскольку их источник – соседние кабели, уложенные в ту же самую кабельную трассу.

Каждый раз, когда тестируется сегмент неэкранированной витой пары UTP в пучке, где несколько кабелей находятся в работе, очень велика вероятность, что тестер обнаружит внешние переходные помехи. В особенности если по этим кабелям передается трафик 100BASE-TX. Тогда прибор сообщит о наличии внешнего шума. Однако для скоростей ниже 10GBASE-T обычно внешние переходные помехи не оказывают заметного влияния на сетевой трафик.

Практически все переходные помехи на дальнем конце возникают в вилке, в гнезде или в результате индуктивной связи одной пары с другой, в то время как практически все переходные помехи на ближнем конце – это следствие емкостной связи по длине кабеля. Тем не менее, устранение сбоев по наводкам на ближнем конце NEXT, как правило, одновременно приводит к устранению большинства проблем с наводками на дальнем конце FEXT. В измерениях эти параметры чаще всего обозначаются как ACR-F или ELFEXT. Так происходит потому, что становятся значимыми только собственные электрические характеристики соединений.

Попробуйте заменить вилку RJ45 на том конце сегмента, где тестер показывает сбой. Если это не помогает, то замените имеющиеся вилку и гнездо на парные вилку и гнездо от одного и того же производителя.

Помехи из-за отражений в линии.

Помехи из-за отражений учитывают все отражения, которые происходят в сегменте по всей его длине по причине несоответствия импедансов. Этот параметр показывает, насколько характеристический импеданс кабельной системы соответствует номинальному полному сопротивлению по всему диапазону частот.

Помехи из-за отражений от коннекторов в сегменте.

Сбои в кабельной среде обнаруживаются и устраняются непосредственно после монтажа кабельной системы, и после некоторого периода эксплуатации. Виды сбоев и их причина показаны в таблице 8.3.2.1.

8.3.3 Поиск и устранение сбоев в волоконно-оптической линии связи

Меры предосторожности

При работе с оптикой следует принимать меры предосторожности. Длины волн, которые используются в оптических сетях, относятся к невидимому диапазону. Человеческий глаз воспринимает излучение от фиолетового цвета (длина волны около 380 нм) до красного (около 750 нм). Рисунок 8.3.3.1. Многие источники, применяемые в оптических сетях, используют лазеры, и некоторые из них имеют очень большую мощность. Никогда не смотрите в торец оптического волокна, в оптический порт или проходник. Если какой-то оптический порт не используется, закройте его специальным колпачком. Эта мера убережет глаза от повреждения невидимым излучением и одновременно защитит оптический разъем от загрязнения.

Таблица 8.3.2.1 Основные виды сбоев кабельных тестов и их причины.

Описание	Обрыв	Короткое замыкание	Разрезанная пара	Перекрещенные пары	Разделенные пары	Сбой по длине	Смещение задержки	Вносимые потери	Наводки NEXT	Возвратные потери	Помехозащищенность ACR-F	Межкабельные наводки
Кабель перекушен, оборван или поврежден иным способом	•	•				•				•		
Повреждена вилка или гнездо RJ45	•	•										
В сегменте использованы обе схемы разводки: T56A и T568B				•								
Для разных пар используется разный материал изоляции							•					
Низкое качество монтажа при разделке кабеля на коннектор			•		•	•		•	•	•		
Неправильный порядок проводников при разделке кабеля на коннектор									•	•		
Соединитель или адаптер RJ45 имеет низкое качество, неправильную разводку или предназначен только для телефонии									•	•		
Низкое качество вилок/гнезд RJ45 или характеристики слишком низкой категории									•	•	•	•
Патч-шнур(ы) плохого качества либо с повреждениями									•	•		
В сегменте используется участок 100-омного кабеля и участок кабеля иного типа										•		
Кабель слишком длинный либо установлено неправильное значение NVP						•		•				
Расплетенные либо плохо сплетенные пары кабеля (включая слишком редкий шаг повива пар, например, в кабелях Категории 5e в сравнении с Категорией 6)									•	•	•	•
По длине кабеля слишком туго затянуты хомуты-стяжки									•	•		
Источник внешнего шума недалеко от кабеля									•		•	•
Кабели лежат слишком плотно друг к другу на среднем или большом протяжении. Удалите хомуты-стяжки и/или расположите кабели более свободно												•

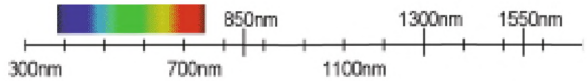


Рисунок 11: Видимый свет находится в области более короткие длин волн (от 380 до 750 нм), чем те, что используются в компьютерных сетях.

Рисунок 8.3.3.1

Если вам необходимо визуально идентифицировать порт и вы используете источник видимого света, то самый безопасный способ – направить конец оптического кабеля на лист белой бумаги либо поднести лист бумаги к месту оптического подключения. Никогда не смотрите прямо в коннектор – всегда есть риск, что из него исходит невидимое излучение.

В соответствии с правилами техники безопасности все работы по тестированию следует выполнять в защитных очках, поскольку они оберегают глаза от типичного для оптических линий излучения. Рисунок 8.3.3.2

Рисунок 8.3.3.2

Тестирование непрерывности

Для проверки непрерывности оптического сегмента и полярности парных оптических волокон при-

меняются устройства, использующие видимый свет. Большинство таких устройств представляют собой фонарики, испускающие белый свет или другие цвета.

Если в оптическом кабеле волокно повреждено или разбито, то при использовании визуального определителя дефектов VFL можно заметить это место визуально. Свет будет проникать наружу в тех местах, где в оболочке волокна в результате перегиба, разрыва или плохой сварки имеется участок повышенного рассеяния. Однако так происходит не со всеми типами кабеля. В некоторых кабелях из-за определенного типа и количества оболочек свет снаружи не виден.

Поскольку наблюдать за ним иногда приходится при ярком свете, в некоторых приборах оно модулируется низкой частотой (около 1 Гц) для улучшения видимости. На кабеле будут видны постоянные или мерцающие красные пятна.

Определение места и характера повреждения оптоволоконного кабеля

Алгоритм поиска неисправности в ВОЛС приведён на рисунке .8.3.3.3

Первой задачей поиска неисправности в ВОЛС является анализ, относится ли неисправность к электрической части оборудования или к оптической. Для этого с помощью оптического измерителя мощности (Optical Power Meter, далее – OPM) измеряется уровень оптической мощности и затем производится сравнение с нормативным значением. Если уровень оптической мощности находится в пределах нормы, неисправность находится в электронной части аппаратуры передачи, которая нуждается в замене или ремонте.

Рисунок 8.3.3.3 Алгоритм поиска неисправности в ВОЛС

Если уровень принимаемой мощности слишком низкий, неисправность находится либо в передатчике, либо в волоконно-оптическом кабеле. Для дальнейшего поиска необходимо измерение выходной мощности передатчика, для этого используются ОРМ и тестовый кабель. Если выходная мощность передатчика низкая, он должен быть отремонтирован. Если мощность находится в пределах нормы, неисправность связана с волоконным кабелем.

Поиск неисправности в кабеле начинается с анализа его неоднородности с использованием визуального дефектоскопа в случае кабелей малой протяженности или оптического рефлектометра OTDR (Optical Time Domain Reflectometer) - в случае протяженных кабелей. Основными неисправностями кабеля обычно являются коннекторы, сварки с плохим качеством, соединения и обрывы кабеля, обусловленные внешними воздействиями. Для поиска неисправности в коннекторах применяются эксплуатационные микроскопы. Для диагностики сварок и локализации обрывов применяются OTDR.

Основные виды неисправностей в ВОЛС приведены в таблице 8.3.3.1.

Таблица 8.3.3.1. Основные виды неисправностей в ВОЛС

Неисправность	**Причина**	**Оборудование диагностики**	**Процедура устранения**
Коннектор	Пыль или загрязнение	Микроскоп	Очищение, полировка, обновление

Неисправность	Причина	Оборудование диагностики	Процедура устранения
Кабель pig-tail	Перекручивание кабеля	Визуальный дефектоскоп	Устранение перекручивания
Локальный всплеск затухания в кабеле	Перекручивание кабеля	OTDR	Устранение перекручивания
Распределенное увеличение затухания в кабеле	Некачественный кабель	OTDR	Замена участка кабеля
Потери в сварочном узле	Некачественная сварка Потери, связанные с близким расположением волокон в сварочном узле	OTDR Визуальный дефектоскоп	Вскрытие узла и проведение сварки заново
Обрыв кабеля	Внешние воздействия	OTDR, визуальный дефектоскоп	Ремонт/замена

8.3.4 Программные средства для поиска неисправностей в ЛВС ПЦО.

Для поиска неисправности в сети используют встроенные средства тестирования (утилиты) операционной системы Windows. Сетевые команды диагностики сети TCP/IP являются первичным программным инструментом для обнаружения причин сбоев в рабо-

те сети. Для запуска утилит необходимо открыть окно DOS, которое открывается следующим образом:

Кнопка Пуск→Все программы→Стандартные→Командная строка

Проверка сетевого имени компьютера с помощью утилиты hostname.

Кнопка Пуск→Все программы→Стандартные→Командная строка→ **hostname.** →Кнопка Ввод**.**

На экран будет выведено сетевое имя компьютера. Рисунок.8.3.4.1

```
D:\Documents and Settings\Skalozubov.NIC>hostname
skalozubov
```

Рисунок.8.3.4.1. Вывод сетевого имени компьютера.

Данная утилита определяет правильность сетевых настроек компьютера.

Проверка определения основных параметров, задающих подключение компьютера в сеть с помощью утилиты ipconfig

Кнопка Пуск→Все программы→Стандартные→Командная строка→ **ipconfig** →Кнопка Ввод**.**

Утилита **Ipconfig** показывает текущую конфигурацию TCP/IP на локальном компьютере. На экран будет выведено следующее сообщение, показанное на рисунке. 8.3.4.2.:

```
D:\Documents and Settings\Skalozubov.NIC>ipconfig

Настройка протокола IP для Windows


Подключение по локальной сети - Ethernet адаптер:

        DNS-суффикс этого подключения . . : NIC
        IP-адрес  . . . . . . . . . . . . : 192.168.0.116
        Маска подсети . . . . . . . . . . : 255.255.254.0
        IP-адрес  . . . . . . . . . . . . : fe80::280:48ff:fe16:f5bd%4
        Основной шлюз . . . . . . . . . . :

Teredo Tunneling Pseudo-Interface - туннельный адаптер:

        DNS-суффикс этого подключения . . :
        IP-адрес  . . . . . . . . . . . . : fe80::ffff:ffff:fffd%5
        Основной шлюз . . . . . . . . . . :

Automatic Tunneling Pseudo-Interface - туннельный адаптер:

        DNS-суффикс этого подключения . . : NIC
        IP-адрес  . . . . . . . . . . . . : fe80::5efe:192.168.0.116%2
        Основной шлюз . . . . . . . . . . :
```

Рисунок. 8.3.4.2. Вывод текущей конфигурации TCP/IP на локальном компьютере.

Данная утилита позволяет определить четыре основных параметра настройки протокола TCP/IP: DNS суффикс, IP-адрес, маску подсети и основной шлюз. Приведенный вызов утилиты **ipconfig** позволяет определить только лишь самые важные параметры подключения.

При необходимости получить значения других параметров, определяющих данное подключение, используется вызов утилиты **ipconfig** с ключом **/all**.

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **ipconfig/all**. →Кнопка Ввод

На экран будут выведены все действующие параметры протокола.

Если утилита покажет, что сетевому адаптеру присвоен адрес 169.254.134.123 (или аналогичный), то можно сделать заключение, что в сети недоступен сервер, автоматически присваивающий параметры IP-протокола (DCHP). Часто причиной подобной ошибки (если ранее компьютер нормально работал в сети) является нарушение контакта в подсоединении сетевого кабеля.

Проверка достижимости ближайших компьютеров сети с компьютером рабочей станции с помощью утилиты ping.

Ping - диагностическая утилита, которая проверяет возможность соединения с удаленным компьютером, задав в качестве параметра утилиты IP-адрес компьютера или его имя.

Эта команда посылает на заданный компьютер последовательность символов определенной длины и выводит на экран информацию о времени ответа удаленной системы. Ключами команды можно регулировать количество отсылаемых символов и время ожидания ответа (через этот период выводится сообщение о превышении периода ожидания; если ответ придет позже, то он не будет показан программой). При тестировании подключения рекомендуется применять следующую последовательность операций:

1. Проверить правильность установки стека TCP/IP на собственном компьютере с помощью утилиты, указав ей в качестве IP-адреса зарезервированный специальный IP-адрес 127.0.0.1, всегда указывающий на тот же самый компьютер, с которого запускается утилита.

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **ping 127.0.0.1**→Кнопка Ввод. На экран будет выведено сообщение: рисунок 8.3.4.3

```
D:\Documents and Settings\Skalozubov.NIC>ping 127.0.0.1

Обмен пакетами с 127.0.0.1 по 32 байт:

Ответ от 127.0.0.1: число байт=32 время<1мс TTL=64
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=64
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=64
Ответ от 127.0.0.1: число байт=32 время<1мс TTL=64

Статистика Ping для 127.0.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 8.3.4.3. Обмен пакетами с собственным компьютером.

Эта команда проверяет прохождение сигнала "на самого себя". Она может быть выполнена без наличия какого-либо сетевого подключения.

Если будет показано сообщение о недостижимости адресата, то это означает ошибку установки протокола IP. В этом случае целесообразно удалить протокол из системы, перезагрузить компьютер и вновь установить поддержку протокола TCP/IP.

2. Проверить ответ локального компьютера, которому присвоили конкретный IP-адрес. Например, **192.168.0.11**. Для этого следует выполнить:

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **ping 192.168.0.11**→Кнопка Ввод.

Результат, который должен быть выведен на экран в случае нормальной работы, практически аналогичен полученному результату в предыдущем примере: рисунок 8.3.4.4.

```
D:\Documents and Settings\Skalozubov.NIC>ping 192.168.0.11

Обмен пакетами с 192.168.0.11 по 32 байт:

Ответ от 192.168.0.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.11: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.11: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 8.3.4.4. Обмен пакетами с локальным компьютером 192.168.0.11.

Наличие отклика от локального компьютера свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса

3. Проверить выполнение команды ping с указанием IP-адреса любого ближайшего компьютера. Можно использовать любой адрес, относительно которого вы уверены, что он достижим в локальной сети на момент проверки. Например, можно записать IP-адрес шлюза или адрес DNS-сервера. Наличие отклика свидетельствует, что канал связи установлен и работает. Отсутствие ответа обычно говорит либо о повреждении кабельной сети (например, нет контакта в разъеме), либо о неверно установленных параметрах статического адреса.

Проверка функционирования серверов имен. (DNS-серверов)

Для проверки работоспособности сервера имен следует выполнить команду **ping**, указав в качестве параметра не IP-адрес, а доменное имя какого-либо компьютера: **ping <имя>** Например, **servernic.**

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **ping servernic**→Кнопка Ввод**.** На экран будет выведено сообщение: рисунок 8.3.4.5.

```
D:\Documents and Settings\Skalozubov.NIC>ping servernic

Обмен пакетами с servernic [192.168.0.1] по 32 байт:

Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Рисунок 8.3.4.5. Проверка работоспособности сервера имен.

Если команда сможет "разрешить" IP-адрес хоста и покажет отклик, то это означает работоспособность системы распознавания имен. Практически это говорит о правильной настройке протокола TCP/IP и работоспособности канала связи. Если не будет ответа на ввод команды с именем существующего хоста, то это может свидетельствовать либо об ошибке в задании DNS-серверов, либо об их неработоспособности.

Проверка определения компьютеров в сети.

Для определения компьютеров в сети используют команду **net view**.

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **net view**→Кнопка Ввод**.** На экран будет выведено сообщение: рисунок 8.3.4.6.

```
D:\Documents and Settings\Skalozubov.NIC>net view
Имя сервера             Заметки

-------------------------------------------------
\\AMOROZ
\\ANYUHIN
\\BALUEVA
\\BARINOV_INET          Stend_busy_line
\\BATMAN-ПК
\\BELAN
\\BOBROVA
\\BODJAGINA
\\BORISOV               K603
\\CAPLINA
\\CTECKIY
\\DEMIN
\\FAMILNOV
\\FEDIN
\\GENERALOV-POWER
\\GOLUBKOV
\\GOLUBYH
\\GURASHOFF             ROMAN
\\GUSEVA
\\GUSKOV
\\HARAPONOVA-PC
\\HOLOSTOVA
\\IMOROZ
\\INET_MOROZ
```

Рисунок 8.3.4.6. Список компьютеров, функционирующих в сети.

На подключенных, но не функционирующих компьютерах в сети потребуется проверить правильность установки стека TCP/IP , исправность сетевого адаптера или наличие контакта в подсоединении сетевого кабеля к сетевому адаптеру.

Проверка качества канала связи

При работе в Интернете одни информационные серверы открываются быстрее, другие медленнее, бывают случаи недостижимости желаемого хоста. Часто причиной этого бывает недостаточное качество канала связи: большое время ожидания данных или существенный процент потерь пакетов, что обычно приводит к повторам передачи.

С помощью утилит **tracert и pathping** можно оценить качество канала связи по всей цепочке до желаемого источника. Например сайт **nicohrana.ru. или (IP 195.146.67.105)**

Кнопка Пуск→Все программы→Стандартные→Командная строка→ **tracert 195.146.67.105**→Кнопка Ввод. На экран будет выведено сообщение: рисунок 8.3.4.7.

```
D:\Documents and Settings\Skalozubov.NIC>tracert 195.146.67.105

Трассировка маршрута к 195.146.67.105 с максимальным числом прыжков 30

  1  Заданный узел недоступен.

Трассировка завершена.
```

Рисунок 8.3.4.7 . Трассировка к сайту nicohrana.ru.

В данном случае маршрутизатор блокирует доступ к сайту Интернету. Он или неисправен или не настроен.

Трассировка к сайту **nicohrana.ru.** с компьютера, имеющего доступ к сайту Интернета. На экран будет выведено сообщение: рисунок 8.3.4.8.

```
C:\Users\Helgi>tracert nicohrana.ru

Трассировка маршрута к nicohrana.ru [195.146.67.105]
с максимальным числом прыжков 30:

  1     2 ms     1 ms     3 ms  n003-000-000-000.static.ge.com [3.3.3.3]
  2     2 ms     1 ms     1 ms  n003-000-000-000.static.ge.com [3.3.3.3]
  3     1 ms     1 ms     1 ms  10.244.14.34
  4     2 ms     1 ms     2 ms  83.167.99.104
  5     1 ms     2 ms     1 ms  213.171.37.97
  6     5 ms     4 ms     3 ms  iki-crs.comcor.ru [62.117.100.73]
  7     5 ms     5 ms     3 ms  212.45.12.218
  8     7 ms     3 ms     4 ms  m9-crs-1-be6.msk.stream-internet.net [195.34.59.
241]
  9     3 ms     4 ms     3 ms  212.188.42.106
 10     3 ms     4 ms     3 ms  212.188.12.246
 11     3 ms     3 ms     7 ms  ihome.ihome.ru [85.112.127.226]
 12     4 ms     3 ms     3 ms  sis.ihome.ru [85.112.114.38]
 13     3 ms     4 ms     3 ms  n253-183.sserv.ru [95.215.183.253]
 14     4 ms     5 ms     4 ms  195.146.65.24
 15     5 ms     5 ms     6 ms  n237-87.relline.ru [195.146.87.237]
 16     4 ms     6 ms     4 ms  hosting.icomisp.ru [195.146.67.105]

Трассировка завершена.
```

Рисунок 8.3.4.8. Трассировка к сайту nicohrana.ru.

Утилита **tracert** выводит на экран время отклика каждой системы, находящейся на пути передачи данных к искомому серверу. Точка, после которой время отклика резко увеличено, свидетельствует о наличии в этом месте узкого "горлышка", не справляющегося с нагрузкой.

Более точную усредненную статистику достижимости удаленного хоста можно получить с помощью команды **pathping.** Утилита **pathping** объединила в себе **ping** и **traceroute.** Она отражает маршрут про-

хождения и предоставляет статистику потери пакетов на промежуточных маршрутизаторах.

Кнопка Пуск→Все программы→Стандартные→ Командная строка→**pathping nicohrana.ru** →Кнопка Ввод.

На экран будет выведено сообщение: рисунок 8.3.4.9.

```
C:\Users\Helgi>pathping nicohrana.ru

Трассировка маршрута к nicohrana.ru [195.146.67.105]
с максимальным числом прыжков 30:
  0  HOME [192.168.1.101]
  1  n003-000-000-000.static.ge.com [3.3.3.3]
  2  n003-000-000-000.static.ge.com [3.3.3.3]
  3  10.244.14.34
  4  83.167.99.104
  5  213.171.37.97
  6  iki-crs.comcor.ru [62.117.100.73]
  7  212.45.12.218
  8  m9-crs-1-be6.msk.stream-internet.net [195.34.59.241]
  9  212.188.42.106
 10  212.188.12.246
 11  ihome.ihome.ru [85.112.127.226]
 12  sis.ihome.ru [85.112.114.38]
 13  n253-183.sserv.ru [95.215.183.253]
 14  195.146.65.24
 15  n237-87.relline.ru [195.146.87.237]
 16  hosting.icomisp.ru [195.146.67.105]

Подсчет статистики за: 400 сек. ...
           Исходный узел     Маршрутный узел
Прыжок  RTT    Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                            HOME [192.168.1.101]
                                 0/ 100 =  0%   |
  1    5мс     0/ 100 =  0%     0/ 100 =  0%  n003-000-000-000.static.ge.com [3.
3.3.3]
                                 0/ 100 =  0%   |
  2    3мс     0/ 100 =  0%     0/ 100 =  0%  n003-000-000-000.static.ge.com [3.
3.3.3]
                                 0/ 100 =  0%   |
  3  ---     100/ 100 =100%   100/ 100 =100%  10.244.14.34
                                 0/ 100 =  0%   |
  4  ---     100/ 100 =100%   100/ 100 =100%  83.167.99.104
                                 0/ 100 =  0%   |
  5  ---     100/ 100 =100%   100/ 100 =100%  213.171.37.97
                                 0/ 100 =  0%   |
  6    6мс     0/ 100 =  0%     0/ 100 =  0%  iki-crs.comcor.ru [62.117.100.73]

                                 0/ 100 =  0%   |
  7   12мс     0/ 100 =  0%     0/ 100 =  0%  212.45.12.218
                                 0/ 100 =  0%   |
  8    7мс     0/ 100 =  0%     0/ 100 =  0%  m9-crs-1-be6.msk.stream-internet.n
```

Рисунок 8.3.4.9. Трассировка к сайту nicohrana.ru.

Утилита **pathping** посылает на каждый промежуточный хост серию пакетов и выводит информацию о количестве откликов и среднем времени ответа.

После опубликования цепочки хостов, через которые проходит сигнал по пути к заданному серверу, программа **pathping** выводит статистические данные о достижимости каждого промежуточного хоста, причем время усреднения выбирается исходя из конкретной ситуации. Первым параметром выводится время доступа к данному хосту, затем показано количество отправленных на него пакетов и число неполученных ответов (с процентом успеха). После этого отображаются аналогичные значения для достижимости конечного хоста при расчете прохождения пакетов от данной промежуточной точки. В завершение после имени данного промежуточного хоста утилита сообщила количество успешных пакетов.

Праверка текущей информации сетевого соединения TCP/IP с помощью утилиты Netstat.

Для определения параметров сетевого подключения компьютера используется утилита **Netstat**

Кнопка Пуск→Все программы→Стандартные →Командная строка→ **Netstat** →Кнопка Ввод

На экран будет выведено сообщение: рисунок 8.3.4.10.

```
D:\Documents and Settings\Skalozubov.NIC>Netstat

Активные подключения

  Имя     Локальный адрес        Внешний адрес          Состояние
  TCP     skalozubov:1866        localhost:12882        TIME_WAIT
  TCP     skalozubov:1581        192.168.0.40:netbios-ssn  ESTABLISHED
```

Рисунок 8.3.4.10. Вывод информации об активных TCP соединениях, используемых портов.

Приложение А

Стандартные сегменты Ethernet и Fast Ethernet

А.1 Аппаратура 10BASE5

Толстый кабель - это первый, классический тип кабеля, который использовался в Ethernet с самого начала. В настоящее время он не очень широко распространен, хотя и обеспечивает максимальную протяженность сети с топологией «шина».

Толстый коаксиальный кабель представляет собой 50-омный кабель диаметром около 1 см и отличается высокой жесткостью. Он имеет два основных типа оболочки: стандартная PVC желтого цвета и тефлоновая Teflon оранжево-коричневого цвета. Широко распространены толстые кабели типа RG-11 и RG-58. У толстого кабеля лучше помехоустойчивость, меньше затухание и выше механическая прочность.

По стандарту к одному сегменту (длиной до 500 метров) не должно подключаться более 100 абонентов. Расстояния между точками их подключения не должно быть меньше, чем 2,5 метра, иначе возникают искажения передаваемых сигналов. Поэтому для удобства пользователя на оболочку кабеля часто наносятся черные полоски как раз через каждые 2,5 метра.

Аппаратные средства 10BASE5 представлены на рис. А.1.1. Они включают в себя кабель, разъемы, терминаторы, трансиверы и трансиверные кабели.

Для соединения кусков толстого коаксиального кабеля и присоединения к нему терминаторов используются разъемы так называемого N-типа, установка

которых довольно сложна и требует специальных инструментов (в противном случае возможны искажения сигналов на стыках). Два разъема N-типа для увеличения длины кабеля могут соединяться с помощью Barrel-коннекторов.

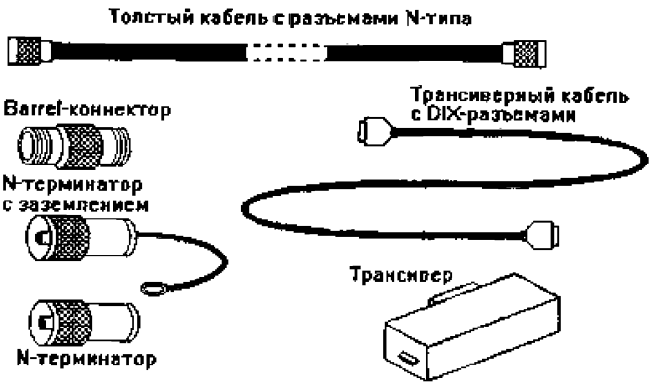


Рис. А.1.1. Аппаратура 10BASE5

На обоих концах кабеля сегмента должны быть установлены 50-омные терминаторы N-типа, один (и только один) из которых надо заземлить.

Толстый кабель никогда не подводят непосредственно к каждому компьютеру сети, это сложно и неудобно для использования, так как компьютеры будут совершенно неподвижны. Его прокладывают по стене или по полу помещения. Для присоединения сетевых адаптеров к толстому кабелю служат специальные трансиверы (см. рис. А.1.2.). Трансивер (он же MAU, Medium Attachment Unit - устройство присоединения к

среде) устанавливается непосредственно на толстом кабеле и связывается с адаптером трансиверным кабелем. Для присоединения трансиверов к толстому кабелю чаще всего используются специальные соединительные устройства, предложенные корпорацией AMP, которые не требуют разрезания кабеля в точке присоединения, а просто прокалывают оболочку и изоляцию кабеля и обеспечивают механическое и электрическое соединение как с оплеткой, так и с центральной жилой кабеля. Другой тип соединителя требует разрезания кабеля и установки на оба конца разъемов, поэтому он гораздо менее популярен.

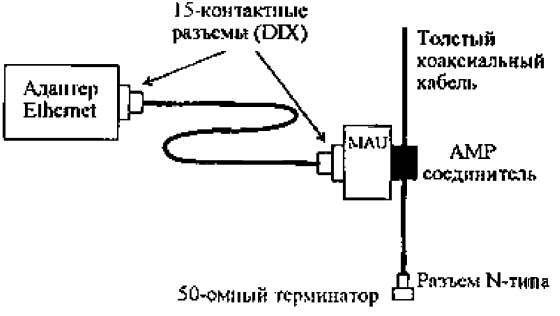


Рис. А.1.2. Подсоединение адаптера к толстому кабелю

Трансиверный кабель представляет собой гибкий многопроводный кабель диаметром около 1 см, содержащий четыре экранированные витые пары. Длина обычного трансиверного кабеля может достигать 50 метров, а более тонкого и гибкого офисного варианта трансиверного кабеля - 12,5 метров, чем

обеспечивается достаточная свобода перемещения компьютеров. На концах трансиверного кабеля устанавливаются 15-контактные разъемы (DIX-разъемы типа «вилка», DB-15P). Трансиверный кабель называется также AUI-кабелем (Attachment Unit Interface) или Drop-кабелем, спусковым кабелем, а его разъемы — AUI-разъемами. Трансивер питается от внутреннего источника питания компьютера.

Сетевой адаптер, работающий с толстым кабелем, должен иметь внешний 15-контактный АШ-разъем (разъем DIX типа «розетка», DB-15S). Гальваническая развязка в данном случае осуществляется внутри трансивера. Напряжение изоляции между абонентами может достигать 5 киловольт.

Схема соединения компьютеров сегмента сети на толстом кабеле показана на рис. А.1.3.

Максимальное количество сегментов при реализации всей сети только на толстом коаксиальном кабеле не должно превышать пяти (общая длина сети - 2,5 км). Потребуется четыре репитера. То есть общее количество компьютеров, подсоединенных к толстому кабелю, в принципе не может превышать пятисот.

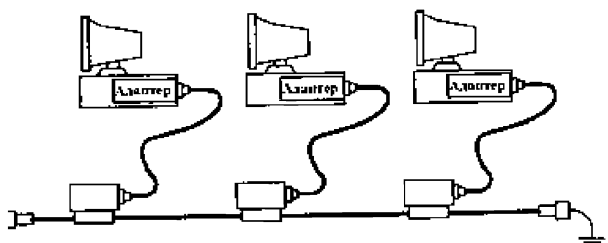


Рис. А.1.3. Соединение компьютеров сети толстым кабелем

А.2 Аппаратура 10BASE2

Тонкий коаксиальный кабель отличается от толстого вдвое меньшей толщиной (диаметр около 5 мм), значительно большей гибкостью, большим удобством монтажа, меньшей стоимостью (примерно в три раза дешевле толстого). Не удивительно, что сети на его основе получили гораздо большее распространение. Тонкий кабель, как и толстый, имеет волновое сопротивление 50 Ом и требует такого же 50-омного оконечного согласования. Если толстый кабель обязательно должен быть надежно закреплен, например, на стене или на полу помещения, то тонкий кабель вполне может быть проложен навесным монтажом, что позволяет довольно просто перемещать компьютеры в пределах помещения.

Самым большим недостатком тонкого кабеля является меньшая допустимая длина сегмента (до 185 м). Иногда, правда, изготовители сетевых адаптеров указывают допустимую длину сегмента 200 м или даже 300 м. В последнем случае может оказаться, что такие сетевые адаптеры не способны связываться с адаптерами других типов, так как используют нестандартные уровни сигналов. Наиболее распространенный тип тонкого коаксиального кабеля - это RG-58 A/U.

Аппаратура для работы с тонким кабелем (рис. А.2.1.) гораздо проще, чем в случае толстого кабеля. Помимо сетевых адаптеров, требуются только кабели соответствующей длины, разъемы, Т-коннекторы и терминаторы (один с заземлением). Между каждой парой абонентов прокладывается отдельный кусок кабеля с двумя байонетными разъемами типа BNC на

концах. Минимальная длина куска кабеля - 0,5 метра. Допускается, хотя и не рекомендуется, соединение кусков кабеля между собой с помощью BNC I-коннекторов (Barrel-коннекторов).

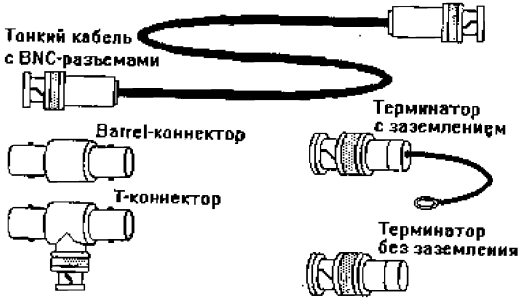


Рис. А.2.1. Аппаратура 10BASE2

На плате адаптера должен находиться BNC-разъем, к которому присоединяется BNC Т-коннектор, соединяющий плату с двумя кусками кабеля (рис. А.2.2.). Гальваническую развязку осуществляет сам адаптер, напряжение изоляции составляет 100 В, что значительно меньше, чем в случае толстого кабеля.

Если вся сеть выполняется на тонком кабеле, (Рис. А.2.3.) то, согласно стандарту, количество сегментов не должно превышать пяти (таким образом, общая длина сети составит 925 м, потребуется четыре репитера). Максимальное количество абонентов на одном сегменте (включая репитеры) не должно быть больше 30, то есть общее число абонентов в сети на базе тонкого кабеля в принципе не может быть больше 150.

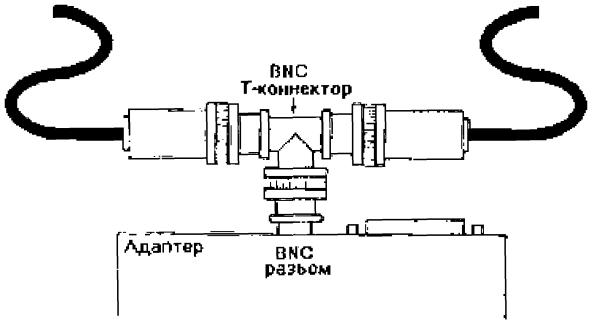


Рис. А.2.2. Присоединение адаптера к тонкому коаксиальному кабелю

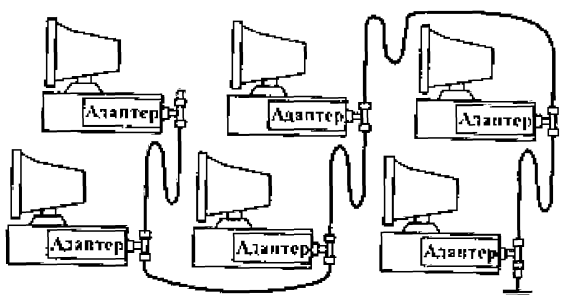


Рис. А.2.3. Соединение компьютеров сети тонким кабелем

А.3 Аппаратура 10BASE-T

Сеть Ethernet на базе витой пары развивается с 1990 года и становится все более популярной. Во многом это объясняется модой, а вовсе не преимуществами витой пары. Ведь оборудование для нее обычно дороже, чем для 10BASE2. Однако 10BASE-T действительно имеет важные достоинства, главное из которых состоит в возможности плавного перехода на Fast Ethernet, чего не могут обеспечить сегменты на коаксиальном кабеле. Повреждение одного из кабелей не ведет к выходу из строя всей сети. Отказы оборудования проще локализовать. К тому же монтаж сети на витой паре проще. Удобно и то, что к каждому компьютеру подходит только один кабель, а не два, как в случае 10BASE2.

В сегменте 10BASE-T передача сигналов осуществляется по двум витым парам проводов, каждая из которых передает только в одну сторону (одна пара - передающая, другая - принимающая). Кабелем, содержащим такие двойные витые пары, каждый из абонентов сети присоединяется к концентратору (хабу), использование которого в данном случае в отличие от рассмотренных ранее обязательно. Концентратор производит смешение сигналов от абонентов для реализации метода доступа CSMA/CD, то есть в данном случае реализуется топология «пассивная звезда» (рис.А.3.1), которая, как уже отмечалось, равноценна топологии «шина».

Длина соединительного кабеля между адаптером и концентратором не должна превышать 100 м. Кабель используется гибкий, диаметром около 6 мм. Из четырех витых пар, входящих в кабель, использу-

ются только две. Наиболее распространенный тип кабеля — это кабель EIA/TIA категории 3. Рекомендуется использовать более качественный кабель категории 5 (или даже выше), который позволяет без проблем переходить на Fast Ethernet.

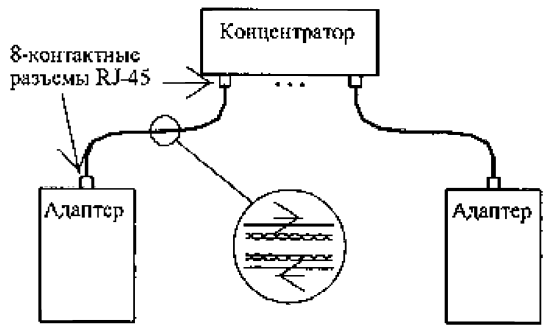


Рис. А.3.1. Подключения абонентов сети с помощью витой пары

Кабели присоединяются к адаптеру и к концентратору 8-контактными разъемами типа RJ-45 (рис. А.3.2.). Назначение контактов разъема приведено в табл. А.3.1.

Монтаж и обслуживание неэкранированных кабелей с витыми парами (UTP-кабелей) гораздо проще, чем коаксиальных кабелей, так как они не имеют металлической оплетки. Что касается стоимости кабеля, то UTP-кабели стоят примерно вдвое дешевле, чем тонкий коаксиальный кабель.

Табл. А.3.1. Назначение контактов разъема RJ-45 сегмента 10BASE-T

Контакт	Назначение	Цвет провода
1	TX+	Белый/оранжевый
2	TX-	Оранжевый/белый
3	RX+	Белый/зеленый
4	Не используется	
5	Не используется	
6	RX-	Зеленый/белый
7	Не используется	
8	Не используется	

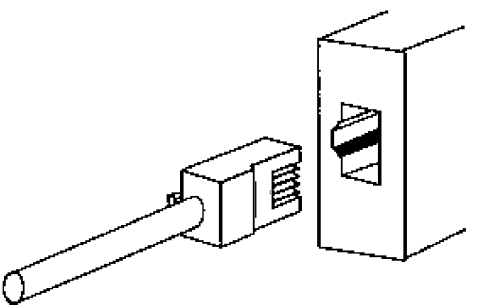


Рис. А.3.2. Разъем RJ-45

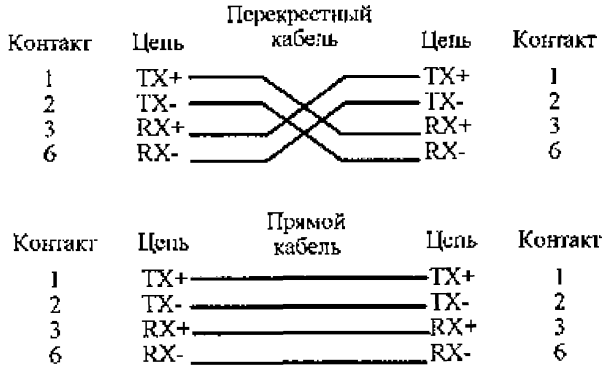


Рис. А.3.3. Соединение проводов прямого и перекрестного кабелей сегмента 10BASE-T

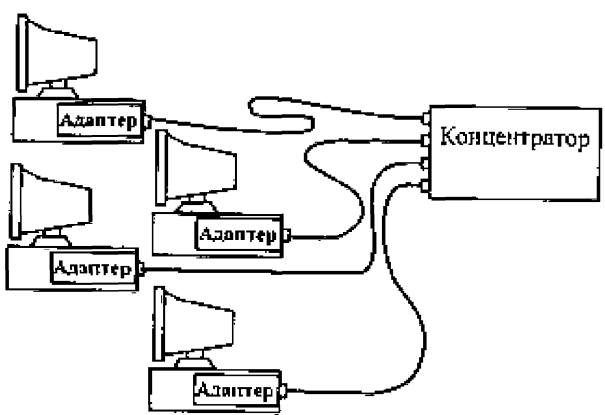


Рис. А.3.4. Соединение компьютеров сети 10BASE-T

В сети 10BASE-T применяются два вида соединения проводов кабеля (рис. А.3.3.). Если надо объединить в сеть всего два компьютера, то можно обойтись вообще без концентратора, применив так называемый перекрестный кабель (crossover cable), который соединяет передающие контакты одного разъема RJ-45 с приемными контактами другого разъема RJ-45 и наоборот. А для соединения компьютеров с концентратором обычно используется прямой кабель (direct cable), в котором соединяются между собой одинаковые контакты обоих разъемов (рис. А.3.4). На такой прямой кабель рассчитано большинство концентраторов.

Следует также отметить такую особенность адаптеров и концентраторов, рассчитанных на работу с витой парой, как наличие в них встроенного контроля правильности соединения сети. При отсутствии передачи информации они периодически передают тестовые импульсы (NLP - Normal Link Pulse), по наличию которых на приемном конце определяется целостность кабеля. Для визуального контроля правильности соединений предусмотрены специальные светодиоды «Link», которые горят при правильном соединении аппаратуры. Это очень удобно и выгодно отличает сегмент 10BASE-T от 10BASE2 и 10BASE5, где подобная функция из-за шинной структуры в принципе не может быть предусмотрена.

А.4 Аппаратура 1OBASE-FL

Широко использовать оптоволоконный кабель в Ethernet начали сравнительно недавно. Его применение позволило сразу же значительно увеличить допустимую длину сегмента и существенно повысить помехоустойчивость передачи. Полная гальваническая развязка компьютеров сети. Возможность плавного перехода на Fast Ethernet, так как пропускная способность оптоволокна позволяет достигнуть не только 100 Мбит/с, но и более высоких скоростей передачи.

Передача информации в данном случае идет по двум оптоволоконным кабелям, передающим сигналы в разные стороны (рис. А.4.1.). Стоимость оптоволоконного кабеля не слишком высокая (она близка к стоимости тонкого коаксиального кабеля). Аппаратура заметно дороже, из-за использования дорогих оптоволоконных трансиверов.

Аппаратура 10BASE-FL имеет сходство как с аппаратурой 10BASE5 (здесь тоже применяются внешние трансиверы, соединенные с адаптером трансиверным кабелем), так и с аппаратурой 10BASE-T (здесь также применяется топология «пассивная звезда» и два разнонаправленных кабеля).

Оптоволоконный трансивер называется FOMAU (Fiber Optic MAU). Он выполняет все функции обычного трансивера (MAU), но, кроме того, преобразует электрический сигнал в оптический при передаче и обратно при приеме. FOMAU также формирует и контролирует сигнал целостности линии связи, передаваемый в паузах между передаваемыми пакетами. Целостность линии связи, как и в случае 10BASE-

T, индицируется светодиодами «Link». Для присоединения трансивера к адаптеру применяется стандартный АШ-кабель, такой же, как и в случае 10BASE5, но длина его не должна превышать 25 м.

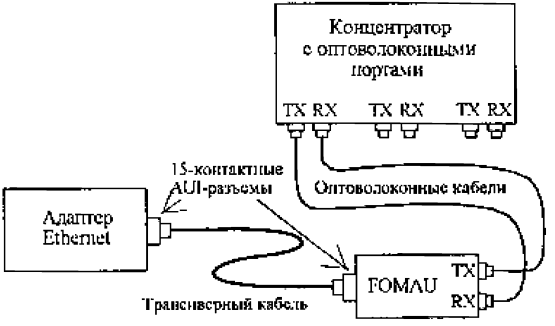


Рис. А.4.1. Соединение адаптера и концентратора в 10BASE-FL

Длина оптоволоконных кабелей, соединяющих трансивер и концентратор, может достигать 2 км без применения каких бы то ни было ретрансляторов.

10BASE-FL наиболее распространен в настоящее время. Он обеспечивает связь между двумя компьютерами, между двумя репитерами или между компьютером и репитером. Максимальное расстояние - до 2000 м.

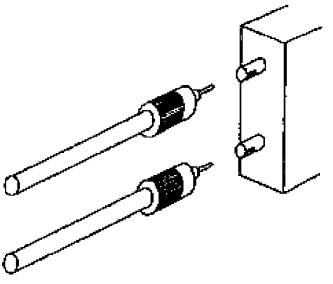


Рис. А.4.2. ST-разъем для оптоволоконного кабеля

Стандартный оптоволоконный кабель 10BASE-FL должен иметь на обоих концах оптоволоконные байонетные ST-разъемы, показанные на рис. А.4.2. (стандарт BFOC/2.5). Используются также разъемы типа SC, присоединяемые подобно RJ-45 путем простого вставления в гнездо. Разъемы SC обычно жестко соединены по два для двух кабелей (рис. А.4.3.). Существуют также разъемы типа MIC FDDI, подобно разъемам SC вставляемые в гнездо.

В соответствии со стандартом, в 10BASE-FL используется мультимодовый кабель и свет с длиной волны 850 нм, хотя в перспективе не исключен переход на одномодовый кабель. Суммарные оптические потери в сегменте (как в кабеле, так и в разъемах) не должны превышать 12,5 дБ. При этом потери в кабеле составляют около 4-5 дБ на километр длины кабеля, а потери в разъеме - от 0,5 до 2,0 дБ (эта величина сильно зависит от качества установки разъема). Только при таких величинах потерь можно гарантировать устойчивую связь на предельной длине кабеля.

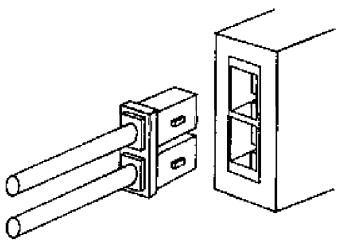


Рис. А.4.3. SC-разъем для оптоволоконного кабеля

Если требуется соединить больше двух компьютеров, то надо использовать концентратор, (рис. А.4.4) имеющий оптоволоконные порты. Каждый компьютер снабжается трансивером и трансиверным кабелем, а также двумя оптоволоконными кабелями с соответствующими разъемами.

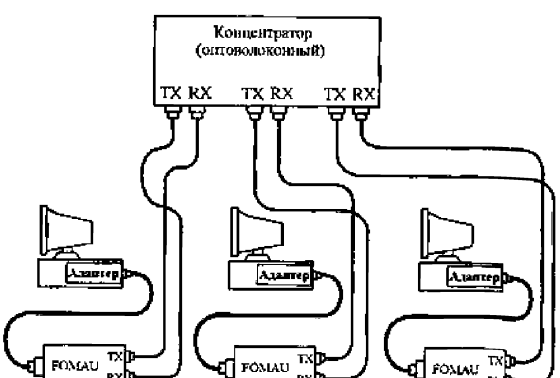


Рис. А.4.4. Объединение компьютеров в сеть по стандарту 10BASE-FL

А.5 Аппаратура 100BASE-TX

Схема объединения компьютеров в сеть 100BASE-TX практически ничем не отличается от схемы в случае 10BASE-T (рис. А.5.1.). Однако в этом случае необходимо применение кабелей с неэкранированными сдвоенными витыми парами (UTP) категории 5 или выше.

Для присоединения кабелей так же, как и в случае 10BASE-T, используются 8-контактные разъемы типа RJ-45. Но эти разъемы (категории 5) несколько отличаются от разъемов категории 3. Как и для 10BASE-T, длина кабеля не может превышать 100 м, используется топология «пассивная звезда» с концентратором в центре. Только сетевые адаптеры должны быть Fast Ethernet, и концентратор должен быть рассчитан на подключение сегментов 100BASE-TX. Именно поэтому рекомендуется при установке сети 10BASE-T сразу же прокладывать кабель категории 5. Между адаптерами и кабелями сети могут включаться выносные трансиверы.

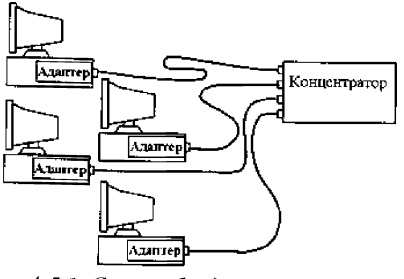


Рис. А.5.1. Схема объединения компьютеров по стандарту 10OBASE-TX

Хотя максимальная длина кабеля как в 10BASE-T, так и в 100BASE-TX равна 100 м, но природа этих ограничений различна. В случае 10BASE-T предельная длина кабеля в 100 м ограничена только качеством кабеля (точнее, затуханием сигнала в нем) и в принципе может быть увеличена при использовании более совершенного кабеля (например, до 150 м). А в случае 100BASE-TX предельная длина 100 м определяется заданными временными соотношениями обмена (установленным ограничением на двойное время прохождения) и не может быть увеличена ни при каких условиях. Поэтому стандарт даже рекомендует ограничиваться длиной сегмента в 90 м, чтобы иметь 10-процентный запас.

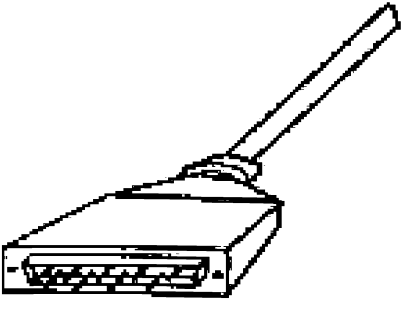


Рис. А.5.2. Разъем DB-9

Табл. А.5.1. Распределение контактов разъема типа RJ-45

Контакт	Назначение	Цвет провода
1	TX+	Белый/оранжевый
2	TX-	Оранжевый/белый
3	RX+	Белый/зеленый
4	Не используется	
5	Не используется	
6	RX-	Зеленый/белый
7	Не используется	
8	Не используется	

Из восьми контактов разъема RJ-45 используется только 4 контакта (табл. А.5.1): два для передачи информации (TX+ и TX-) и два для приема информации (RX+ и RX-). Передача производится дифференциальными сигналами. Стандарт предусматривает также возможность применения экранированного кабеля с двумя витыми парами проводов (волновое сопротивление - 150 Ом). В этом случае должен применяться 9-контактный экранированный разъем DB-9, он же разъем STP IBM типа 1 (рис. А.5.2.). Назначение контактов этого разъема приведено в табл. А.5.2.

Табл. А.5.2. Распределение контактов разъема DB9

Контакт	Назначение	Цвет провода
1	RX+	Оранжевый
2	Не используется	
3	Не используется	
4	Не используется	
5	TX+	Красный
6	RX-	Черный
7	Не используется	
8	Не используется	
9	TX-	Зеленый

Как и в случае 10BASE-T, в сети 100BASE-TX могут использоваться два типа кабеля: прямой и перекрестный (рис. А.5.3). Для соединения двух компьютеров без применения концентраторов используется стандартный перекрестный (crossover) кабель. А для присоединения компьютера к концентратору применяется прямой (direct) кабель с соединенными между собой одинаковыми контактами разъемов. Если перекрестное соединение предусмотрено внутри концентратора, то соответствующий порт его должен быть помечен буквой «X». Как видим, здесь все точно так же, как и в случае 10BASE-T.

Для контроля целостности сети в 100BASE-TX предусмотрена передача в интервалах между сетевыми пакетами специальных сигналов (FLP — Fast Link Pulse), выполняющих также функцию автоматического согласования скорости передачи аппаратных средств.

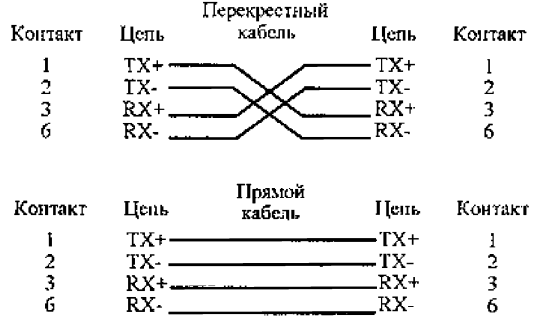


Рис. А.5.3. Прямой и перекрестный кабели, применяемые в сегменте 10OBASE-TX

А.6 Аппаратура 100BASE-T4

Основное отличие аппаратуры 100BA5E-T4от 100BASE-TX состоит в том, что передача производится по счетверенным неэкранированным витым парам. При этом кабель может быть менее качественным, чем в случае 100BASE-TX (категории 3,4 или 5). Принятая в 100BASE-T4 система кодирования сигналов обеспечивает ту же самую скорость 100 Мбит/с на любом из этих кабелей, хотя стандарт рекомендует, если есть такая возможность, использовать кабель категории 5.

Схема объединения компьютеров в сеть ничем не отличается от 100BASE-TX (рис. А.5.1). Компьютеры присоединяются к концентратору по схеме пассивной звезды. Длина кабелей точно так же не может превышать 100 м (стандарт и в этом случае рекомендует ограничиваться 90 м для 10-процентного запаса). Между адаптерами и кабелями в случае необходимости могут включаться выносные трансиверы.

Как и в случае 100BASE-TX, для подключения сетевого кабеля к адаптеру (трансиверу) и к концентратору используются 8-контактные разъемы типа RJ-45. Но в данном случае задействованы все 8 контактов разъема. Назначение контактов разъемов представлено в таблице табл.А.6.1 .

Обмен данными идет по одной передающей витой паре, по одной приемной витой паре и по двум двунаправленным витым парам с использованием трехуровневых дифференциальных сигналов.

Табл. А.6.1. Распределение контактов разъема типа RJ-45 для сегмента 10OBASE-T4 (TX - передача

данных, RX - прием данных, BI - двунаправленная передача)

Контакт	Назначение	Цвет провода
1	TX_D1+	Белый/оранжевый
2	TX_D1-	Оранжевый/белый
3	RX_D2+	Белый/зеленый
4	BI_D3+	Голубой / белый
5	BI_D3-	Белый / голубой
6	RX_D2-	Зеленый/белый
7	BI_D4+	Белый / коричневый
8	BI_D4-	Коричневый / белый

Для связи двух компьютеров без применения концентраторов используется перекрестный кабель. В обычном же прямом кабеле, применяемом для соединения компьютера с концентратором, соединены одноименные контакты обоих разъемов. Схемы кабелей приведены на рис А.6.1. Если перекрестное соединение предусмотрено внутри концентратора, то соответствующий порт должен помечаться буквой «X». Как видим, и здесь все точно так же, как в случае 100BASE-TX и 10BASE-T.

Для контроля целостности сети в 100BASE-T4 также предусмотрена передача специального сигнала FLP между сетевыми пакетами. Наличие связи индицируется светодиодами «Link».

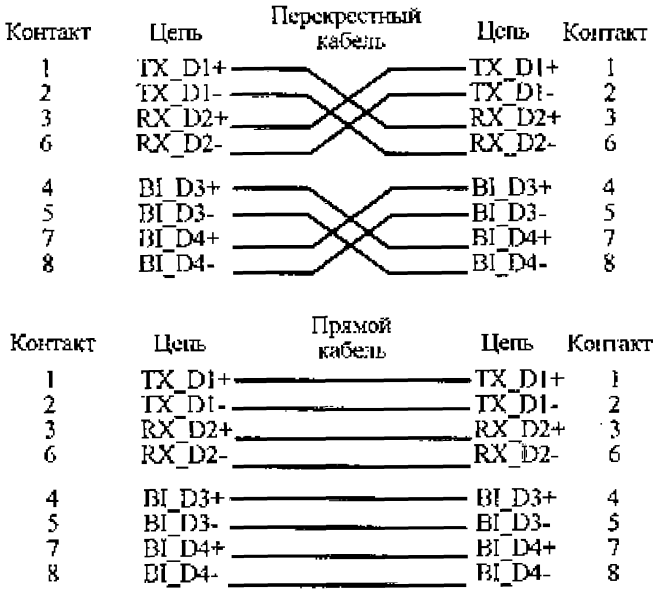


Рис. А.6.1. Прямой и перекрестный кабель сети 10OBASE-T4

А.7 Аппаратура 100BASE-FX

Применение оптоволоконного кабеля в сегменте 100BASE-FX позволяет существенно увеличить протяженность сети, а также избавиться от электрических наводок и повысить секретность передаваемой информации.

Аппаратура 100BASE-FX очень близка к аппаратуре 10BASE-FL. Точно так же здесь используется топология «пассивная звезда» с подключением компьютеров к концентратору с помощью двух разнонаправленных оптоволоконных кабелей (рис. А.7.1). Между сетевыми адаптерами и кабелями возможно включение выносных трансиверов. Как и в случае сегмента 10BASE-FL, оптоволоконные кабели подключаются к адаптеру (трансиверу) и к концентратору с помощью разъемов типа SC, ST или FDDI. Для присоединения разъемов SC и FDDI достаточно просто вставить их в гнездо, а разъемы ST имеют байонетный механизм.

Максимальная длина кабеля между компьютером и концентратором составляет 412м, причем это ограничение определяется не качеством кабеля, а установленными временными соотношениями. Согласно стандарту, применяется мультимодовый или одномодовый кабель с длиной волны света 1,35 мкм. В последнем случае потери мощности сигнала в сегменте (в кабеле и разъемах) не должны превышать 11 дБ. При этом надо учитывать, что потери в кабеле составляют 1-5 дБ на километр длины, а потери в разъеме - от 0,5 до 2 дБ (при условии, что разъем установлен качественно).

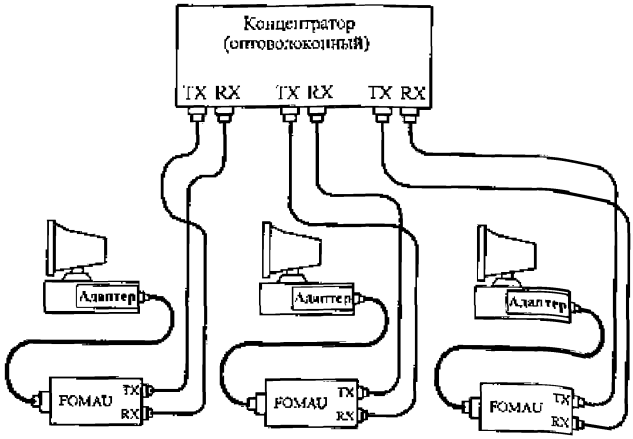


Рис. А.7.1. Подключение компьютеров к сети 10OBASE-FX

Как и в других сегментах Fast Ethernet, в 100BASE-FX предусмотрен контроль за целостностью сети, для чего в промежутках между сетевыми пакетами по кабелю передается специальный сигнал. Целостность сети индицируется светодиодами «Link».

Прокладывание локальной сети

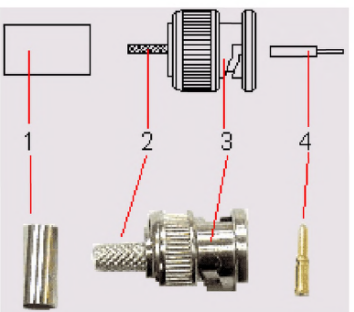
Б.1 Прокладывание локальной сети 10Base2

Перед прокладыванием локальной сети, необходимо определиться с взаимным расположением компьютеров, которые вы планируете объединить между собой. В случае если предполагается создание системы «точка-точка», то есть локальной сети, состоящей из двух компьютеров, вам потребуется один-единственный отрезок коаксиального кабеля, общей длиной не более 185 м. Если же создаваемая вами система будет объединять несколько ПК, следует заранее определить последовательность их подключения, поскольку в сетях 10Base2 компьютеры соединяются между собой «цепочкой». Когда вопрос с конфигурацией сети будет решен, необходимо отрезать несколько частей коаксиального кабеля соответствующей длины, их количество должно совпадать с количеством сетевых сегментов. Также вам потребуется по два разъема BNC для каждого из полученных отрезков, по одному Т-коннектору для каждого из подключаемых к сети компьютеров и два терминатора.

Б.2 Монтаж разъемов BNC

В нашей стране наиболее распространены три типа разъемов BNC: «под пайку» отечественного производства марки «СР», предназначенные для использования в сетях с волновым сопротивлением 50 Ом и частотой до 10 ГГц, а также «под обжим» и «под накрутку» импортного производства. Разъемы «под пайку» обычно не обеспечивают должного качества соединения,

поскольку малейшая неосторожность в припаивании контакта центральной жилы или экрана приводит к тому, что при случайном шевелении кабеля сеть перестает работать, и локализовать сбойный участок оказывается крайне сложно. Поэтому опытные специалисты рекомендуют приобретать разъемы BNC «под обжим», которые не только полностью соответствуют стандарту Ethernet 10Base2, но и крайне просты в монтаже (рис. Б.2.1).



Условные обозначения: 1— манжета; 2— контактная площадка заземления; 3— разъем; 4 — контакт центрального провода

Рис. Б.2.1. Разъем BNC «под обжим»:

Рис. Б.2.2. Обжимной инструмент для коаксиального кабеля

Такой разъем состоит из трех элементов: это сам разъем с рифленой контактной площадкой заземления, контакт центрального провода и металлическое цилиндрическое кольцо — манжета. Помимо самого разъема вам понадобится также специальный обжимной инструмент для коаксиального кабеля (рис. Б.2.2). Если обжимного инструмента нет под рукой, можно воспользоваться обыкновенными пассатижами. Порядок монтажа разъема BNC (рис. Б.2.3).

1. Ровно обрежьте край коаксиального кабеля таким образом, чтобы на его торце не было зазубрин и скосов. Наденьте на кабель металлическую муфту разъема BNC.

2. При помощи острого ножа или скальпеля удалите верхний защитный изоляционный слой коаксиального кабеля на расстояние приблизительно 20-25 мм от края. Аккуратно расплетите оплетку экрана и разведите ее в стороны.

3. Стараясь не повредить центральный проводник, снимите острым ножом или скальпелем защит-

ный слой проводящей жилы коаксиального кабеля на расстояние примерно 5-8 мм. Наденьте на проводящую жилу контакт центрального провода.

4. Посредством обжимного инструмента или тонких плоскогубцев зажмите цилиндрическую часть контакта центрального провода таким образом, чтобы он надежно зафиксировался на проводящей жиле. При отсутствии обжимного инструмента контакт центрального провода можно припаять к проводящей жиле.

5. Наденьте на кабель разъем до щелчка таким образом, чтобы контакт центрального провода показался из соответствующего отверстия во внутренней части разъема. Равномерно обмотайте ранее расплетенные вами проводники экранирующей оплетки вокруг рифленой контактной площадки заземления.

6. Надвиньте на контактную площадку заземления с обмотанным вокруг нее экранирующим проводником металлическую муфту разъема и надежно зафиксируйте ее при помощи обжимного инструмента или плоскогубцев.

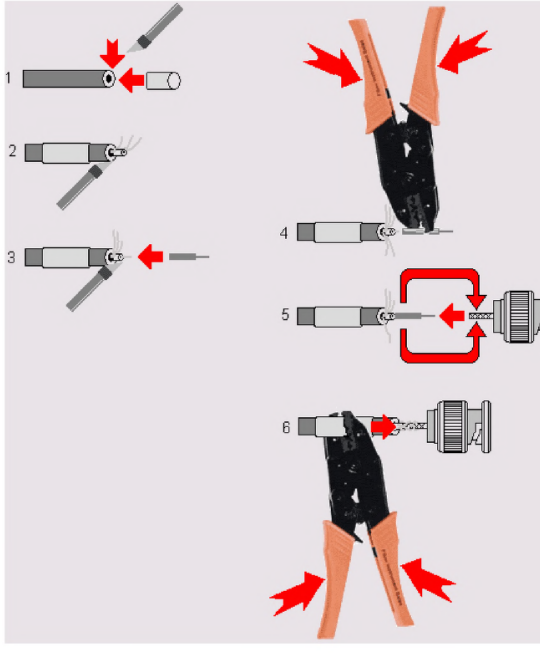


Рис. Б.2.3. Порядок монтажа разъема BNC

Б.3 Общая схема подключений

Общая схема подключений в локальной сети 10Base2, состоящей из трех компьютеров, показана на рис. Б.3.1.

К оконечным разъемам Т-коннекторов, к которым не присоединяется более никаких устройств, подключаются терминаторы.

На участках сети, где требуется соединить два отрезка коаксиального кабеля без подключения промежуточного устройства, используются так называемые I-коннекторы или прямые переходы.

При такой конфигурации допустимо выключать питание любого из входящих в сеть компьютеров без потери соединения для всех остальных узлов сети. Локальная сеть перестает работать только в том случае, если на одном из участков линии (в разъеме, Т-коннекторе или прямом переходе) потерян контакт, либо если один из отрезков коаксиального кабеля неплотно подключен к соответствующему разъему. В некоторых случаях отказ сети бывает вызван потерей сопротивления нагрузки в одном из терминаторов.

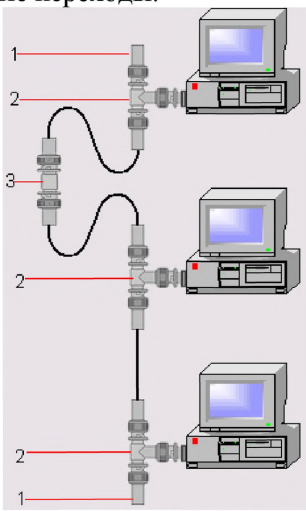


Рис. Б.3.1. Общая схема подключений в сети 10Base2

1 - терминатор; 2 - Т-коннектор; 3 - I-коннектор (прямой переход).

Б.4 Установка Т-коннекторов

Т-коннекторы предназначены для организации надежного соединения коаксиального кабеля с разъемом сетевого адаптера рабочей станции в сетях 10Base2. Внешне Т-коннектор представляет собой Т-образный трехсекционный разъем, к двум противоположным секциям которого подключаются разъемы BNC коаксиального кабеля, а третий фиксируется в соответствующем гнезде сетевого адаптера (рис. Б.4.1).

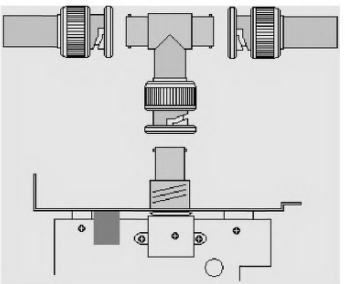


Рис. Б.4.1. Т-коннектор

Последовательность установки Т-коннекторов и подключения к ним сетевого кабеля:

1. Установите Т-коннектор в ответный разъем BNC сетевого адаптера таким образом, чтобы штырьки замка разъема вошли в соответствующие пазы на вращающейся шайбе Т-коннектора. Проверните шайбу до полной фиксации Т-коннектора в разъеме.

2. Аналогичным образом наденьте на боковые секции Т-коннектора разъемы сетевого кабеля и зафиксируйте их поворотом вращающейся шайбы.

Б.5 Установка терминаторов

Терминаторы, либо, как их еще называют, колпачки или заглушки — это специальные металлические насадки, подключающиеся к разъемам Т-коннекторов на крайних сегментах локальной сети 10Base2 и создающие в сети требуемое сопротивление нагрузки (рис. 5.6).

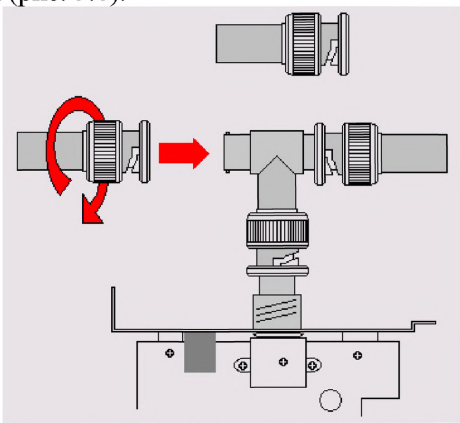


Рис. Б.5.1. Установка терминатора

Согласно стандарту 10Base2, один из двух подключенных к сети терминаторов должен быть заземлен. Для этого используется терминатор с припаянной к нему металлической цепочкой, оснащенной специальным контактом, который должен быть зафиксирован на металлическом корпусе компьютера. Несоблюдение этого требования может привести к выходу из строя локальной сети или одного из сетевых адаптеров.

Б.6 Переходы прямые

Переходы прямые, или I-коннекторы, применяются в тех случаях, когда возникает необходимость соединить между собой несколько отрезков коаксиального кабеля (сегментов сети) без подключения между ними промежуточного устройства. Например, в случае, если один из компьютеров пришлось физически отключить от локальной сети, и в данном ее сегменте образуется «разрыв». Существует разъемы, пригодные для организации прямых переходов - так называемые I-коннектор (barrel-connector, рис. Б.6.1.)

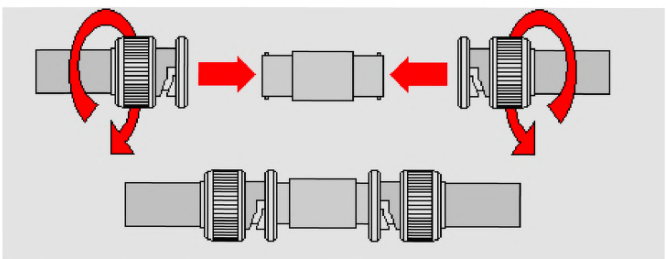


Рис. Б.6.1 I-коннекторы (переходы прямые)

Обычные I-коннекторы представляют собой двухсекционный разъем, позволяющий подключать к каждой из своих секций по одному разъему BNC, установленному на соответствующем отрезке коаксиального кабеля, выполняя, таким образом, непосредственное соединение между собой двух сегментов сети.

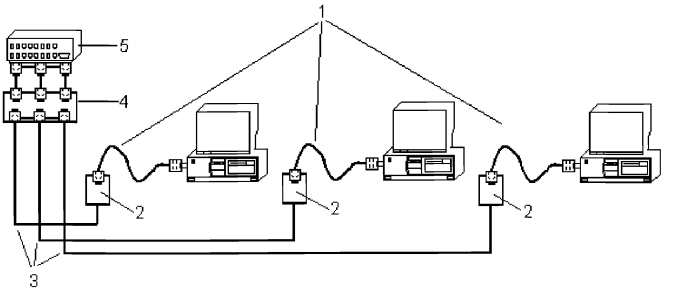
Б.7 Прокладывание локальной сети 10BaseT

Монтаж и прокладывание локальной сети 10BaseT - несколько более сложная задача, чем подготовка к работе сети Thin Ethernet. Во-первых, для этого потребуется значительно больше базовых элементов, чем в случае 10Base2, а во-вторых, сам монтаж такой сети требует более кропотливой и тонкой работы. Итак, прежде, чем приступить к работе над прокладыванием сети, нужно запастись необходимым набором компонентов, которые должны находиться под рукой. Исключение составляет только вариант, при котором в сеть 10BaseT объединяются два компьютера по принципу «точка-точка»: в этом случае вам необходимо приобрести один отрезок кабеля «витая пара» необходимой длины и два разъема RJ-45.

Б.8 Общая схема подключений

Перед прокладыванием локальной сети класса 10BaseT необходимо тщательно продумать взаимное расположение компьютеров. В конфигурации 10BaseT компьютеры подключаются к концентратору не напрямую, а через специальные сетевые розетки RJ-45 (рис. Б.8.1).

Сетевые розетки монтируются на стену в непосредственной близости от подключаемого к локальной сети компьютера. Каждая розетка соединяется с разъемом RJ-45, расположенным на сетевом адаптере ПК, при помощи небольшого отрезка кабеля «витая пара», который принято называть Path cord или «поводок». Длина этого кабеля не должна превышать 10 м, на концах провода Path cord крепится два разъема RJ-45.



Условные обозначения: 1— Path Cord;
2— сетевые розетки RJ-45;
3— кабель «витая пара»;
4— path panel;
5— концентратор.

Рис. Б.8.1. Общая схема подключений устройств в сети 10BaseT:

Такая конфигурация подключений крайне удобна, потому что, во-первых, позволяет быстро присоединять и отсоединять компьютеры от локальной сети, а также менять их местами - для этого достаточно вытащить Path cord из розетки, а во-вторых, сетевой кабель не натягивается при прокладывании и не путается под ногами. От каждой сетевой розетки отходит еще один отрезок кабеля «витая пара», с одной стороны смонтированный непосредственно в розетке, с другой стороны — оснащенный разъемом RJ-45. Длина каждого отрезка такого кабеля не может превышать 90 м. Оконечные разъемы всех идущих от сетевых розеток отрезков кабеля присоединяются к комбинированной многопортовой сетевой розетке Path panel, либо к равному количеству обычных сете-

вых розеток RJ-45. В свою очередь, маленькие отрезки кабеля «витая пара», смонтированные в Path panel (длиной не более 1 м) и оснащенные на концах собственными разъемами RJ-45, вставляются в соответствующие гнезда концентратора. Path panel или дополнительный набор сетевых розеток применяются только исходя из удобства администрирования локальной сети: во-первых, каждую из таких розеток или каждое из гнезд Path panel можно промаркировать - если концентратор расположен на значительном удалении от рабочих мест, порой бывает трудно определить, какой из проводов ведет к нужному компьютеру. Во-вторых, используя Path panel, можно без труда переместить любой из проводов между имеющимися в наличии разъемами, быстро подключив его таким образом к другому порту концентратора. На практике дополнительный набор сетевых розеток или Path panel обычно не монтируются - участки кабеля, идущие от розеток RJ-45 на рабочих местах, как правило, подключаются к концентратору напрямую. Во избежание путаницы их просто фиксируют прикрученной к стене поблизости от концентратора металлической пластиной и на каждый провод приклеивают при помощи скотча бумажку с указанием, от какой именно розетки он идет. Такой монтаж гораздо более удобен и надежен, хотя и может вызвать определенные неудобства в случае необходимости изменения конфигурации локальной сети. Общая последовательность действий при монтаже сети 10BaseT:

1. Составьте точный план помещения, в котором вы планируете проложить сеть, и определите, где именно будут располагаться рабочие места пользова-

телей и где будет смонтирован концентратор. Большинство моделей концентраторов требуют подключения питания от электрической сети. Точно измерьте расстояния между точкой подключения концентратора и рабочими местами, определите, где именно будет пролегать сетевой кабель.

2. Смонтируйте концентратор - обычно он привинчивается к стене при помощи специальных фиксирующих винтов.

3. Изготовьте необходимое количество проводов Patch cord, их число должно соответствовать числу рабочих мест в локальной сети. Для этого вам придется отрезать требуемое количество частей кабеля «витая пара» и смонтировать на концах каждого отрезка разъем RJ-45. Длина Path cord не должна превышать 10 м (рекомендуемая длина — 2-3 м).

4. Смонтируйте вблизи каждого рабочего места сетевую розетку RJ-45, закрепив ее при помощи фиксирующих винтов на стене. Смонтируйте внутри каждой розетки отрезок кабеля «витая пара». Длина этого отрезка должна соответствовать расстоянию от розетки до концентратора, но она не может превышать установленное стандартное значение 90 м.

5. Проложите каждый отрезок кабеля «витая пара» от розетки до концентратора, укрепив его вдоль плинтуса или на стене помещения специальными фиксирующими скобами.

6. Смонтируйте на противоположном от розетки конце каждого отрезка сетевого кабеля разъем RJ-45.

7. Подключите оконечные разъемы RJ-45 в соответствующие гнезда концентратора и включите его питание.

Технические требования к прокладке сетевого кабеля 10BaseT:

- минимальный радиус изгиба кабеля «витая пара» должен составлять 1 дюйм (2,5 см) или величину, равной четырем диаметрам кабеля; рекомендуемый радиус изгиба — 2 дюйма (5 см);

- минимальное расстояние от кабеля «витая пара» до близлежащего силового электрического кабеля с напряжением до 2 кВ должно быть более 5 дюймов (12,5 см), от кабеля с напряжением более 2 кВ — не менее 10 дюймов (25 см);

- участок сети от концентратора до сетевого адаптера не должен включать более трех отдельных отрезков кабеля (соединенных, например, посредством розеток или устройств Path-panel);

- все отрезки кабеля локальной сети (включая Path cord) должны быть одной категории. Рекомендуемый к использованию кабель — восьмижильная «витая пара» категории 5 или 5+ диаметром AWG=22 или 24.

Б.9 Монтаж разъемов RJ-45 на кабеле Path cord

Кабель Path cord — это небольшой отрезок кабеля «витая пара» длиной от 1 до 10 м, на обоих концах которого смонтирован разъем RJ-45. Этот кабель образует участок локальной сети от гнезда сетевого адаптера на компьютере до ближайшей сетевой розетки. Для изготовления одного провода Path cord вам потребуется, помимо отрезка кабеля, два защитных колпачка, два разъема RJ-45 и обжимной инструмент для этих разъемов.

Б.10 Обжимной инструмент

Обжимной инструмент для разъемов RJ-45 несколько отличается от инструмента, используемого при прокладывании сетей 10Base2 (рис. Б.10).

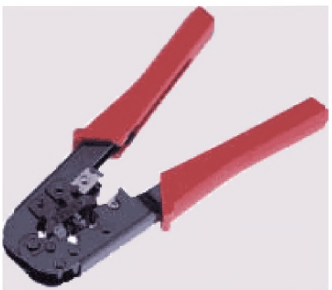


Рис Б.10. Обжимной инструмент для разъемов RJ-45

Обжимной инструмент данного типа отличает, прежде всего, наличие специального выреза в форме разъема RJ-45 (в некоторых случаях рабочая часть инструмента имеет дополнительный вырез под разъем RJ-11, используемый в телефонии), помимо этого многие модели оснащены режущей кромкой для ровной обрезки кабеля «витая пара».

Б.11 Защитные колпачки

Защитные колпачки внешне напоминают небольшие полые изнутри чехлы, повторяющие своей формой очертания разъема RJ-45, выполнены они из мягкого пластика или резины различных цветов. Многообразие расцветок защитных колпачков позволяют

определить по цвету колпачка, к какому именно компьютеру ведет тот или иной шнур.

Защитные колпачки призваны предохранять место соединения кабеля «витая пара» с разъемом RJ-45 от изгибов и заломов. Существует два типа защитных колпачков: литые - они надеваются на кабель до монтажа разъема RJ-45 и позже сдвигаются по направлению к разъему до нужной позиции, и разборные - они состоят из двух половинок, оснащенных замком, и могут надеваться на разъем уже после окончания его монтажа.

Б.12 Разъем RJ-45

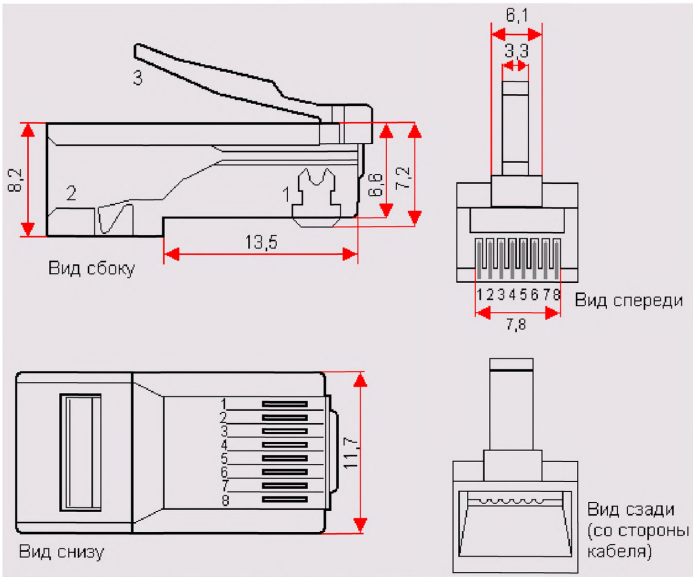
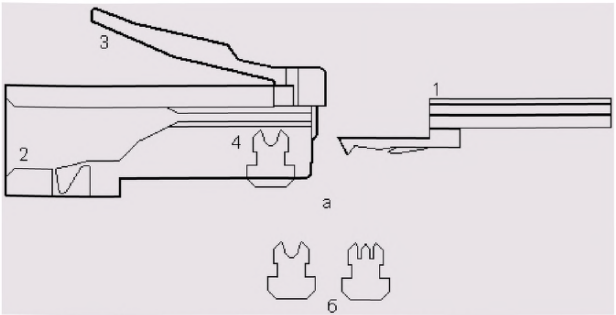


Рис. Б.12.1. Разъем RJ-45: 1 — контакты; 2— держатель кабеля; 3— замок разъема

Разъемы RJ-45 представляют собой полый прозрачный пластиковый корпус с фиксирующим замком, внутри которого расположено восемь подвижных металлических контактов. В новом, необжатом разъеме контакты выходят за пределы корпуса, после обжима они вдавливаются внутрь, прорезая наружный изолирующий слой на проводниках, расположенных внутри кабеля «витая пара», и замыкаясь на проводящую жилу. Существует два типа разъемов RJ-45: с контактной вставкой и без таковой (разъем RJ-45 без контактной вставки показан на рис. Б.12.1). В дальнейшем мы будем рассматривать разъемы RJ-45 без контактной вставки.

Разъем с контактной вставкой несколько отличается по своему устройству от стандартного разъема RJ-45: он состоит из двух независимых элементов - вставки и собственно корпуса разъема (рис.Б.12.2,а). Последовательность монтажа таких разъемов иная по сравнению с обычными: сначала проводники кабеля «витая пара» до упора вставляются в контактную вставку, затем вставка заводится до щелчка в корпус разъема, после чего разъем обжимается.

Верхняя кромка подвижных контактов разъема RJ-45 - острая, она имеет, как правило, два или три зубца (рис.Б.12.2, б). При обжиме разъёма контакты утапливаются внутрь его корпуса, при этом верхняя кромка прорезает изолирующий слой проводника и впивается в проводящую жилу. Практика показывает, что контакты с тремя зубцами обеспечивают более высокую надежность соединения, но при этом двузубые контакты лучше режут изоляцию проводника. Обобщая можно сказать, что глобальных различий в качестве соединения при использовании этих двух типов разъемов нет, то есть можно смело покупать любой тип разъема RJ-45...



Условные обозначения: 1- контактная вставка;
2- держатель контактной вставки;
3- замок разъема;
4- контакты

Рис. Б.12.2. Разъем PJ-45 с контактной вставкой:

Б.13 Последовательность монтажа разъема

1. Наденьте на кабель «витая пара» защитный колпачок.

2. Удалите верхний защитный слой кабеля на расстояние 0,5 дюйма (12,5 мм). Как правило, обжимной инструмент имеет специальную режущую кромку и ограничитель на это расстояние, позволяющий точно проделать указанную процедуру, не выверяя требуемый размер по линейке.

3. Аккуратно расплетите свитые пары проводников. Зачищать их изоляцию до проводящей жилы не требуется.

4. Расположите проводники витой пары в порядке, соответствующем выбранной вами схеме заделки

кабеля. Всего для восьмижильного кабеля существует три возможные схемы заделки: EIA/TIA-568A, EIA/TIA-568B (рис. Б.13.1) и Cross-Over, которая предназначена для прямого соединения двух компьютеров без использования концентратора.

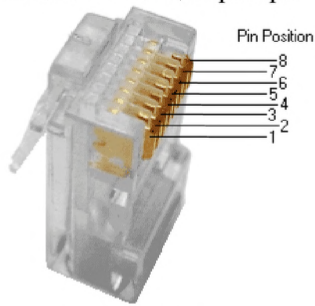
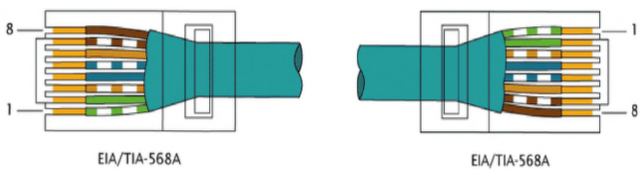
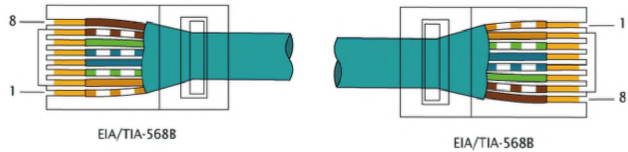


Рис. Б.13.1.а) Нумерация контактов в разъеме.



Условные обозначения: 1 – (зб) зелено-белый проводник;
2 – (з) зеленый проводник;
3 – (об) оранжево-белый проводник;
4 – (с) синий проводник;
5 – (сб) сине-белый проводник;
6 – (о) оранжевый проводник;
7 – (кб) коричнево-белый проводник;
8 – (к) коричневый проводник

Рис. Б.13.1.б) Вариант обжима по стандарту TIA/EIA-568A

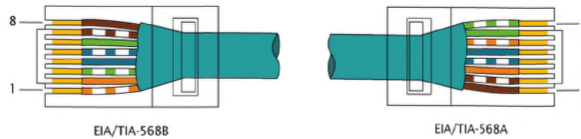


Условные обозначения: 1 – (об) оранжево-белый проводник;
2 – (о) оранжевый проводник;
3 –(зб) зелено-белый проводник;
4 – (с) синий проводник;
5 – (сб) сине-белый проводник;
6 –(з) зеленый проводник;
7 – (кб) коричнево-белый проводник;
8 – (к) коричневый проводник

Рис. Б.13.1.в) Вариант обжима по стандарту TIA/EIA-568B (используется чаще)

Указанные схемы в целом идентичны, однако следует понимать, что на обоих концах кабеля схема должна быть одинаковой, за исключением случая, когда посредством кабеля «витая пара» напрямую соединяется два компьютера (речь о таком соединении пойдет дальше). Выбор конкретного порядка следования проводников зависит от уже используемой в вашей локальной сети схемы заделки.

Перекрестный кабель (crossover cable) используется для соединения однотипного оборудования (например, компьютер-компьютер). Однако большинство сетевых устройств способно автоматически определить метод обжима кабеля и подстроиться под него (Auto MDI/MDI-X).



Условные обозначения вариант для EIA/TIA-568B:

1 – (об) оранжево-белый проводник;
2 – (о) оранжевый проводник;
3 –(зб) зелено-белый проводник;
4 – (с) синий проводник;
5 – (сб) сине-белый проводник;
6 –(з) зеленый проводник;
7 – (кб) коричнево-белый проводник;
8 – (к) коричневый проводник.

Вариант для EIA/TIA-568A:

1 – (зб) зелено-белый проводник;
2 – (з) зеленый проводник;
3 – (об) оранжево-белый проводник;
4 – (с) синий проводник;
5 – (сб) сине-белый проводник;
6 – (о) оранжевый проводник;
7 – (кб) коричнево-белый проводник;
8 – (к) коричневый проводник

Рис. Б.13.1.г) Варианты обжима crossover cable для скорости 100 Мбит/с.

5. В случае если вы используете четырехжильный кабель «витая пара», схема его заделки и расположение в разъеме будут несколько отличаться от описанного выше (рис. Б.13.2). Проводники располагаются в следующем порядке: оранжево-белый, оранжевый, сине-белый, синий, причем первые три подключаются к контактам разъема с 1 по 3, а последний — к контакту 6.

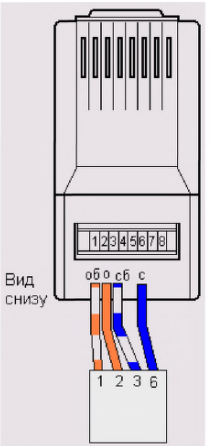
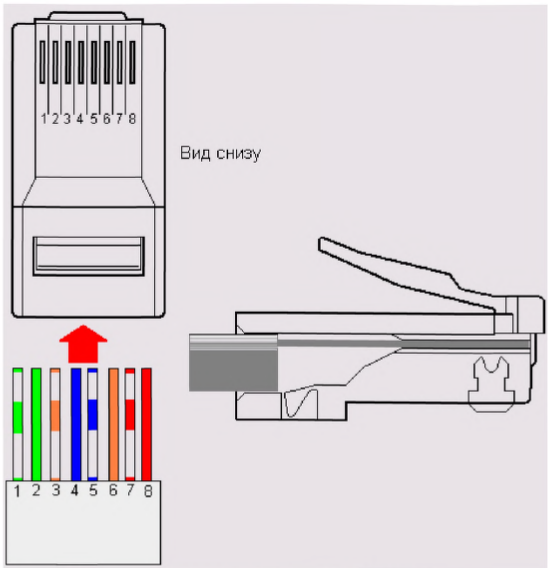


Рис. Б.13.2. Схема заделки четырехжильного кабеля «витая пара»

6. Расположив проводники соответствующим образом, возьмите в руки разъем RJ-45, переверните его контактами к себе, разместив тыльной стороной к кабелю - так, чтобы крепление замка оказалось на противоположной от кабеля стороне разъема, и до предела надвиньте его на выступающие из кабеля проводники (рис. Б.13.3).

7. Вставьте разъем с кабелем в углубление, расположенное на рабочей поверхности обжимного инструмента, и сильным быстрым нажатием на ручки обожмите кабель. При этом выступающие из корпуса разъема контакты и держатель кабеля должны полностью утопиться внутрь разъема.

8. Смонтируйте аналогичным образом все требуемые разъемы RJ-45.



Один из вариантов расположения проводников:

1 – (зб) зелено-белый проводник;
2 – (з) зеленый проводник;
3 – (об) оранжево-белый проводник;
4 – (с) синий проводник;
5 – (сб) сине-белый проводник;
6 – (о) оранжевый проводник;
7 – (кб) коричнево-белый проводник;
8 – (к) коричневый проводник

Рис. Б.13.3. Расположение кабеля «витая пара» в разъеме перед обжимом.

Б.14 Монтаж сетевых розеток

Сетевые розетки под «витую пару» представляют собой пластмассовый короб со съемной крышкой, в верхней части которого смонтирована ответная часть разъема RJ-45, оснащенная восемью подпружиненными контактами, а также имеется то или иное приспособление для подключения проводников сетевого кабеля. Обычно розетка имеет либо специальный клеящий слой, либо отверстия под винты для крепления ее к стене. Если развернуть розетку разъемом к себе таким образом, чтобы контакты оказались внизу, то номера контактов отсчитываются с 1 по 8 справа налево (рис. Б.14.1).

Так же, как и сам кабель «витая пара», сетевые розетки различаются по категориям, наиболее распространенными из которых являются категория 3 (рис. Б.14.1,а) и категория 5 (рисунок Б.14.1,б). В сетевых розетках категории 3 проводники «витой пары» обычно крепятся к контактным площадкам с помощью винтов, что не обеспечивает требуемой надежности соединения. Для монтажа кабеля в таких розетках проводники «витой пары» необходимо расплести на необходимую длину, освободить от изоляции и, вставив в соответствующие контакты, зафиксировать прижимными винтами. При этом необходимо следить за тем, чтобы длина расплетенных проводников была не слишком большой, в противном случае между ними могут возникнуть паразитные наводки. Определить, какой провод «витой пары» должен идти к каждому из прижимных винтов, можно по номерам контактов разъема розетки: в целом схема подключения проводников должна соответствовать выбранной вами схеме заделки кабеля (рис. Б. 13.1).

В более современных розетках категории 5 проводники витой пары просто вставляются в щели специальных контактных площадок, расположенных под углом в 90° к плоскости разъема RJ-45 (рис. Б.14.1,б). При этом удаления защитного слоя с проводников не требуется: щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию. Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, однако в большинстве случаев можно прекрасно обойтись обыкновенным пинцетом и отверткой. Все контакты в розетках категории 5, как правило, пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

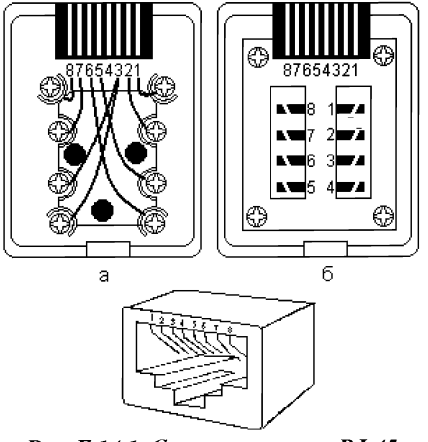


Рис. Б.14.1. Сетевая розетка RJ-45

Общая последовательность монтажа сетевых розеток RJ-45:

1. Снимите крышку розетки, либо надавив на нее сбоку, либо поддев края крышки отверткой (в зависимости от устройства замка крышки).

2. Закрепите розетку на стене вблизи рабочего места либо на фиксирующих винтах, либо на клею.

3. Освободите от наружной изоляции оконечность идущего от розетки к концентратору кабеля «витая пара» на требуемую глубину и аккуратно расплетите проводники.

4. Присоедините проводники к контактам розетки согласно выбранной вами схеме заделки кабеля.

5. Закройте крышку розетки.

6. На противоположном от розетки конце кабеля «витая пара» смонтируйте разъем RJ-45, соблюдая выбранную вами схему заделки.

7. Проложите кабель до места крепления концентратора, фиксируя его через равные промежутки на плинтусе или на стене специальными крепежными скобами.

8. Подключите разъем RJ-45 в соответствующий порт концентратора.

Б.15 Монтаж разъема RJ-45 если нет обжимного инструмента

Если под рукой не оказалось обжимного инструмента, разъем RJ-45 можно смонтировать при помощи обыкновенной отвертки. В процессе проведения подобной операции следует проявлять крайнюю осторожность, поскольку, во-первых, обжим разъема «вручную» далеко не всегда обеспечивает требуемую

надежность соединения, а во-вторых, многократно увеличивает опасность испортить разъем. Вместе с тем, такой способ монтажа вполне имеет право на жизнь, и более того, нередко применяется на практике.

Последовательность операций при монтаже разъема RJ-45 без обжимного инструмента такова (рис. Б.15.1).

1. Вставьте в разъем кабель «витая пара», предварительно распределив проводники согласно выбранной вами схеме заделки.

2. Переверните разъем замком вниз, контактами к себе. Уложите его на ровную поверхность таким образом, чтобы края разъема имели надежную опору, а замок находился в свободном положении во избежание его случайных повреждений - например, между двух дощечек или двух книг.

3. Взяв в руки твердую отвертку, осторожным нажатием утопите вниз фиксатор кабеля до тех пор, пока он не перестанет выступать из корпуса разъема. Кабель будет надежно закреплен в корпусе (рис. Б.15.1,а).

4. Осторожными нажатиями на отвертку утопите в корпус разъема до упора все восемь выступающих наружу контактов — они должны проткнуть изоляционный слой проводников и «впиться» в проводящую жилу. Внимательно следите за тем, чтобы не погнуть и не повредить иным способом тонкие пластины контактов (рис. Б.15.1.б)

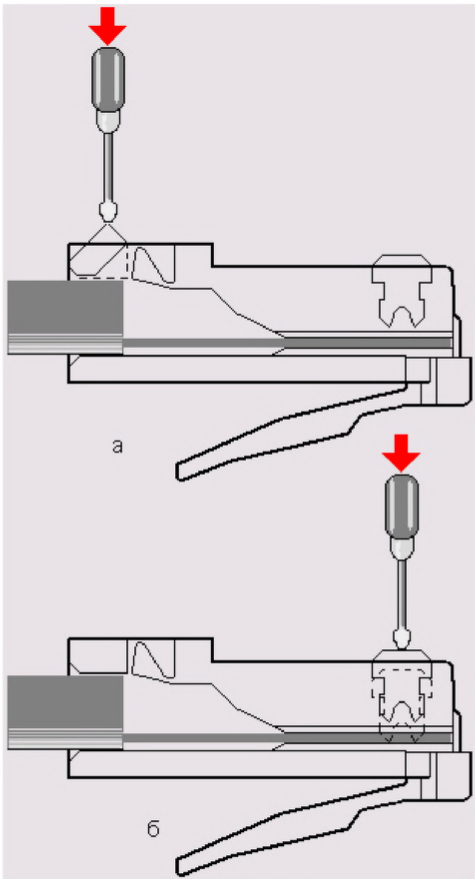
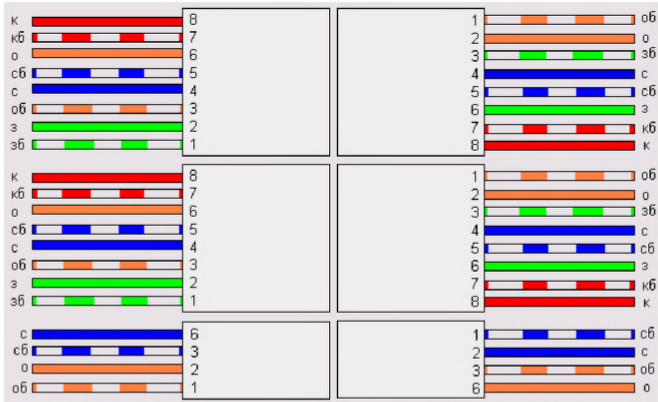


Рис. Б.15.1. Монтаж разъема RJ-45 без обжимного инструмента

Б.16 Прямое соединение двух компьютеров по схеме «точка—точка»

Для соединения двух компьютеров в сеть по технологии Ethernet 10BaseT без использования каких-либо дополнительных устройств, таких как концентраторы или сетевые розетки, вам потребуется специальным образом смонтированный кабель «витая пара», который подключается непосредственно к разъемам RJ-45 присоединенных к сети компьютеров. Такой монтаж кабеля принято называть cross-over, MDI-X или null-hub cable. Длина cross-over-кабеля не должна превышать 100 м. Порядок следования проводников в разъемах для восьмижильного и четырехжильного кабеля при заделке по стандарту cross-over показан на рис. Б.16.1. Для восьмижильного кабеля на иллюстрации предлагается два альтернативных варианта, которые в целом функционально идентичны.

Обратите внимание на тот факт, что при использовании четырехжильного кабеля монтаж первых трех проводников в разъем осуществляется подключением к контактам 1, 2 и 3, а последнего — к контакту 6.



Условные обозначения: зб— зелено-белый проводник;
з— зеленый проводник;
об— оранжево-белый проводник;
о—оранжевый проводник;
сб— сине-белый проводник;
с— синий проводник;
кб— коричнево-белый проводник;
к— коричневый проводник

Рис. Б.16.1. Схема заделки кабеля «витая пара» при cross-over подключении:

Литература:

Айвенс К. «Компьютерные сети. Хитрости.» - Питер, 2000 г

Буравчик .Д «Локальная сеть без проблем» - Москва, 2005 г.

Галкин В.А., Григорьев Ю.А. «Телекоммуникации и сети: Учеб. пособие для вузов». - М.: Изд-во МГТУ им. Н.Э. Баумана, 2003 г.

Гук.М. «Аппаратные средства локальных сетей. Энциклопедия». Питер, 2000 г.

Коломоец Г.П. «Организация компьютерных сетей.» Запорожье : КПУ, 2012

Короуз.Д., Росс.К. «Компьютерные сети» - Питер, 2004 г.

Кузин А. В. « Компьютерные сети». - 3-е изд., перераб. и доп.- М.: ФОРУМ: ИНФРА-М

Куин Л., Рассел. Р. «Fast Ethernet» 1998 г.

Минаев И. Я. «Локальная сеть своими руками» - М. 2004 г

Новиков Ю.В., Кондратенко.С.В. «Локальные сети: архитектура, алгоритмы, проктирование.» - М. 2000 г

Олифер В.Г, Олифер Н.А. «Компьютерные сети. Принципы, технологии, протоколы.» 4-издание . Питер 2010 г.

Уилсон Э. « Мониторинг и анализ сетей. Метод выявления неисправностей.» - М. 2002 г.

Уэнделл О. «Компьютерные сети.» - Москва, Питер, Киев. 2006 г.

Шиндер Д. Л. «Основы компьютерных сетей.» - М. 2002

Приказ МВД РФ от 16.06.2011 №676 «Об утверждении Инструкции по организации работы пунктов централизованной охраны подразделений вневедомственной охраны» через источники бесперебойного питания»

«Методические рекомендации Р78.36.021-2012 Примерные должностные инструкции инженерно-технического состава и дежурной смены пунктов централизованной охраны подразделений вневедомственной охраны».

Романов В. П. «Техническое обслуживание средств вычислительной техники. Учебно-методическое пособие.» ФГОУ СПО «Кузнецкий индустриальный техникум», Новокузнецк, 2008 г.

«Обслуживание сетевого оборудования. Поиск неисправностей в локальных сетях. Лекции физического факультета Кемеровского Государственного Университета.»
http://physic.kemsu.ru/pub/library/learn_pos/Udin/oo_lec_8.pdf

«Руководство по устранению сбоев в компьютерных сетях.» Fluke Corporation, 2012 г.