Тема 16.
ЛОКАЛЬНЫЕ СЕТИ.

Лекция.1. Архитектура и протоколы.

16.1.1. Традиционные локальные сети Ethernet и Token Ring.

Ethernet и Token Ring - самые распространенные и наиболее апробированные стандарты, используемые для создания локальных связей в сетях. Хотя их пропускная способность - 10 и 16 Мб/с соответственно - во многих случаях уже недостаточна для некоторых современных приложений даже на клиентских компьютерах, тем не менее огромная инсталляционная базах этих стандартов оставит их еще на некоторое время в поле зрения сетевых интеграторов.

Стандарты Ethernet разработаны комитетом 802.3, а стандарты Token Ring - комитетом 802.5 института IEEE.

Поскольку информация о стандартах Ethernet и Token Ring является широкодоступной, далее приводится обзор основных правил и ограничений, действующих при создании базовых сегментов Ethernet и Token Ring. Под базовыми в данном случае понимаются сегменты, которые строятся только с помощью сетевых адаптеров, кабелей и концентраторов-повторителей.

Основные характеристики протокола Ethernet

• Битовая скорость: 10 Мб/с.

• Максимальный размер поля данных кадра: 1500 байтов.

• Минимальный размер поля данных кадра: 46 байтов.

• Полезная производительность для кадров максимальной длины: 9.74 Мб/с (1.22 Мбайт/с, 812 кадров/с).

• Полезная производительность для кадров минимальной длины: 5.48 Мб/с (684 Кбайт/с, 14880 кадров/с).

• Тип протокола – дейтаграммный.

• Методы и кадры самотестирования – отсутствуют.

• Задержки доступа к среде резко возрастают при коэффициенте загрузки канала 30% и выше.

<u>Правила построения сегментов Ethernet</u>

Ethernet 10Base-5

Базовая топология сети, состоящей из двух сегментов, соединенных повторителем, показана на рисунке 16.1.

• Сегменты Ethernet спецификации 10Base-5 строятся на основе коаксиального кабеля RG-6, называемого часто "толстым" коаксиалом.

• Общее количество станций в сети: 1024.

• Максимальное количество станций, подключенных к одному сегменту: 100.

• Максимальная длина одного сегмента: 500 м.

• Максимальная долина сети (максимальное расстояние между двумя станциями): 2500 м.

• Максимальное количество повторителей между двумя любыми станциями: 4.

• Максимальная длина кабеля между трансивером (приемопередатчиком) и сетевым адаптером: 50 м.

Ethernet 10Base-2

Базовая топология сети аналогична сети 10Base-5 за исключением того, что трансиверы совмещены с сетевыми адаптерами.

• Сегменты Ethernet спецификации 10Base-2 строятся на основе коаксиального кабеля RG-58 C/U, называемого часто "тонким" коаксиалом.

• Общее количество станций в сети: 1024.

• Максимальное количество станций, подключенных к одному сегменту: 30.

• Максимальная длина одного сегмента: 185 м.

• Максимальная длина сети: 2500 м.

• Максимальное количество повторителей между двумя любыми станциями: 4.

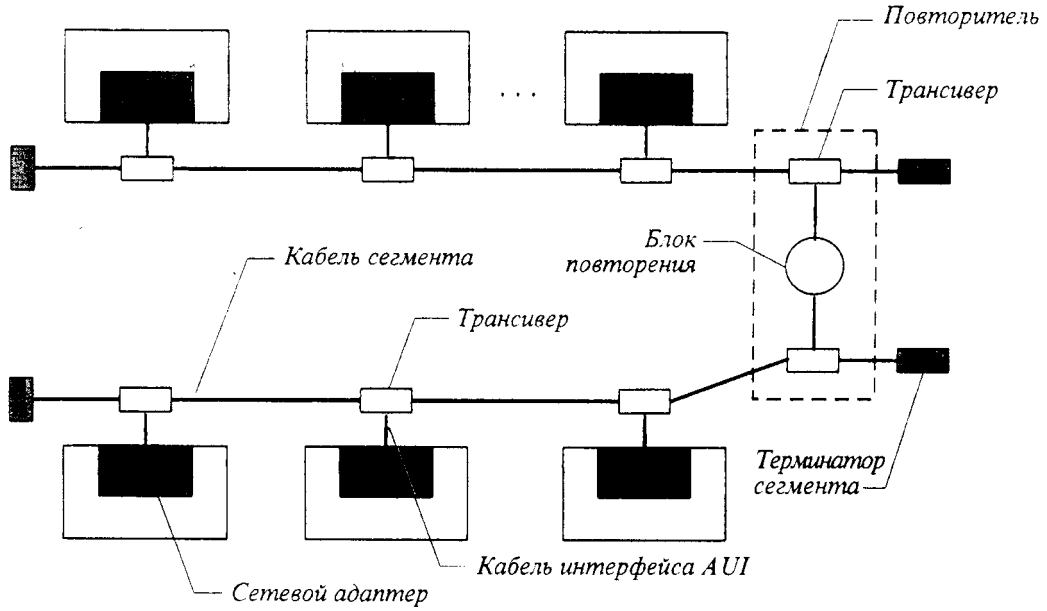


Рис. 16. 1. Компоненты физического уровня сети стандарта 10 Base-5, состоящей из двух сегментов.

Ethernet 10Base-T

Базовая топология сети включает как обязательный элемент многопортовый концентратор-повторитель (рисунок 16.2).

• Сегменты Ethernet спецификации 10Base-T строятся на основе двухпарного кабеля на основе неэкранированной витой пары с волновым сопротивлением 100 Ом категорий 3,4 или 5.

• Общее количество станций в сети: 1024.

• Максимальное количество станций, подключенных к одному концентратору: 1024.

• Максимальная длина кабеля от станции до концентратора: 100 м.

• Максимальная длина кабеля между концентраторами: 100 м.

• Максимальная длина сети: 2500 м.

• Максимальное количество повторителей между двумя любыми станциями: 4.

Ethernet FOIRL, 10Base-FL, 10Base-FB

Стандарт FOIRL (Fiber Optic Inter-Repeater Link) - это первый стандарт комитета 802.3 для использования оптоволокна в сетях Ethernet.

Стандарт 10Base-FL (Fiber Link) предназначен для соединения конечных узлов с концентратором.

Стандарт 10Base-FB (Fiber Backbone) предназначен для магистрального соединения концентраторов.

Базовая топология этих сетей аналогична топологии сети 10Base-T.

• Сегменты Ethernet стандартов FOIRL, 10Base-FL и 10Base-FB строятся на основе двухжильного оптоволоконного кабеля.

• Общее количество станций в сети: 1024.

• Максимальное количество станций, подключенных к одному концентратору: 1024.

• Максимальная длина одного сегмента: FOIRL: до 1000м, 10Base-FL: до 2000м, 10Base-FB: до 2000м (до 4000м у некоторых производителей).

• Максимальная длина сети: FOIRL, 10Base-FL: 2500 м, 10Base-FB: 2740м.

• Максимальное количество повторителей между двумя любыми станциями: FOIRL, 10Base-FL: 4, 10Base-FB: 5.

• Стандарт 10Base-FB поддерживает автоматический переход на резервные связи за счет постоянного тестирования кабелей специальными сигналами.

Основные характеристики протокола Token Ring.

• Битовая скорость: 4/16 Мб/с.

• Максимальный размер поля данных кадра: 16 Кбайт.

• Минимальный размер поля данных кадра: 0 байтов.

• Полезная производительность для кадров максимальной дайны: около 15 Мб/с.

• Тип протокола - дейтаграммный с подтверждением доставки.

• Методы и кадры самотестирования – имеются.

• Возможна приоритетная обработка трафика.

• Задержки доступа к среде резко возрастают при коэффициенте загрузки канала: 60% и выше - для скорости 4 Мб/с, 80% и выше - для скорости 16 Мб/с.

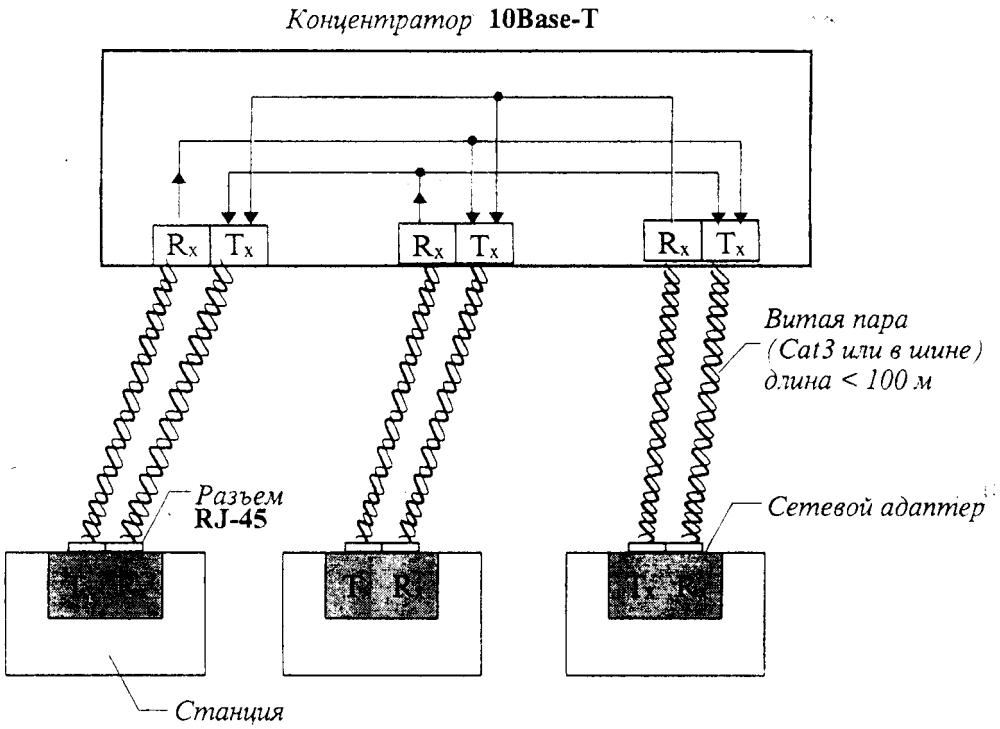


Рис. 16.2. Сеть 10Base-T- один домен коллизий.
T - передатчик, R - приемник

Правила построения сегментов Token Ring 4/16.

Стандарт Token Ring фирмы IBM предусматривает построение связей в сети как с помощью непосредственного соединения станций друг с другом, так и путем образования кольца с помощью концентраторов (называемых MAU - Media Attachment Unit или MSAU - Multi-Station Access Unit).

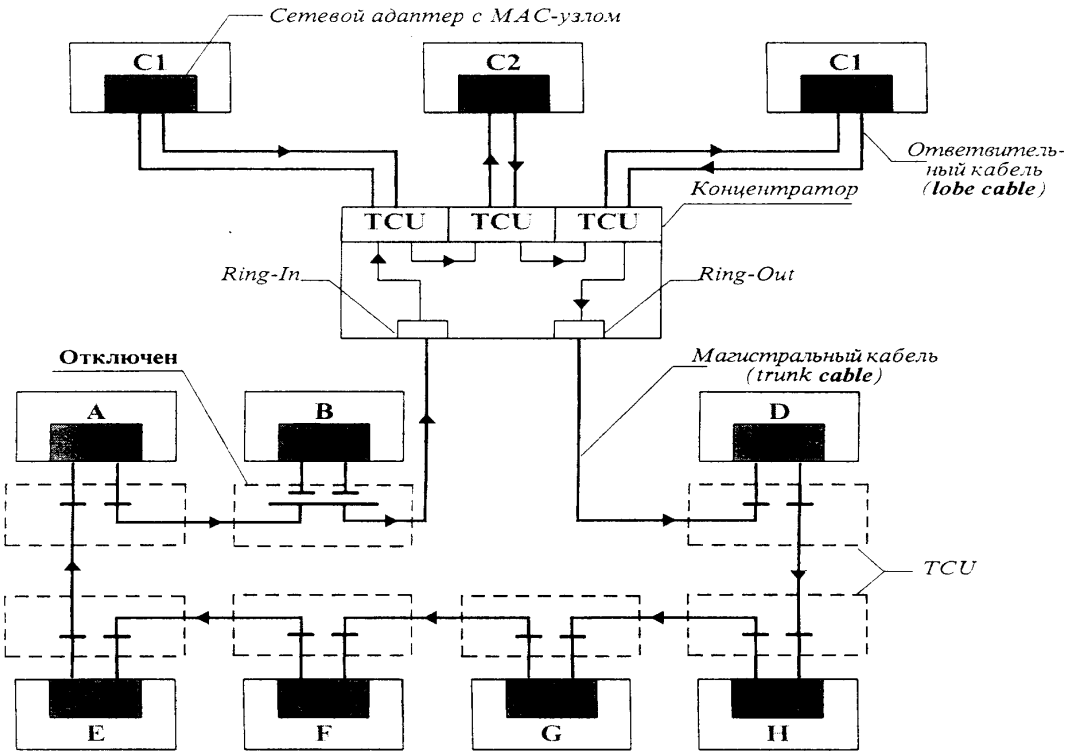
На рисунке 16.3 показаны основные аппаратные элементы сети Token Ring и способы их соединения.

В приведенной конфигурации показаны станции двух типов.

Станции С1, С2 и С3 - это станции, подключаемые к кольцу через концентратор. Обычно такими станциями являются компьютеры с установленными в них сетевыми адаптерами. Станции этого типа соединяются с концентратором ответвительным кабелем (lobe cable), который обычно является экранированной витой парой (Shielded Twisted Pair, STP), соответствующей стандартному типу кабеля из кабельной системы IBM (Type 1,2,6,8.9), или двужильным многомодовым оптоволоконным кабелем.

Концентраторы Token Ring делятся на активные и пассивные. *Пассивные концентраторы* обеспечивают только соединения портов внутри концентратора в кольцо, а активные выполняют и функции повторителя, обеспечивая ресинхронизацию сигналов и исправление их амплитуды и формы. Естественно, что *активные концентраторы* поддерживают большие расстояния до станции, чем пассивные.

Остальные станции сети соединены в кольцо непосредственными связями. Такие связи называются магистральными (trunk cable). Обычно связи такого рода используются для соединения концентраторов друг с другом для образования общего кольца. Порты концентраторов, предназначенные для такого соединения, называются портами Ring-In и Ring-Out.



С 1, С2, С3 - *станции, подключенные к концентратору*

A, B, D, E, F, C, H - *станции, непосредственно подключенные к кольцу*

Рис. 16.3. Конфигурация кольца Token Ring.

TCU (trunk coupling unit) - устройство подключения к магистрали.

Для предотвращения влияния отказавшей или отключенной станции на работу кольца, станции подключаются к магистрали кольца через специальные устройства, называемые устройствами подключения к магистрали (Trunk Coupling Unit, TCU).

В функции такого устройства входит образование обходного пути, исключающего заход магистрали в MAC-узел станции при ее отключении или отказе. Обычно для этих целей в TCU используются реле, которые подпитываются постоянным током во время нормальной работы. При пропадании тока подпитки контакты реле переключаются и образуют обходной путь, исключая станцию.

При подключении станции в кольцо через концентратор, устройства TCU встраивают в порты концентратора.

Существуют сетевые адаптеры и концентраторы Token Ring, которые кроме экранированной витой пары и оптоволокна поддерживают неэкранированную витую пару.

Сети Token Ring работают с двумя битовыми скоростями - 4 Мб/с и 16 Мб/с. Первая скорость определена в стандарте 802.5, а вторая является новым стандартом де-факто, появившимся в результате развития технологии Token Ring, Смешение станций, работающих на различных скоростях, в одном кольце не допускается.

Сети Token Ring. работающие со скоростью 16 Мб/с, имеют и некоторые усовершенствования в алгоритме доступа по сравнению со стандартом 4 Мб/с.

<u>Правила построения сегментов Token Ring:</u>

• Максимальный диаметр сети: 1000 м для STP,

• Максимальное расстояние между узлами: 100 м (UTP, STP), 2000 м для оптоволокна,

• Максимальное количество станций в кольце: 260 (STP), 144 (UTP).

16.1.2. Локальные сети на быстрых протоколах: FDDI, Fast Ethernet и 100VG-AnyLAN.

В современной сети невозможно обойтись без быстрых протоколов. Даже на уровне клиентских персональных компьютеров существует большое количество приложений, которые не устраивает пропускная способность в 1.2 Мбайт/с, которую может предоставить обычный Ethernet, и даже пропускная способность в 1.8 Мбайт/с, которую может предоставить технология Token Ring. Примерами служат мультимедийные приложения, которые работают со статическими мегабайтными файлами изображений и звука, или же приложения организации видеоконференций, которые обрабатывают мультимедийную информацию в реальном времени. Кроме того, в начале 90-х годов пропускная способность подсистемы ввода-вывода превысила возможности сетевых адаптеров Ethernet и Token Ring, создавая предпосылки для использования более скоростных протоколов на уровне персональных компьютеров.

Еще более остро ощущается потребность в скоростных протоколах на магистральных каналах корпоративных сетей, где суммируется трафик отдельных рабочих групп и отделов,

Желательно, чтобы помимо скорости такие протоколы обладали еще и несколькими дополнительными свойствами:

• обеспечивали приоритетную обработку синхронного мультимедийного трафика.

• предоставляли некоторые гарантии по величине пропускной способности, предоставляемой конкретному соединению,

• работали в различных средах передачи данных, поддерживая более дешевые соединения на коротких расстояниях и обеспечивая связи в пределах кампуса или города на оптоволокне,

• обеспечивали самотестирование кабельных связей и поддерживали автоматический переход на резервные связи в случае отказа основных,

• поддерживали иерархию скоростей, что позволяет использовать один и тот же протокол на разных уровнях иерархии транспортной системы корпоративной сети.

Сегодня имеется несколько скоростных протоколов, которые можно использовать в локальных сетях: FDDI, Fast Ethernet, 100VG-AnyLAN и ATM.

Технология ATM в наибольшей степени удовлетворяет перечисленным выше требованиям, но она одновременно является и наиболее далекой от окончательного оформления в виде серии стандартов. Ввиду того, что у ATM очень много общего с технологиями глобальных сетей, эта технология будет рассмотрена после раздела, посвященного глобальным сетям.

Стандарт FDDI.

Высокоскоростной протокол FDDI (Fiber Distributed Data Interface) - оптоволоконный интерфейс распределенных данных - появился значительно раньше, чем Fast Ethernet и 100Vg-AnyLAN. Сейчас это наиболее отработанный высокоскоростной стандарт, который применяется на магистралях сетей кампусов и даже сетей масштаба города.

Проблемная группа X3T9.5 института ANSI разработала стандарт FDDI, который обеспечивает передачу кадров по двойному волоконно-оптического кольцу со скоростью *100 Мб/с.* Протокол специально разрабатывался, чтобы быть как можно больше похожим на стандарты Token Ring и IEEE 802,5, и отличаться от них только теми особенностями, которые необходимы для поддержки большей скорости и больших расстояний.

Основные характеристики протокола FDDI:

• Битовая скорость: 100 Мб/с,

• Максимальный размер пакета: около 4 Кбайт,

• Высокая отказоустойчивость,

• Собственный протокол управления кольцом – SMT.

Базовая топология кольца FDDI показана на рисунке 16.4.

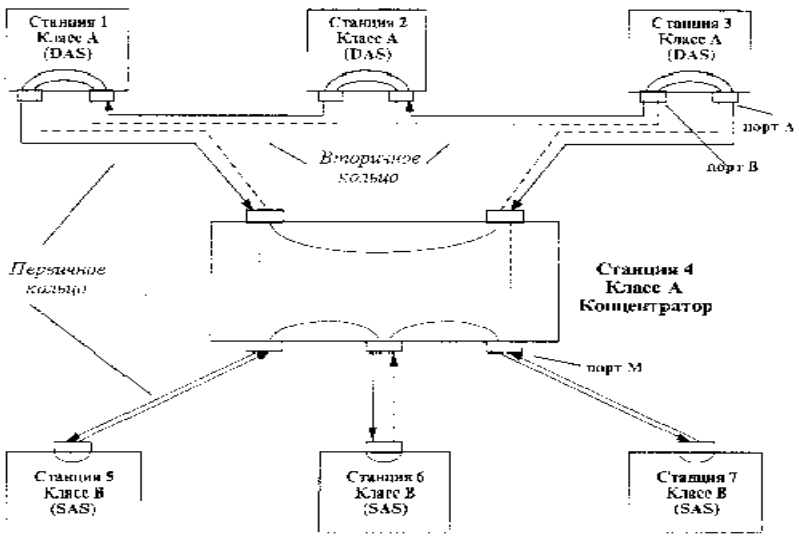


Рис. 16.4. Кольца стандарта FDDI

Правила построения кольца FDDI.

• Максимальные расстояния между станциями:

до 2 км - многомодовый оптоволоконный кабель,
20-60 км (конкретное предельное значение зависит от используемого оборудования) - одномодовый оптоволоконный кабель,
до 100 м - неэкранированная витая пара категории 5 (подстандарт TP-PMD).

• Максимальная общая длина кольца FDDI составляет 100 километров.

• Максимальное число станций класса А в кольце – 500.

• Передача информации происходит по первичному кольцу, вторичное кольцо используется как резервное.

Поддержка мультимедийного трафика.

Протокол FDDI использует алгоритм для управления доступом к сети, основанный на таймерных интервалах. В стандарте FDDI различаются асинхронные (обычные) пакеты и синхронные - пакеты multimedia, например, пакеты с кодами изображений, которые должны передаваться через строго фиксированные интервалы времени. Каждая станция кольца FDDI учитывает три различных таймерных интервала:

• TRT - интервал между двумя последовательными приходами маркера;

• T - фиксированный интервал, о котором станции договорились при инсталляции:

• THT - время удержания маркера - время, в течение которого станция может удерживать маркер и передавать свои пакеты.

Интервал THT вычисляется по формуле: THT = T - TRT, из которой видно, что чем дольше маркер совершает оборот, тем меньше станции остается времени на передачу своих пакетов. Если THT становится отрицательным, то станция не передает свои пакеты, а передает только маркер. Условие передачи пакета относится только к асинхронным пакетам. Синхронный пакет передается всегда.
Структура кадра данных сети FDDI соответствует структуре кадра данных сети Token Ring, а структура маркера FDDI значительно отличается.

Отказоустойчивость FDDI.

Для обеспечения отказоустойчивости в стандарте FDDI предусмотрено создание двух оптоволоконных колец. При разрыве связей между двумя станциями в первичном кольце происходит использование связей вторичного кольца, причем передача информации во вторичном кольце происходит в обратном направлении (рисунок 16.4). При отказе или отключении какой-либо станции ее сетевой адаптер должен обеспечить обходной путь. В стандарте FDDI допускается использование двух видов подсоединения станций к кольцу. Станции класса А подключаются к первичному и вторичному кольцам и называются DAS или DAC- *Dual Attachment Station* или *Dual Attachment Concentrator* в зависимости от того, представляет ли станция конечный узел (компьютер) или концентратор. Станции класса В подключаются только к первичному, основному кольцу и называются SAS - *Single Attached Station.* Обычно рабочая станция является узлом с одиночными связями, а концентратор - узлом с дуальными связями.

В случае однократного обрыва кабеля можно предусмотреть автоматическую реконфигурацию кольца за счет переключения связей в концентраторе (рисунок 16.5).

Если вышла из строя или была выключена станция класса А, то кольцо FDDI может сохранить работоспособность путем использования обходных оптических переключателей.

И, наконец, станции класса В можно подключать сразу к двум концентраторам, в результате чего образуется основная и резервная связи. Такой способ подключения называется *Dual Homing.*

Управление в сетях FDDI.

Стандарт FDDI определяет собственный протокол наблюдения и управления сетью - протокол SMT. Он отличается от протокола SNMP, обычно используемого для
управления сетями, поэтому для управления FDDI-устройствами с помощью стандартных систем и платформ, основанных на протоколе SNMP, необходимы агенты-посредники (proxy agents), транслирующие протокол SMT в протокол SNMP.

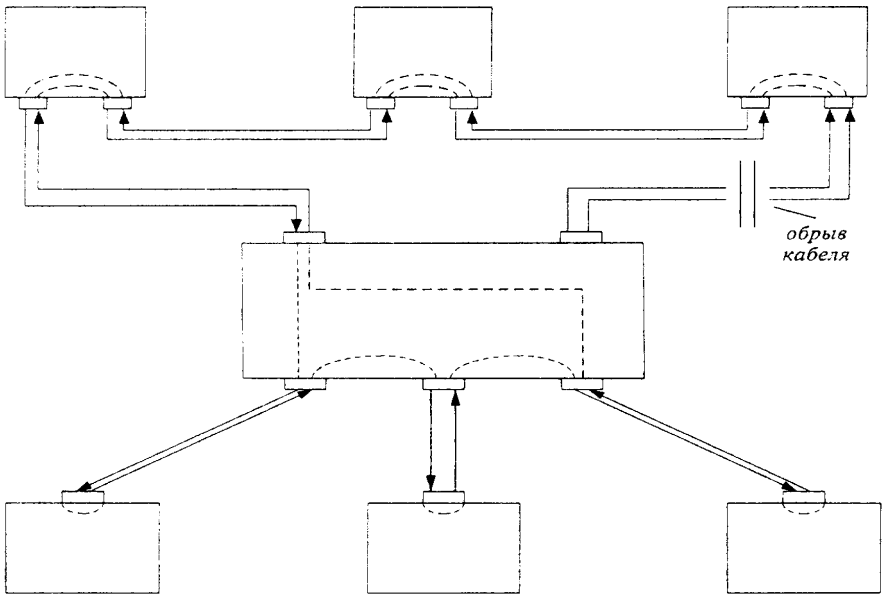


Рис .16.5. Отказоустойчивость колец FDDI

Стандарт Fast Ethernet.

В то время, как переход на FDDI требует не только замены всего сетевого оборудования. но и полного переучивания пользователей, усовершенствованные технологии Ethernet и Token Ring предлагают более безболезненный путь перехода к быстрым сетям. Наибольшее число сторонников завоевал сравнительно новый высокоскоростной стандарт *Fast Ethernet Alliance,* который был предложен в августе 1993 года группой из 10 производителей, включая 3Com, Grand Junction Networks, Intel, Racal Datacorn и Syn-Optics. Стандарт принят комитетом IEEE 802.3 летом 1995 года. В настоящее время оборудование Fast Ethernet выпускают около 120 производителей.

Стандарт Fast Ethernet оставляет неизменным MAC-уровень Ethernet, сохраняя метод доступа, размер и формат пакета, что позволяет использовать прежнее программное обеспечение и средства управления сетями Ethernet.

Однако для поддержки передачи данных со скоростью 100 Мб/с требуется модификация физического уровня. Существуют два конкурирующих и несовместимых варианта реализации физического уровня:

• *Метод 100Base-T/X* основан на использования разных сред передачи: двух неэкранированных витых пар высокого качества (категории 5), двух

экранированных витых пар или многомодового оптоволоконного кабеля. Из-за высокой тактовой частоты в этом варианте нельзя использовать неэкранированную витую пару категории 3 или 4, стандартную для сетей 10Base-T.

• Предложенный позднее *метод 100Base-T4* допускает применение четырех более дешевых неэкранированных витых пар (категории 3, 4, или 5). Производители,
входящие в Fast Ethernet Alliance, разрабатывают продукты, поддерживающие обе спецификации. Из четырех неэкранированных пар, необходимых для метода 100Base-
T, три пары используются для передачи данных, а четвертая - для разрешения конфликтов. Вместо манчестерского кодирования, применяемого в традиционной технологии Ethernet, в 100Base-T используется схема кодирования 8B6T, которая преобразует группы из 8 битов в один из шести троичных (то есть принимающих не два, а три различных состояния) сигналов, распределяемых по четырем парам проводов.

Для поддержки различных стандартов физического уровня в стандарте Fast Ethernet выделены специальные подуровни, показанные на рисунке 16.6. На этом же рисунке приводится для сравнения структура физического уровня стандарта 10Base-T - предшественника стандарта Fast Ethernet. Для обеспечения независимости MAC-уровня от способа кодирования сигнала, верхнюю часть физического уровня составляет подуровень согласования (Reconciliation Sublayer, RS), который преобразует абстрактные сообщения MAC-уровня в конкретный физический код - последовательность полубайтов (nibble-wide chunks или дословно кусочки). На выходе подуровня согласования образуется независимый от среды интерфейс Mil (Media Independent Interface), который можно считать аналогом интерфейса AUI стандартов обычного Ethernet'a.

Далее расположены подуровни, зависящие от конкретной реализации физической среды. Подуровень физического кодирования (Physical Coding Sublayer, PCS) стандарта 100Base-TX преобразует полубайты интерфейса Mil в последовательности из 5 битов в соответствии с кодировкой 4B/5B, а подуровень PCS стандарта 100Base-T4 преобразует байт в 6 элементов, каждый из которых может принимать 3 значения.

Далее закодированные сигналы передаются в блок управления передачей по среде, который собственно и осуществляет передачу сигналов по кабелю с помощью зависящего от среды интерфейса MDI (Media Dependent Interface), который для неэкранированной витой пары представляет собой разъем RJ-45 с соответствующим назначением контактов. Станция стандарта 100Base-T4 всегда использует одну пару из четырех для приема сигналов, являющуюся входом приемника - Rx.

Эта пара необходима для распознавания станцией коллизии. Вторая пара всегда используется для передачи данных и связана с выходом передатчика - Tx. Эти пары соответствуют и по назначению и по разводке контактов назначению пар стандарта 10Base-T и 100Base-TX.

Остальные две пары могут использоваться как для приема, так и для передачи. В результате станции стандарта 100Base-T4 всегда обмениваются данными параллельно по трем парам проводов. При передаче кода 8B6T используется тактовая частота 25 МГц, что совместно с ускорением. достигаемым за счет кодирования 8B6T, дает на трех параллельных линиях пропускную способность 100 Мб/с.

Базовая топология сегмента стандарта Fast Ethernet приведена на рисунке 16.7

Для стандартов 100Base-T4 и 100Base-TX имеются следующие ограничения на конфигурацию сети: максимальная длина сети - 210 м. причем допускается использование не более двух концентраторов-повторителей, расстояние между которыми не должно превышать 10 м, Максимальное расстояние между концентратором и станциями - 100 м.

Существует также вариант стандарта 100Base-FX, использующий два оптоволокна доя соединения станции с концентратором. Максимальное расстояние от конечной станции до концентратора при этом увеличивается до 185 м.

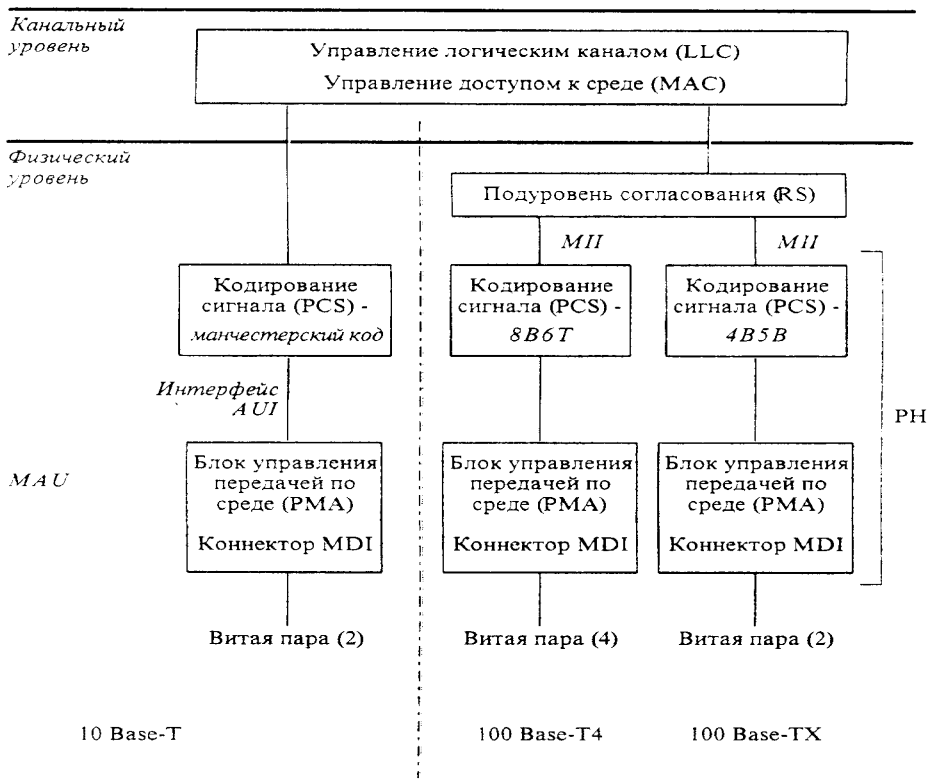


Рис. 16.6. Структура физического уровня стандарта Fast Ethernet

<u>Стандарт 100VG-Any LAN.</u>

В качестве альтернативы 100Base-T фирмы AT&T и HP выдвинули проект 100Base-VG. изменяющий уровень MAC, но сохраняющий размер пакета Ethernet, В сентябре 1993 года фирмы IBM и HP образовали комитет IEEE 802.12 и предложили использовать эту технологию для повышения скорости в сети Token Ring. Эта технология была названа 100VG-AnyLAN. В ней определены новый метод доступа Demand Priority и новая схема квартетного кодирования Quartet Coding – самосинхронизирующийся код 5B6B.

100VG-AnyLAN поддерживает передачу данных по четырем неэкранированным витым парам категорий 3, 4, 5. Данные передаются одновременно по четырем парам со скоростью 25 Мб/с, что в сумме дает 100 Мб/с.

Сеть 100VG-AnyLAN состоит из центрального коммутирующего

концентратора, называемого также корневым, и соединенных с ним конечных узлов и других концентраторов. Допускается три уровня каскадирования. Каждый концентратор 100VG-AnyLAN должен быть настроен либо на работу с кадрами Ethernet, либо Token Ring, причем все концентраторы в сети должны быть настроены на один и тот же тип кадра. Специальное программное обеспечение концентратора 100VG-AnyLAN позволяет установить мост с низкоскоростной сетью Ethernet или Token Ring в зависимости от типа высокоскоростной сети. Фирмы IBM и HP объявили, что идет

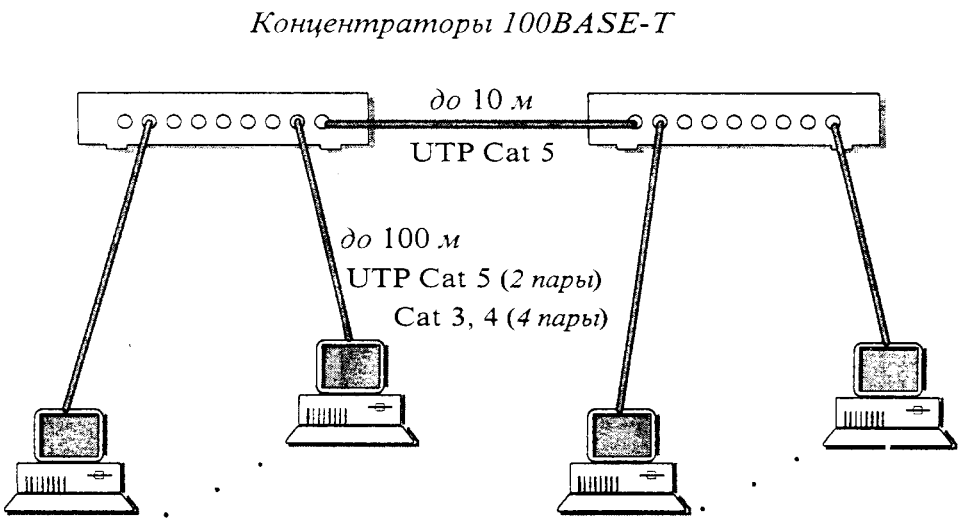


Рис. 16.7. Структура сети 100Base-T

разработка метода, позволяющего обрабатывать в одном устройстве кадры обоих типов одновременно.

Рисунок 16.8 иллюстрирует работу протокола Demand Priority.

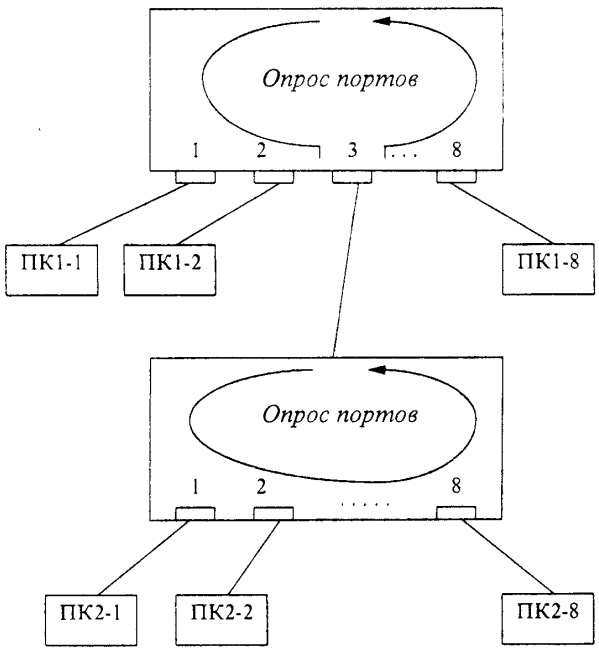


Рис. 16.8. Протокол Demand Priority стандарта 100VG-AnyLAN.

Согласно этому методу концентратор циклически выполняет опрос портов. Станция, желающая передать пакет, посылает низкочастотный сигнал концентратору, запрашивая низкий приоритет для обычных данных и высокий приоритет для данных, чувствительных к временным задержкам (например, мультимедиа). Приоритеты запросов имеют статическую и динамическую составляющие. Если сеть свободна, концентратор разрешает передачу пакета. После анализа адреса получателя в принятом пакете концентратор автоматически отправляет пакет станции назначения. Если сеть занята, концентратор ставит полученный запрос в очередь, которая обрабатывается в соответствии с порядком поступления запросов и с учетом приоритетов. Если к порту подключен другой концентратор, то опрос приостанавливается до завершения опроса концентратором нижнего уровня.

Важная особенность метода Demand Priority - сохранение форматов кадров Ethernet и Token Ring. Сторонники 100VG-AnyLAN утверждают, что этот подход облегчит межсетевое взаимодействие через мосты и маршрутизаторы, а также обеспечит совместимость с существующими средствами сетевого управления, в частности, с анализаторами протоколов.

Основное применение технология 100VG-AnyLAN скорее всего найдет в сетях Token Ring, пользователям которых она позволит в 6-25 раз увеличить производительность сети, а также в сетях, активно использующих приложения мультимедиа.

Из-за изменения метода доступа эффективная пропускная способность сети 100VG-AnyLAN примерно в 1.5 раза выше пропускной способности сети Fast Ethernet.

Базовая топология сегмента сети 100VG-AnyLAN показана на рисунке 16.9.

Лекция .2. Кабельные системы для локальных сетей.

16.2.1. Концепция и преимущества структурированной кабельной системы.

Как уже отмечалось, структурированность - это неотъемлемая черта сети и на физическом уровне это свойство выражается в структурированности кабельной системы.

Согласно зарубежным исследованиям (журнал LAN Technologies) 70% времени простоев обусловлено проблемами, возникшими вследствие низкого качества применяемых кабельных систем. Поэтому так важно правильно построить фундамент сети - структурированную кабельную систему.

Структурированная кабельная система (Structured Cabling System, SCS) - это набор коммутационных элементов (кабелей, разъемов, коннекторов, кроссовых панелей и шкафов), а также методика их совместного использования, которая позволяет создавать регулярные, легко расширяемые структуры связей в вычислительных сетях.

Рассмотренные в предыдущих разделах протоколы нижних уровней транспортной подсистемы и базовые топологии физических связей в сегментах локальных сетей, в которых реализуются эти протоколы, позволяют сделать вывод: между различными стандартами есть много общего по отношению к используемой физической основе сети - кабельной системе. Большинство стандартов, как старых, так и новых, использует три основных типа кабелей - неэкранированную витую пару (UTP), экранированную витую пару (STP) и многомодовый оптоволоконный кабель. При этом практически все стандарты используют иерархические древовидные структуры физических связей между конечными станциями и концентраторами, независимо от выполняемых концентраторами функций. Поэтому возможно создание на основе этих видов кабелей такой кабельной системы внутри здания или в пределах комплекса зданий, которую путем перекоммутации кабелей в специальных кроссовых

секциях и шкафах можно было гибко и без больших дополнительных затрат приспосабливать в течение 5 - 10 лет к изменяющейся структуре сети и появляющимся новым протоколам.

Кабельная система такого типа всегда будет обладать некоторой долей избыточности. Так, в каждой комнате здания должно быть разведено достаточное количество оконечных розеток, к которым подключаются сетевые адаптеры компьютеров, даже если в настоящее время в таком количестве розеток и нет необходимости. Эти ненужные розетки могут никуда не подключаться, но быть подведенными к ближайшему кроссовому шкафу, чтобы подключиться к новому концентратору, когда это станет необходимо. Начальная избыточность структурированной кабельной системы окупится достаточно быстро, так как стоимость наращивания кабелей и розеток в действующей кабельной системе всегда выше, чем их установка в период установки всей кабельной системы.

Кроме того, желание получить ясную структуру кабельной системы также приводит к избыточности, так как здесь иногда приходится жертвовать элегантным, но отклоняющимся от общей схемы решением, в пользу избыточного, но единообразного решения.

Преимущества структурированной кабельной системы:

• *Универсальность.* Структурированная кабельная система при продуманной организации может стать единой средой для передачи компьютерных данных в локальной вычислительной сети, организации локальной телефонной сети, передачи видеоинформации и даже передачи сигналов от датчиков пожарной безопасности или охранных систем. Это позволяет автоматизировать многие процессы по контролю, мониторингу и управлению хозяйственными службами и системами жизнеобеспечения.

• *Увеличение срока службы.* Срок морального старения хорошо структурированной кабельной системы может составлять 8-10 лет.

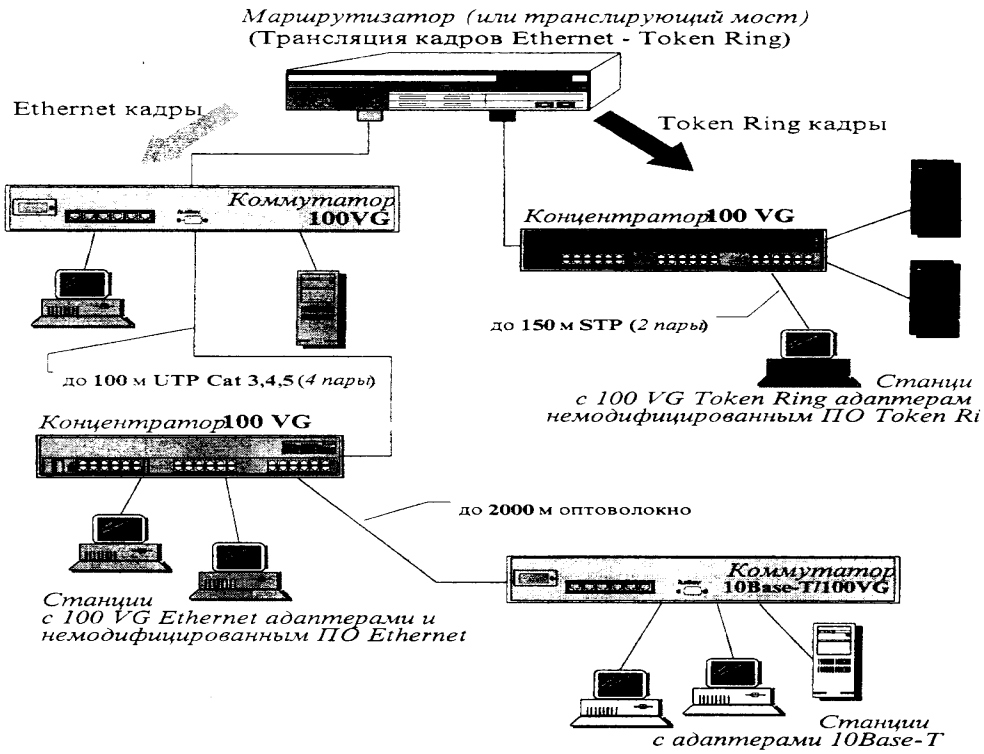


Рис. 16.9. Корпоративная сеть на продуктах 100 VG-AnyLAN

• *Уменьшение стоимости добавления новых пользователей и изменения их мест размещения.* Стоимость кабельной системы в основном определяется не стоимостью

кабеля, а стоимостью работ по его прокладке. Поэтому более выгодно провести однократную работу по прокладке кабеля, возможно с большим запасом по длине, чем несколько раз выполнять прокладку, наращивая длину кабеля. Это помогает быстро и дешево изменять структуру кабельной системы при перемещениях персонала или смене приложений.

• *Возможность легкого расширения сети.* Структурированная кабельная система является модульной, поэтому ее легко наращивать, что позволяет легко и ценой малых затрат переходить на более совершенное оборудование, удовлетворяющее растущим требованиям к системам коммуникаций.

• *Обеспечение более эффективного обслуживания.* Структурированная кабельная система облегчает обслуживание и поиск неисправностей по сравнению с шинной кабельной системой.

• *Надежность.* Структурированная кабельная система имеет повышенную надежность поскольку обычно производство всех ее компонентов и техническое сопровождение осуществляется одной фирмой-производителем.

16.2.2. Выбор кабеля для различных подсистем.

В состав любой кабельной системы входят кабели различных типов, каждый из которых имеет свою область или области назначения. Для определения областей назначения того или иного типа кабеля полезно выделять в кабельной системе отдельные подсистемы. В типичную иерархическую структурированную кабельную систему входят горизонтальные и вертикальные подсистемы, а также подсистема кампуса.

Горизонтальные подсистемы работают в пределах отдела и соединяют кроссовый шкаф этажа с розетками пользователей. Подсистемы этого типа соответствуют этажам здания.

Вертикальные подсистемы работают внутри здания, соединяют кроссовые шкафы каждого этажа с центральной аппаратной здания. *Подсистема кампуса,* работающая в пределах территории между зданиями, соединяет несколько зданий с главной аппаратной всего кампуса. Эта часть кабельной системы обычно называется backbone (или магистралью).

При выборе кабеля для той или иной подсистемы принимаются во внимание следующие его характеристики: полоса пропускания, расстояние, на котором он может работать, защищенность, электромагнитная помехозащищенность, стоимость. Кроме того, при выборе кабеля нужно учитывать, какая кабельная система уже установлена на вашем предприятии, и какие тенденции и перспективы существуют на рынке в данный момент.

Исторически стандарты на различные типы кабелей, которые могут быть применены в локальных вычислительных сетях, разрабатывались различными организациями. Так, стандарты на экранированную витую пару установила компания IBM, разработавшая свою кабельную систему, стандарты на неэкранированную витую пару разрабатывались телефонными компаниями и т. п. В настоящее время принята версия стандарта E1A/T1A 568A, которая определяет основные параметры неэкранированной витой пары 100 0м UTP, экранированной витой пары 150 0м STP и волоконно-оптического кабеля, то есть тех видов кабелей, которые покрывают все разнообразие физических уровней современных стандартов для локальных сетей. Коаксиальный кабель не вошел в этот стандарт, так как он является устаревшим видом носителя, который хотя и можно применять, но не рекомендуется, и отсутствие его в стандарте E1AЛГ1A 568A - аргумент в пользу отказа от коаксиала в новых проектах.

Медный неэкранированный кабель в зависимости от электрических характеристик и производительности разделяют на 5 категорий (или уровней). Кабели категорий 1 и 2 не включены в этот стандарт как не подходящие для передачи данных.

Кабели *1 категории* применяются там, где требования к скорости передачи минимальны, Обычно это кабель для цифровой и аналоговой передачи голоса и низкоскоростной (до 20 кб/с) передачи данных.

Кабели *2 категории* были впервые применены фирмой IBM при построении собственной кабельной системы. Главное требование к кабелям этой категории - способность передавать сигнал с частотой до 1 МГц. Основные приложения второй категории - сети ISDN и низкоскоростная передача данных.

Сводная информация соответствия сетевых стандартов для категорий 3, 4 и 5 приведена в таблице 16.1.

Таблица 16.1

Категория	Кабельные системы	Сетевая среда
Категория 3	UTP до 16 МГц	10Base-T 4 Мб/с Token Ring ARCnet 100VG-AnyLAN 100Base-T4
Категория 4	UTP до 20 МГц	16 Мб/с Token Ring Low loss 10Base-T
Категория 5	UTP, STP до 100МГц	ATM (155 МГц) TP-PMD (CDDI) 100Base-T/X

Необходимо отметить, что стандарт E1A/T1A 568A относится только к сетевому кабелю. Но реальные системы, помимо кабеля, содержат также коннекторы, розетки, распределительные панели и др., т.е. все, что в совокупности составляет понятие кабельной системы. Использование только кабеля типа 5 не гарантирует создание кабельной системы этой категории. Все составные части кабельной системы также должны удовлетворять требованиям соответствующей категории, то есть работать без ухудшения электрических параметров передаваемых сигналов в заданных частотах. Важное значение имеет также технология инсталляции всех компонентов системы, нарушение которой приведет к снижению категории,

В конце 1995 года был принят стандарт TSB-67, который определяет способы сертификации кабельными тестерами коннекторов и проводки из неэкранированной витой пары на соответствие требованиям стандарта E1A/T1A 568A.

Из описанной согласованной схемы стандартов несколько выпадает проверка кабельной проводки категории 5 на возможность использования в сети ATM со скоростью 155 Мб/с, так как указанные стандарты описывают параметры и методику их проверки только до частоты 100 МГц и являются протокольно-независимыми. ATM Forum определил свои требования к качеству сигналов протокола ATM, передаваемых по кабелю категории 5 -это спецификация AF-PHY-0015.000. Такой подход противоречит политике организаций по стандартизации кабельных систем, так как требует сертификации кабельной системы отдельно для каждого применяемого на ней протокола. Тем не менее некоторые производителя. в частности компания Scope Communications (продукт WireScope 155), выпустили кабельные тестеры для проверки возможности работы протокола ATM на скорости 155 Мб/с на конкретном кабеле.

Большинство проектировщиков начинают разработку структурированной кабельной системы с разработки *горизонтальных подсистем,* так как именно к ним подключаются конечные пользователи. При этом они могут выбирать между:

- экранированной витой парой,
- неэкранированной витой парой,

• коаксиальным кабелем,
• волоконно-оптическим кабелем,
• беспроводной связью.

Общим правилом является использование в горизонтальных подсистемах неэкранированной витой пары. За рубежом во многих зданиях имеется неиспользуемая телефонная проводка витой пары. Неэкранированная витая пара поддерживает протоколы Local-Talk, Ethernet, Token Ring, ArcNet, FDDI.

После принятия стандарта 10Base-T количество узлов, использующих неэкранированную витую пару, быстро превзошло количество узлов на коаксиальном кабеле.

Экранированная витая пара по характеристикам полосы пропускания и расстояния также подходит для создания горизонтальных подсистем. Но, так как, неэкранированная витая пара может передавать данные и голос, то она используется чаще. Экранированная витая пара используется для связи в сетях, базирующихся на продуктах IBM и Token Ring.

Коаксиальный кабель - это устаревшая технология, которую следует избегать, если только она уже широко не используется на вашем предприятии. До 1991 года в мире большая часть сетевых узлов использовала тонкий или толстый коаксиальный кабель. После принятия в 1991 году стандарта 10Base-T произошло резкое увеличение числа использований витой пары. Однако коаксиальный кабель все еще остается одним из возможных вариантов кабеля для горизонтальных подсистем. Особенно в случаях, когда высокий уровень электромагнитных помех не позволяет использовать витую пару.

Сети, использующие тонкий Ethernet, можно быстро собрать, так как компьютеры непосредственно соединяются друг с другом. До появления стандарта 10Base-T тонкий Ethernet был основным кабелем для горизонтальных подсистем. Главный недостаток тонкого Ethernet'a - сложность его обслуживания. Каждый конец кабеля должен завершаться терминатором 50 0м. При отсутствии терминатора или утере им своих рабочих свойств (например, из-за отсутствия контакта) перестает работать весь сегмент сети, подключенный к этому кабелю. Аналогичные последствия имеет плохое соединение любой рабочей станции (осуществляемое через Т-коннектор).

Неисправности в сетях на тонком Ethernet'e сложно локализовать. Часто приходится отсоединять Т-коннектор от сетевого адаптера, тестировать кабельный сегмент и затем последовательно повторять эту процедуру для всех присоединенных узлов. Поэтому стоимость эксплуатации сети на тонком Ethernet'e обычно значительно превосходит стоимость эксплуатации сетей на витой паре, хотя материальные затраты на кабельную систему для тонкого Ethernet'a обычно ниже.

Хотя основное назначение оптического кабеля - это вертикальная подсистема и подсистемы кампусов, волоконно-оптический кабель может использоваться и в горизонтальных подсистемах. Это происходит в тех случаях, когда нужна высокая степень защищенности данных, высокая пропускная способность, устойчивость к электромагнитным помехам или, если кабельная система прокладывается в агрессивной среде. Стоимость установки сетей, которые используют оптоволоконный кабель для горизонтальной подсистемы, оказывается весьма высокой. Эта стоимость складывается из стоимости сетевых адаптеров (2-3 тысячи долларов каждый) и из стоимости монтажных работ, которая в случае оптоволокна гораздо выше, чем при работе с другими видами кабеля (примерно 200 долларов на подвод к одному рабочему месту). С волоконно-оптическим кабелем работают протоколы AppleTalk, ArcNet, Ethernet, FDDI и Token Ring, а также новые протоколы 100VG-AnyLAN, Fast Ethernet, ATM.

Беспроводная связь является новой и многообещающей технологией, однако

из-за сравнительной новизны ее лучше использовать в ограниченных масштабах для неответственных применений.

Кабель, передающий данные в *вертикальной (или магистральной) подсистеме,* должен передавать данные на большие расстояния и с большей скоростью по сравнению с кабелем горизонтальной подсистемы. В прошлом основным видом кабеля для вертикальных подсистем был коаксиальный кабель. Теперь для этой цели все чаще используется оптоволоконный кабель.

Для вертикальной подсистемы выбор кабеля в настоящее время ограничивается тремя вариантами:

- оптоволокно,
- толстый коаксиал,
- широкополосный кабель.

Применение *волоконно-оптического кабеля* в вертикальной подсистеме имеет ряд преимуществ.

Он передает данные на значительно большие расстояния без необходимости регенерации сигнала. Он имеет сердечник меньшего диаметра, поэтому может быть проложен в более узких местах. Так как передаваемые по нему сигналы являются световыми, а не электрическими, то оптоволоконный кабель не чувствителен к электромагнитным и радиочастотным помехам, в отличие от медного коаксиального кабеля. Это делает оптоволоконный кабель идеальной средой передачи данных для сетей, работающих в промышленности. Оптоволоконному кабелю не страшна молния, поэтому он хорош для внешней прокладки. Он обеспечивает более высокую степень защиты от несанкционированного доступа, так как ответвление гораздо более легко обнаружить, чем в случае медного кабеля. (При ответвлении резко уменьшается интенсивность света.)

Оптоволоконный кабель имеет и недостатки. Он гораздо дороже чем, медный кабель, дороже обходится и его прокладка. Оптоволоконный кабель менее прочный, чем коаксиальный. Инструменты, применяемые при прокладке и тестировании оптоволоконного кабеля, имеют высокую стоимость и сложны в работе. Присоединение коннекторов к оптоволоконному кабелю требует большого искусства и времени, а, следовательно, и денег.

Толстый коаксиальный кабель также может использоваться в качестве позвоночника сети, однако для новых кабельных систем более рационально использовать оптоволоконный кабель, так как он имеет больший срок службы и сможет в будущем поддерживать высокоскоростные и мультимедийные приложения. Но для уже существующих систем толстый коаксиальный кабель служил многие годы позвоночником системы, и с этим нужно считаться. Причинами его широкого использования были его широкая полоса пропускания, хорошая защищенность от электромагнитных помех и низкое радиоизлучение.

Хотя толстый коаксиальный кабель и дешевле, чем оптоволокно, но с ним еще более сложно работать. Он особенно чувствителен к различным уровням напряжения заземления, что часто бывает при переходе от одного этажа к другому.

Для *подсистемы кампуса,* объединяющей несколько зданий, расположенных в радиусе нескольких километров, также как и для вертикальных подсистем, оптоволоконный кабель является наилучшим выбором. Для этой подсистемы также подходят толстый коаксиальный кабель и широкополосный кабель.

При выборе кабеля для кампуса нужно учитывать воздействие среды на кабель вне помещения. Для предотвращения поражения молнией лучше выбрать для внешней проводки неметаллический оптоволоконный кабель. По многим причинам внешний кабель производится в полиэтиленовой защитной оболочке высокой плотности. При подземной прокладке кабель должен иметь специальную влагозащитную оболочку (от дождя и подземной влаги), а также металлический защитный слой от грызунов и вандалов. Влагозащитный кабель имеет прослойку из инертного газа между диэлектриком, экраном и внешней оболочкой.

16.2.3. Примеры промышленных структурированных кабельных систем

К числу наиболее распространенных структурированных кабельных систем относятся кабельная система, разработанная компанией IBM, Cabling System, AT&T - Premises Distributed System и SYSTIMAX, а также кабельная система корпорации Digital Equipment -OPEN DECconnect. Различные производители дают своим кабельным системам различные названия, но общие принципы их организации остаются одинаковыми.

Первая из них служит для объединения в единую систему разнообразной сетевой продукции компании IBM (включая сети Token Ring) и использует широкий диапазон типов кабелей (коаксиальный, твинаксиальный, экранированную и неэкранированную витые пары). В результате, если после начальной установки кабельной системы изменить тип используемого оборудования, то может потребоваться замена кабельной системы. Этого можно избежать, установив сразу все типы наиболее используемых кабелей для разных типов оборудования. Кабельная система имеет топологию "звезда" и может использоваться также для связи терминального оборудования (например, Wang) и построения сетей, отличных от Token Ring (например, Ethernet).

OPEN DECconnect представляет собой структурированную кабельную систему, поддерживающую широкий спектр приложений: FDDI, Ethernet, 4- и 16-мегабитный Token Ring, ISDN, AS400, AppleTalk и многие другие.

В этой системе также применена топология "звезда" и три типа кабелей: оптоволоконный, экранированная и неэкранированная витые пары. Витая пара применяется для организации средне- и низкоскоростных каналов данных (до 16 Мб/с) на коротких расстояниях. Для передачи высокоскоростных данных (до 100 Мб/с) и соединений на большие расстояния используется оптоволоконный кабель. Таким образом, решения для высокоскоростных приложений получаются достаточно дорогими. OPEN DECconnect также поддерживает кабельную систему ThinWare на коаксиальном кабеле.

Удачным вариантом кабельной системы для создания информационной инфраструктуры зданий и офисов является решение корпорации AT&T.

SYSTIMAX - это распределенная структурированная кабельная система внутри здания или комплекса зданий. Установив такую кабельную систему, пользователь получает возможность использовать одновременно как линии передачи данных, локальные сети компьютеров, так и телефонную систему, сеть датчиков пожарной и охранной сигнализации.

Компания AT&T вводит собственную классификацию подсистем в зависимости от функционального назначения и места расположения компонентов кабельной системы:

• *Подсистема кампуса или внешняя подсистема* (campus subsystem) состоит из медного и оптоволоконного кабеля, устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят устройства интерфейса внешних кабельных линий с внутренними коммуникационными каналами.

• *Техническое помещение* (equipment room) служит для размещения различного коммуникационного и служебного оборудования, предназначенного для обеспечения работы административной подсистемы.

• *Административная подсистема* (administrative subsystem) предназначена для быстрого и легкого управления кабельной системой SYSTIMAX при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно), устройства коммутации и сопряжения основной магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т.д.

• *Основная магистраль* (backbone cabling) состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она обеспечивает главные кабельные каналы в здании и связывает между собой этажи здания или большие площади одного и того же этажа.

• *Горизонтальная подсистема* (horizontal subsystem) на базе витого медного кабеля расширяет основную магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

• *Подсистема рабочего места* (work location subsystem) включает в себя соединительные кабели, удлинители, адаптеры, устройства сопряжения и обеспечивает физическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемой,

В SYSTIMAX используется 2 среды для передачи сигнала по коммуникационным линиям - оптическое волокно и медный кабель.

При использовании оптоволоконных кабелей скорость передачи сигнала может достигать 155 Мб/с. Наличие защищенных и бронированных кабелей позволяет устанавливать оптоволоконные соединения не только в офисе или банке, но и в производственном здании или на территории производственного, делового или жилого комплекса. Корпорация AT&T предлагает все необходимые материалы и инструменты для установки оптоволоконных кабельных систем, включая устройства сопряжения с медным неэкранированным витым кабелем или коаксиальным кабелем.

Внедрение полного диапазона кабельной продукции пятой, наиболее "быстрой" категории, обеспечивает скорость передачи данных до 100 Мб/с.

Характеристики продукции SYSTIMAX позволяют не только интегрировать ее в офисные и банковские компьютерные системы, но также использовать и для автоматизации производств, включая производства со сложной окружающей средой. В этом случае SYSTIMAX использует особый подход к организации кабельной системы. Основная магистраль состоит из комбинации оптоволоконного и медного кабеля и объединяет различные помещения производства, а локальные подсети построены с использованием медного неэкранированного кабеля.

К сети можно подключать множество устройств. включая устройства прямого и удаленного управления, компьютерные терминалы для административной поддержки, датчики телеметрии.

Рисунок 16.10 иллюстрирует применение основных соединительных конструктивных элементов, используемых для разводки кабеля на основе неэкранированной витой пары на этаже.

Лекция .3. Многосегментные локальные сети.

16.3.1. Структуры и средства.

Без активного коммуникационного оборудования - концентраторов, мостов, коммутаторов и маршрутизаторов, которые соединяются с конечными узлами сети с помощью гибкой кабельной системы, транспортная подсистема не сможет выполнить свои функции так, как это от нее требуется в большой гетерогенной сети. Общий подход при структурировании заключается в образовании в большой сети с помощью концентраторов некоторого количества не связанных между собой сегментов сети (рисунок 16.11) как основы для дальнейшего соединения этих сегментов через мосты, коммутаторы или маршрутизаторы.

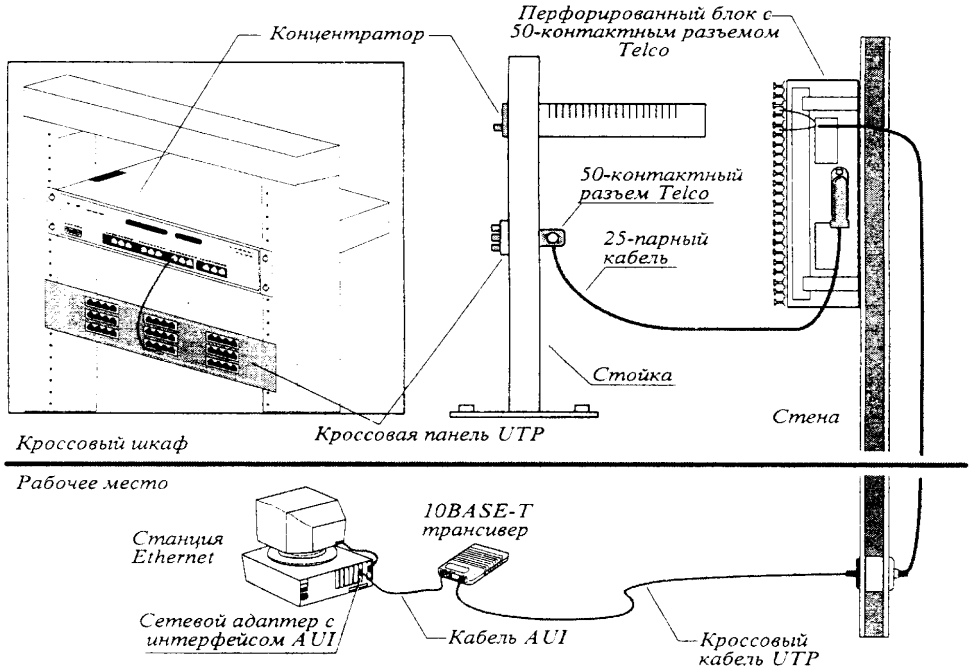


Рис. 16.10. Разводка витой пары на этаже

При использовании почти во всех протоколах локальных сетей (кроме ATM) общих сред передачи данных, размер сегмента ограничивается его загруженностью (30% для Ethernet и Fast Ethernet, 80% доя Token Ring, FDDI и 1OOVG-AnyLAN). Кроме этого, размер сегмента может быть ограничен и по другим причинам - например, из-за определенного количества компьютеров в отделе или на этаже здания.

16.3.2. Применение концентраторов.

Основные функции концентраторов неразрывно связаны с тем протоколом канального уровня, который данный концентратор поддерживает. Эти функции были рассмотрены при рассмотрении каждого из протоколов локальных сетей.

Кроме этих основных функций, концентраторы часто выполняют и *дополнительные функции,* которые увеличивают степень их активного воздействия на обрабатываемый трафик.

Различные производители концентраторов реализуют в своих устройствах различные наборы вспомогательных функций, но наиболее часто встречаются следующие.

• Объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно).

• Автосегментация портов (partitioning) - отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной долины и т.п.). Это свойство существенно повышает эксплуатационные характеристики сети, так как отключает некорректно работающее устройство (например, сетевой адаптер, постоянно генерирующий последовательность единиц, отключается от сегмента, что локализует неисправность и позволяет остальным станциям сегмента не прерывать работу).

• Поддержка резервных связей между концентраторами, которые используются при отказе основных (рисунок 16.12). Резервные связи (порты) обычно должны конфигурироваться администратором с указанием активной

связи, которую дублирует резервная, и если основной порт отказывает (сегментируется), то концентратор автоматически делает резервный порт активным.

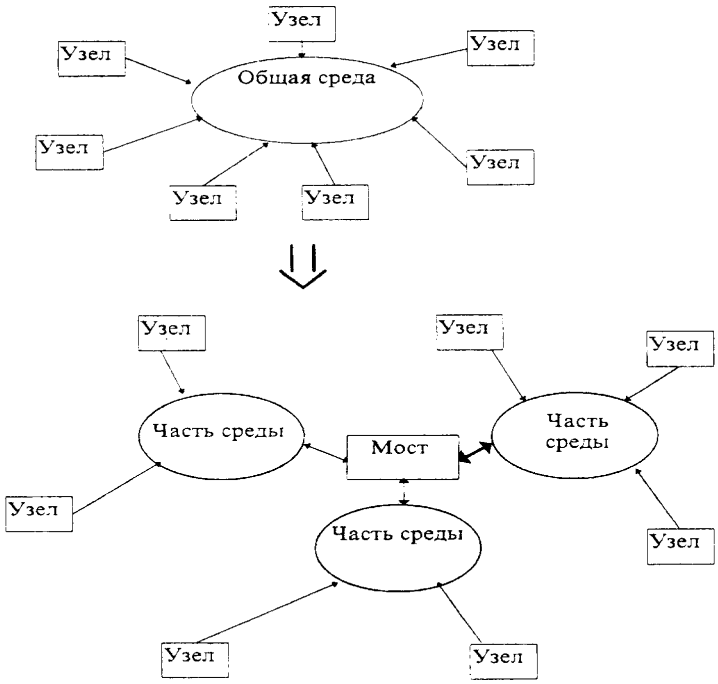


Рис. 16.11 . Мосты. Основная функция - разделение общей среды передачи данных локальной сети на несколько частей

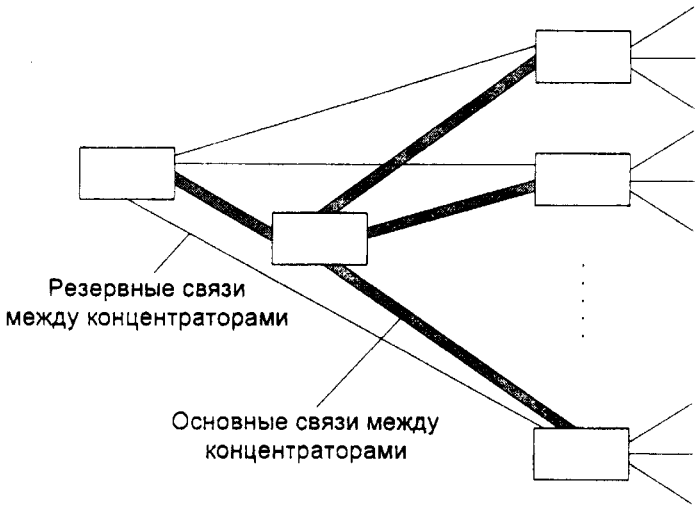


Рис. 16.12. Поддержка резервных связей между концентраторами

• Защита от несанкционированного доступа к передаваемым по сети данным.

• Наиболее простой способ - назначение разрешенных МАС-адресов портам концентратора (рисунок 16.13). При поступлении на порт кадра с недопустимым МАС-адресом, этот кадр отфильтровывается, а факт нарушения прав доступа может быть зафиксирован.

• Кроме ограничения доступа станций к портам, концентратор может осуществлять шифрацию поля данных проходящих через него кадров. Так как

процесс истинной шифрации требует большой вычислительной мощности, то на уровне повторителей часто вместо шифрации применяется метод случайного искажения поля данных в пакетах, передаваемых портам с адресом, статичным от адреса назначения пакета. Этот метод сохраняет логику случайного доступа к среде, так как все станции видят занятость среды кадром информации, но только станция, которой послан этот кадр, может понять содержание поля данных кадра (рисунок 16.14).

• Поддержка средств управления сетями - протокола SNMP, баз управляющей информации M1B (как стандартных, так и частных). Управляемые концентраторы (часто называемые также интеллектуальными) позволяют администраторам сети и обслуживающему персоналу из одного центрального пункта контролировать состояние своих портов, включать и отключать порты и конфигурировать концентраторы для выполнения остальных дополнительных функций, описанных выше.

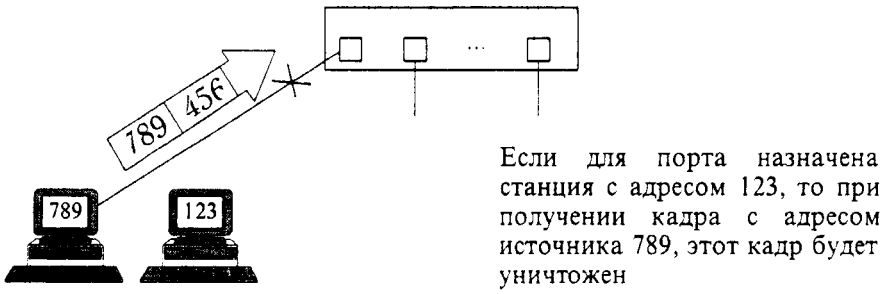


Рис. 16.13. Осуществление изоляции портов: передача кадров только от станций с фиксированными адресами

Конструктивное исполнение концентраторов также бывает различным:

• *Концентратор с фиксированным количеством портов* - наиболее простое конструктивное исполнение, когда устройство представляет собой отдельный корпус со всеми необходимыми элементами (портами, органами индикации и управления, блоком питания), и эти элементы заменять нельзя. Обычно все порты такого

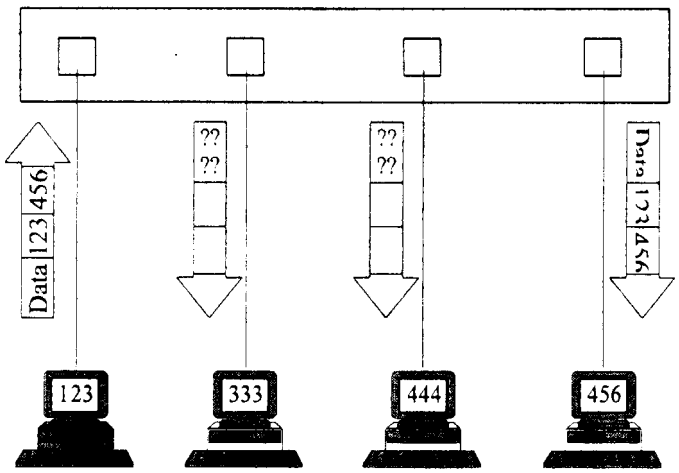


Рис. 16.14. Искажение поля данных в пакетах, не предназначенных для приема узлами (the need to know)

концентратора поддерживают одну среду передачи, общее количество портов изменяется от 4-8 до 24. Один порт может быть специально выделен для подключения концентратора к магистрали сети или же для объединения концентраторов (в качестве такого порта часто используется порт с интерфейсом AUI, в этом случае применение соответствующего трансивера позволяет подключить концентратор к практически любой физической среде передачи данных).

• *Модульный концентратор* - устройство выполняется в виде отдельных модулей с фиксированным количеством портов, устанавливаемых на общее шасси. Шасси имеет шину для объединения отдельных модулей в единый повторитель. Для модульного концентратора могут существовать различные типы модулей, отличающиеся количеством портов и типом поддерживаемой физической среды. Часто функции поддержки протокола SNMP выполняют в виде отдельного модуля, при установке которого концентратор превращается в интеллектуальное устройство. Модульные концентраторы позволяют более точно подобрать необходимую для конкретного применения конфигурацию концентратора, а также гибко и с минимальными затратами реагировать на изменения конфигурации сети.

Часто в модульных концентраторах, рассчитанных на подключение большого количества узлов, шасси содержит несколько независимых шин для объединения портов модулей в единый повторитель. При таком построении концентратор представляет собой многосегментный повторитель, который можно рассматривать как несколько несвязанных повторителей, выполненных в общем корпусе и имеющих общий источник питания, органы управления и индикации, и возможно, общий модуль управления по протоколу SNMP. Каждый из модулей такого концентратора можно приписать к определенной внутренней шине Ethetmet либо аппаратным способом (с помощью установки соответствующего переключателя), либо программно, с помощью поставляемой вместе с концентратором (или отдельно) программы управления. Предполагается, что такие несвязанные между собой сегменты можно при необходимости объединить в единый сегмент с помощью внешнего моста или же образовать интерсеть с помощью маршрутизатора.

В некоторых многосегментных типах концентраторов имеется возможность приписывать к отдельному сегменту не обязательно весь модуль, а только его отдельные порты. Обычно такая операция выполняется программным способом, и соответствующее свойство концентратора называется конфигурационной или же статической коммутацией (в отличие от динамической коммутации, когда устройство выполняет функции не повторителя, а многопортового моста). Концентратор с конфигурационной коммутацией позволяет быстро изменять распределение узлов сети по отдельным сегментам сети без физической перекоммутации связей, что бывает необходимо в различных случаях - при балансировке загрузки сегментов, при добавлении новых пользователей, при переходе пользователей из одной рабочей группы в другую или же при переезде пользователя из одного помещения в другое.

• *Стековый концентратор* - он как и концентратор с фиксированным числом портов выполнен в виде отдельного корпуса без возможности замены отдельных его модулей, но имеет специальные порты и кабели для объединения нескольких таких корпусов в *единый повторитель,* который обеспечивает общую синхронизацию всех своих портов и поэтому с точки зрения правила 4-х повторителей считается одним повторителем. Число объединяемых в стек

корпусов может быть достаточно большим (обычно до 8). Стековые концентраторы могут поддерживать различные физические среды передачи, что делает их почти такими же гибкими, как и модульное концентраторы, но при этом стоимость его в расчете на один порт получается обычно ниже. Стековые концентраторы чаще поддерживают только один сегмент (одну шину объединения корпусов), хотя имеются и многосегментные стековые концентраторы.

Стековые концентраторы, выпускаемые одним производителем, выполняются в едином конструктивном стандарте, что позволяет легко устанавливать их друг на друга, образуя единое настольное устройство, или помещать их в общую стойку.

Для нескольких устройств, объединенных в стековых повторитель, можно использовать единый модуль управления (который вставляется в один из корпусов стека как дополнительный модуль), а также общий избыточный источник питания, что уменьшает общую стоимость стека.

Для создания центров обработки пакетов, реализующих не только функции повторителей, но и функции мостов, коммутаторов и маршрутизаторов, некоторые производители оборудования выпускают такие устройства в стековом исполнении, то есть в корпусах конструктивно совместимых с корпусами стековых повторителей, что позволяет удобно строить единую стойку управления, а также использовать общий резервный источник питания. Функционально установка в общий стек коммутаторов и маршрутизаторов обычно не изменяет совместной работы этих устройств (в отличие от повторителей, которые образуют единый повторитель, а не несколько независимых). Исключением является стековый маршрутизатор ASN компании Bay Networks, корпуса которого образуют общий маршрутизатор.

• *Модульно-стековые концентраторы* представляют собой модульные концентраторы, объединенные специальными связями в стек. Как правило, корпуса таких концентраторов рассчитаны на небольшое количество модулей (1 - 3). Эти концентраторы сочетают достоинства обоих типов концентраторов.

В зависимости от области применения концентраторы делятся на три класса:

• концентраторы рабочих групп,

• концентраторы отделов,

• корпоративные концентраторы.

Концентраторы рабочих групп обычно представляют собой устройства с фиксированным количеством портов (8 - 12), ориентированные на поддержку одного типа кабеля и обладающие минимальным набором дополнительных функций. Все изменения по переносу компьютеров из одной рабочей группы в другую при использовании этих концентраторов осуществляются за счет физической перекоммутации кабелей в кроссовых секциях или на панелях таких коммутаторов. Централизованное наблюдение и управление затруднено, если концентратор не поддерживает протокол SNMP.

Корпоративные концентраторы занимают другую крайнюю позицию - это модульные концентраторы с максимальным набором дополнительных функций. Такие концентраторы имеют модули для поддержки всех основных типов кабелей и разъемов и позволяют в одном корпусе осуществить объединение большого количества физических сегментов - максимальное количество портов может доходить до 200 - 400 в одном корпусе.

В корпоративных концентраторах обычно имеется по нескольку изолированных внутренних шин для всех основных протоколов - Ethernet) Token

Ring, FDDI, Fast Ethernet.

Корпоративные концентраторы применяются как гибкие программируемые центры коммутации, с помощью которых можно централизованно создавать рабочие группы, прикрепленные к одному из внутренних сегментов концентратора. В отличие от распределенных и плохо управляемых концентраторов рабочих групп, корпоративный концентратор позволяет заменить физическую перекоммутацию компьютеров в кроссовых шкафах программной коммутацией, что особенно важно в больших организациях, где такие изменения происходят достаточно часто. Легкость переноса станций из одного сегмента в другой позволяет находить экспериментальным путем рациональное разбиение сети на сегменты.

В корпоративный концентратор могут подходить кабельные связи как от концентраторов более низкого уровня иерархии, так и от отдельных рабочих станций или серверов. Наличие одного устройства - интеллектуального коммутационного центра - позволяет варьировать степень физической распределенности системы, усиливая ее централизацию, что может облегчить ее обслуживание.

Концентраторы отделов занимают промежуточное положение. Здесь часто находят применение стековые и модульно-стековые концентраторы.

16.3.3. Применение мостов и коммутаторов.

Мосты и коммутаторы позволяют улучшить время реакции сети в тех случаях, когда имеются ярко выраженные области локализации трафика, то есть интенсивность трафика между компьютерами одного подмножества компьютеров сети намного выше интенсивности трафика между этим подмножеством и другими компьютерами сети. В таких случаях области локализации трафика имеет смысл выполнять в виде сегментов с разделяемой средой передачи данных, а сегменты соединять мостами или коммутаторами.

Если же ярко выраженных областей локализации трафика в сети нет, то применение мостов или коммутаторов может и ухудшить время реакции, так как эти устройства обычно передают кадры данных между сегментами с некоторой задержкой и при высоко интенсивном трафике могут не справляться с межсегментными передачами и просто терять пакеты из-за переполнения внутреннего буфера.

Поэтому применение мостов и коммутаторов требует тщательного анализа трафика в сети и сопоставления интенсивности межсегментного трафика с возможностями применяемого устройства для связи сегментов.

По своему принципу действия мосты подразделяются на два типа.

Мосты первого типа выполняют так называемую маршрутизацию от источника (Source Routing), метод, разработанный фирмой IBM для своих сетей. Этот метод требует, чтобы узел-отправитель пакета размещал в нем информацию о его маршруте. Другими словами, каждая станция должна выполнять функции по маршрутизации пакетов.

Второй тип мостов осуществляет прозрачную для конечных станций передачу пакетов (Transparent Bridges).

Прозрачные мосты являются наиболее распространенным типом мостов. Для прозрачных мостов сеть представляется наборами MAC-адресов устройств, причем каждый набор связан с определенным портом моста. Они используют эти адреса для принятия решения во время обработки приходящих на порты пакетов.

Мосты не имеют доступа к информации об адресах сетей, относящейся к более высокому уровню. Поэтому они ограничены в принятии решений о возможных путях или маршрутах перемещения пакетов по сети.

Для того, чтобы пакеты не перемещались по замкнутым контурам, большинство мостов поддерживают алгоритм Spanning Tree, обеспечивающий построение на основе всего множества линий связи древовидной структуры, в которой связи, образующие дерево, являются основными, а остальные - резервными.

Вследствие функциональной ограниченности мосты устроены достаточно просто и представляют собой удобное и недорогое средство для построения интерсети.

Коммутаторы (switches) локальных сетей являются в сущности высокоскоростными мостами. То есть, функционально - это мосты, а различие между традиционными мостами и коммутаторами состоит в использовании различных внутренних схем реализации механизма перемещения пакетов между портами, а также иногда и различных схем распространения кадров с неизвестным мосту MAC-адресом назначения.

Мосты регенерируют пакеты, которые они передают с одного порта на другой (операция forwarding). Одним из преимуществ использования мостов является увеличение расстояния, покрываемого интерсетью, так как количество пересекаемых мостов не оказывает влияния на качество сигнала,

При увеличении расстояния увеличиваются задержки передачи пакетов, кроме того, мост сам вносит дополнительную задержку. Суммарная задержка не должна превышать ограничений, присущих используемым сетевым протоколам. Например, максимально допустимая задержка для передачи пакета IPX обычно составляет 1,5 секунды, а для пакета IP - 2 минуты, Для обеспечения приемлемой производительности максимальная задержка должна находиться в пределах от 30 миллисекунд до 1,5 секунд. В сетях Ethernet (10 Мб/сек) это означает, что практически во всех случаях с помощью мостов могут быть последовательно соединены только 7 локальных сегментов. Обычно эта проблема решается параллельным подсоединением всех сегментов к магистральному сегменту.

Гораздо сложнее проблемы, связанные с задержками, решаются тогда, когда мост используется для подсоединения удаленной сети, В этом случае вероятность того, что время задержки, вызванное использованием очень протяженных сред передачи данных, превысит допустимую величину, становится очень высокой.

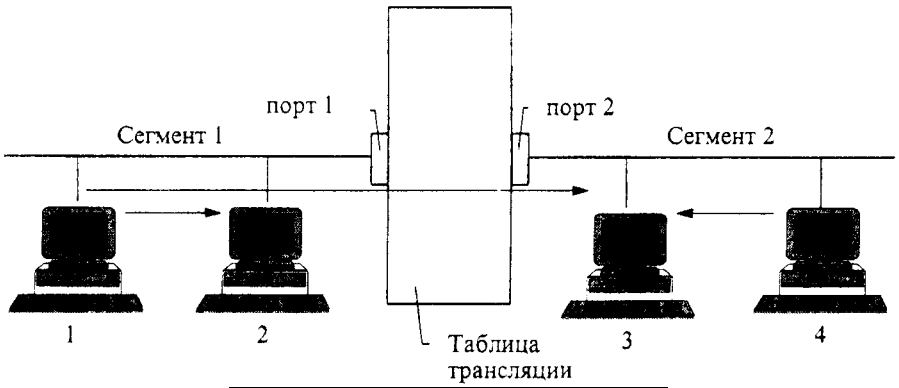
Поскольку мосты оперируют с данными канального уровня модели OSI, они "видят" только MAC-адреса устройств. Хотя сетевые пакеты и содержат высокоуровневую информацию об использующихся протоколах и соединениях, эта "маршрутная" информация невидима для мостов. Таким образом, мосты являются совершенно прозрачными для протоколов, начиная с сетевого и выше.

Эта прозрачность позволяет мостам передавать пакеты различных протоколов высокого уровня, никоим образом не влияя на их содержимое.

Прозрачные мосты имеют дело как с адресом источника, так и с адресом назначения. Мост использует адрес источника для построения своей базы данных адресов устройств, называемой также таблицей адресов устройств. В этой таблице устанавливается принадлежность адреса узла какому-либо порту моста. Все операции, которые выполняет мост, связаны с этой базой данных. На рисунке 16.15 показан фрагмент сети, содержащий двухпортовый мост, и соответствующая этому фрагменту часть таблицы адресов устройств. Все порты моста работают в так называемом "неразборчивом" (promiscuous) режиме захвата пакетов, то есть все поступающие на порт пакеты буферизуются.

Когда мост получает пакет от какого-либо своего порта, то он (после буферизации) сравнивает адрес источника с элементами базы данных адресов. Если адрес отсутствует в базе, то он добавляется в нее. Если этот адрес уже имеется в базе, то возможно два варианта - либо адрес пришел с того же порта, который указан в таблице, либо он пришел с другого порта. В последнем случае строка таблицы, соответствующая обрабатываемому адресу, обновляется - номер порта заменяется на новое значение (очевидно, станцию с данным адресом переместили в другой сегмент сети).

Таким способом мост "изучает" адреса устройств сети и их принадлежность портам и соответствующим сегментам сети. Из-за способности моста к обучению к сети могут добавляться новые устройства без необходимости реконфигурирования моста. Администратор может объявить часть адресов статическими и не участвующими в процессе обучения (при этом он их должен задать сам). В случае статического адреса приход пакета с данным адресом и значением порта, не совпадающим с хранящимся в базе, будет проигнорирован и база не обновится.



MAC-адрес	Порт
1	1
2	1
3	2
4	2

Рис. 16.15. Мост как коммуникационное устройство канального уровня

Каждый раз при получении пакета мост сравнивает адрес назначения пакета с адресами, хранящимися в его базе. Если адрес назначения принадлежит тому же сегменту, что и адрес источника, то мост "фильтрует" (Filter) пакет, то есть удаляет его из своего буфера и никуда не передает. Эта операция помогает предохранить сеть от засорения ненужным трафиком.

Если адрес назначения присутствует в базе данных и принадлежит другому сегменту по сравнению с адресом источника, то мост определяет, какой из его портов связан с этим адресом и "продвигает" (forward) пакет на соответствующий порт.

Если же адрес назначения отсутствует в базе или же это широковещательный адрес, то мост передает пакет на все порты, за исключение того порта, откуда он пришел. Такой процесс называется "затоплением" (flooding) сети. Затопление гарантирует, что пакет будет помещен на все сегменты сети и, следовательно, доставлен адресату или адресатам.

Мосты, работающие по протоколу Source Routing.

Мосты этого типа применяются для соединения колец Token Ring и FDDI, хотя для этих же целей могут использоваться и прозрачные мосты. Маршрутизация от источника (Source Routing, SR) основана на том, что станция-отправитель помещает в посылаемый в другое кольцо кадр всю адресную информацию о промежуточных мостах и кольцах, которые должен пройти кадр перед тем, как попасть в кольцо, к которому подключена станция-получатель.

Хотя в этом способе повсеместно используется термин маршрутизация, настоящей маршрутизации в традиционном понимании этого термина здесь нет, так как мосты и станции по-прежнему используют для передачи кадров данных только информацию MAC-уровня, и заголовки сетевого уровня для мостов данного типа по прежнему остаются неразличимой частью поля данных кадра.

Однако, некоторые приемы, характерные для маршрутизации пакетов на сетевом уровне, алгоритм маршрутизации от источника использует. На рисунке 16.16 приведен фрагмент сети, состоящей из нескольких колец Token Ring, соединенных мостами, работающими по алгоритму маршрутизации от источника (будем их называть SR-мостами). Подобно сетям и маршрутизаторам в алгоритмах маршрутизации на сетевом уровне, кольца и мосты имеют идентификаторы. Однако мосты по-прежнему не строят всей карты связей колец в сети, как это делали бы маршрутизаторы. В отличие от маршрутизаторов они пользуются при принятии решений информацией, имеющейся в соответствующих полях кадра.

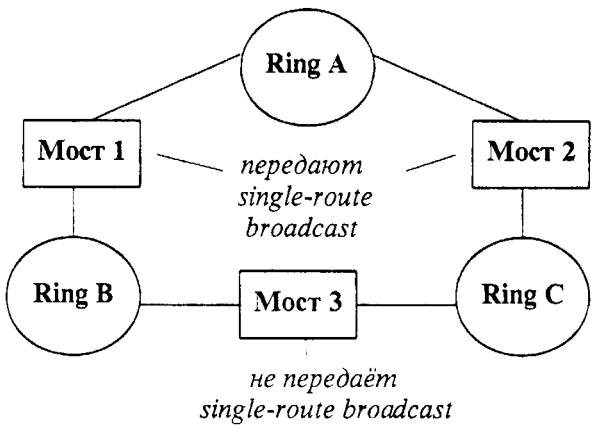


Рис. 16.16. Мосты типа Source Routing

При получении каждого пакета SR-мосту нужно только просмотреть поле маршрутной информации на предмет наличия в нем своего идентификатора, И если он там присутствует и сопровождается идентификатором кольца, которое подключено к данному мосту, то мост передает поступивший кадр на указанное кольцо. В противном случае кадр на другое кольцо не передается. В любом случае

кадр возвращается по исходному кольцу станции-отправителю и, если он был передан на другое кольцо, то бит А (адрес распознан) и бит С (кадр скопирован) поля статуса кадра устанавливаются в 1, чтобы указать станции-отправителю, что кадр был получен станцией назначения (в данном случае передан мостом в другое кольцо).

Так как маршрутная информация в кадре нужна не всегда, а только для передачи кадра между станциями, подключенными к разным кольцам, то бит индивидуального/группового адреса (I/O) в адресе источника используется не по прямому назначению (адрес источника всегда индивидуальный), а для указания присутствия или отсутствия в кадре маршрутной информации.

Для работы алгоритма маршрутизации от источника используются два дополнительных типа кадра - одномаршрутный широковещательный кадр-исследователь (singl-route broadcast frame) и многомаршрутный широковещательный кадр-исследователь (all-route broadcast frame).

Кадр первого типа отправляется станцией, когда она не знает маршрут до станции назначения. В нем станция устанавливает поле маршрутной информации нулевой длины. Как и прозрачные мосты, SR-мосты работают в режиме "неразборчивого" захвата, буферизуя и анализируя все кадры.

При получении одномаршрутного широковещательного кадра-исследователя, SR-мост передает его в исходном виде на все порты, входящие в конфигурацию покрывающего дерева. SR-мосты определяют ее примерно так же, как и мосты, поддерживающие алгоритм Spanning Tree. Необходимость в конфигурации без петель для кадров-исследователей первого типа вызвана тем, что таким способом предотвращается возможность бесконечного зацикливания пакетов. Топология покрывающего дерева в алгоритме SR используется только для кадров этого типа.

В конце концов кадр-исследователь, распространяясь по сети, доходит до станции назначения. В ответ станция назначения отправляет многомаршрутный широковещательный кадр-исследователь станции-отправителю. В отличие от одномаршрутного кадра, этот кадр передается мостами на все порты, а не только на входящие в активную конфигурацию. При приеме такого кадра, каждый промежуточный мост добавляет в поле маршрутной информации новый описатель маршрута (свой идентификатор и идентификатор сегмента, с которого получен кадр), наращивает длину поля маршрутной информации и широковещательно его распространяет.

Станция-источник получает в общем случае несколько кадров-ответов, прошедших по всем возможным маршрутам составной сети, и выбирает наилучший маршрут (обычно по числу пересечений мостов).

Затем маршрутная информация помещается в таблицу маршрутизации станции и используется для отправки кадров данных станции назначения по наилучшему маршруту.

Так как многомаршрутные кадры-исследователи не учитывают конфигурацию покрывающего дерева, то для предотвращения зацикливания мосты обрабатывают их следующим образом. Перед передачей кадра на какой-либо сегмент мост проверяет, нет ли идентификатора этого сегмента в списке маршрутов кадра. Если такой сегмент уже был пройден кадром, то кадр в данный сегмент не направляется.

Мосты с маршрутизацией от источника имеют по отношению к прозрачным мостам и преимущества, и недостатки (таблица 16.2).

Наличие двух возможных алгоритмов работы мостов - от источника и в

Таблица 16.2

Преимущества	Недостатки
Более рациональные маршруты	Более дорогие сетевые адаптеры - принимают участие в
Проще и дешевле - не нужно строить таблицы фильтрации	Сеть не прозрачна - кольца имеют номера
Более высокая скорость - не нужно просматривать таблицы фильтрации	Увеличивается трафик за счет широковещательных пакетов

прозрачном режиме - создает трудности для построения сложных многопротокольных сетей с сегментами Token Ring. Мосты, работающие от источника, не могут поддерживать сегменты, рассчитанные на работу в прозрачном режиме, и наоборот.

До недавнего времени организации решали эту проблему двумя способами. Один способ заключался в использовании во всех сегментах либо только маршрутизации от источника, либо только прозрачных мостов. Другим способом была установка дополнительных устройств образования интерсети - маршрутизаторов. Оба решения стоили дорого и требовали значительных усилий для реализации.

Сегодня имеется третье решение. Оно основано на новом стандарте, который позволяет объединить обе технологии работы моста в одном устройстве. Этот стандарт, называемый SRT (Source Route Transparent), позволяет мосту работать в любом режиме. Мост просматривает специальные флаги в заголовке кадров Token Ring и автоматически определяет, какой из алгоритмов нужно применить.

Главными параметрами моста являются:

- размер внутренней адресной таблицы;
- скорость фильтрации (Filtering);
- скорость маршрутизации (forwarding).

Макси.иальная емкость адресной таблицы определяет максимальное количество MAC-адресов, которыми может оперировать мост. Для пользователя это выражается максимальным количеством MAC-адресов, которые можно подключить к одному порту моста. Типичные значения лежат в пределах от 500 до 8000. В случае появления новых адресов при полностью заполненной таблице, мост вытесняет старые адреса и помещает в нее новые. Следовательно, это обстоятельство только замедлит работу моста, но не вызовет его отказа.

Скорости фильтрации и маршрутизации пакетов характеризуют производительность моста по отношению к двум главным операциям, выполняемым мостом.

Скорость фильтрации определяет скорость, с которой мост буферизует прибывающие кадры, просматривает адресную таблицу и уничтожает пакет, если он не должен передаваться далее.

Скорость маршрутизации обычно несколько ниже, чем скорость фильтрации, так как эта операция, включая все действия по фильтрации, заменяет последний этап - уничтожение пакета - более медленным действием - передачей пакета на выходной порт.

Если эти скорости ниже максимально возможной скорости передачи пакетов для конкретного протокола, то мост может являться причиной задержек и

снижения производительности. Если выше - значит стоимость данного моста скорее всего выше минимально возможной. Например, для прокола Ethernet максимальная производительность составляет 14880 пакетов в секунду (для пакетов 64 байта + 8 байтов преамбулы). Если мост подсоединяет к сети FDDI N сетей протокола Ethernet, то его скорости фильтрации и маршрутизации должны быть равны N*14880 пакетов в секунду.

Максимально возможная скорость фильтрации пакетов протокола FDDI составляет около 500000 пакетов в секунду.

Дополнительные функции мостов.

Мосты также различаются выполняемыми ими дополнительным функциям, среди которых наиболее важными являются следующие.

• *Поддержка алгоритма покрывающего дерева STA.*

• *Поддержка алгоритма прозрачной маршрутизации от источника.*

• *Возможность объединения сетей с различными протоколами канального уровня* (транслирующие мосты).

До недавнего времени единственным средством объединения сетей с различными протоколами канального уровня были маршрутизаторы. Однако в последнее время появилось много моделей мостов, которые способны передавать кадры, например, из сегмента Ethernet в сегмент FDDI и наоборот.

По принципу передачи пакетов между сетями с разными канальными протоколами мосты подразделяются на *инкапсулирующие* (encapsulating) и *транслирующие* (translational). Инкапсулирующие мосты упаковывают при передаче пакеты канального уровня одной сети в пакеты канального уровня другой сети. После прохождения пакета по второй сети аналогичный мост удаляет оболочку промежуточного протокола, и пакет продолжает свое движение в исходном виде.

Очевидно, что при таком методе взаимодействие со станциями второй сети невозможно и эта сеть используется только как промежуточное транспортное средство.

Транслирующие мосты выполняют преобразование из одного протокола канального уровня в другой. Такой метод имеет преимущества - меньше накладные расходы, так как не нужно передавать два заголовка канального уровня, станции другой сети становятся доступными. Но транслирующие мосты вносят дополнительную задержку при преобразовании форматов кадров, а также при новом вычислении контрольной суммы кадра. Но самый главный недостаток транслирующих мостов состоит в том, что они имеют существенное ограничение - максимальный размер кадров у сетей, соединяемых таким мостом, должен быть одинаковым.

• *Установка пользовательских фильтров.*

Это свойство предоставляет администратору возможность определить условия фильтрации (то есть блокировки передачи) кадров, основанные на любом компоненте кадра, например на типе протокола, адресе источника или назначения, типе кадра или даже на значении любой последовательности битов в поле данных кадра. Такие фильтры помогают разделить сеть на части для повышения ее производительности или же повысить уровень защиты данных, разрешив только определенные виды сервиса, например, только услуги электронной почты.

• *Адресное ограничение передачи пакетов.*

Позволяет усилить защиту данных от несанкционированного доступа, изолируя некоторые устройства от некоторых сегментов или других устройств.

• *Использование различных классов сервиса (class-of-service).*

Позволяет администратору назначить различным типам пакетов различные приоритеты обработки их мостами. При этом мост поддерживает несколько очередей необработанных кадров и может быть сконфигурирован, например, так, что он передает один низкоприоритетный пакет на каждые 10 высокоприоритетных пакетов. Это свойство может особенно пригодиться на низкоскоростных линиях и при наличии приложений, предъявляющих различные требования к допустимым задержкам.

• *Поддержка протокола управления SNMP.*

Мосты выполняют более интеллектуальные функции по сравнению с повторителями, поэтому многие мосты поддерживают управление по сети с помощью протокола SNMP.

Это дает возможность администратору централизованно:

• *Конфигурировать порты мостов.*

• *Производить сбор статистики и анализ трафика.*

Например, для каждой подключенной к сети станции можно получить информацию о том, когда она последний раз посылала пакеты в сеть, о количестве пакетов и байтов, переданных в сеть, количестве пакетов и байтов, переданных за пределы сети, количестве переданных широковещательных пакетов и т.п.

- *Устанавливать дополнительные фильтры на порты моста по физическим адресам сетевых устройств* с целью усиления защиты от несанкционированного доступа или повышения эффективности работы отдельных сегментов.

• *Оперативно получать сообщения о всех возникающих проблемах в сети и локализовать их.*

• Проводить диагностику модулей моста,

• Просматривать в графическом формате изображения панелей модулей, установленных в удаленных мостах, включая текущее состояние индикаторов.

Особенности применения коммутаторов.

Технология коммутации сегментов Ethernet была предложена фирмой Kalpana в 1990 году в ответ на растущие потребности в повышении пропускной способности связей высокопроизводительных серверов с сегментами рабочих станций. Эта технология основана на отказе от использования разделяемых линий связи между всеми узлами сегмента и использовании коммутаторов, позволяющих одновременно передавать пакеты между всеми его парами портов.

Функционально многопортовый коммутатор работает как многопортовый мост. но новшество заключается в том, что он, во-первых, одновременно осуществляет передачу кадров MAC-уровня между несколькими портами, а традиционные мосты делали это последовательно, а, во-вторых, обеспечивает очень маленькую задержку между приходом пакета на входной порт и появлением его первых байтов на выходном порту, в то время как традиционный мост всегда сначала полностью буферизует пакет, а только затем начинает его передачу на другой порт. В результате внутренняя производительность (forwarding) коммутирующего моста значительно превышает внутреннюю производительность обычного моста, что и служит предпосылкой для увеличения общей производительности сети, в которой установлены коммутаторы.

В отличие от таких новых технологий как ATM, технология коммутации

сохраняет аппаратуру и алгоритмы работы оборудования канального уровня в конечных узлах, что и обеспечило ей большой успех.

На рисунке 16.17 показан принцип использования коммутатора Ethernet для повышения пропускной способности сети. При подключении к портам коммутатора по одной конечной станции каждой такой станции предоставляется полная пропускная способность Ethernet в 10 Мб/с, которая в случае объединения п станций в один домен коллизий уменьшилась бы для каждой станции до величины 10/п Мб/с.

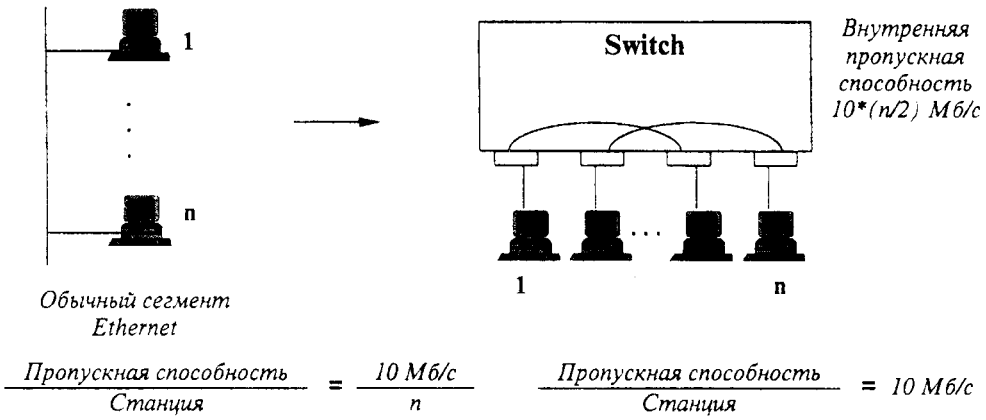


Рис. 16.17. Switching Ethernet

Многие другие фирмы стали развивать этот подход для коммутации и других традиционных технологий, таких как Token Ring и FDDI, также оставляя неизменными алгоритмы работы конечных узлов. Коммутирующие концентраторы могут также прозрачно взаимодействовать и с традиционными мостами и маршрутизаторами, что также очень важно. Обычно коммутирующие концентраторы имеют внутреннюю суммарную производительность, равную сумме пропускных способностей всех его портов. Поэтому такой коммутатор не создает ограничений по пропускной способности при межсегментных обменах при *сбалансированном* трафике. Под сбалансированным трафиком понимается трафик, равномерно распределенный между портами коммутатора. В этом случае коммутатор полностью используют свою большую внутреннюю производительность, которая в старших моделях доходит до 10 - 14 Гб/с. Пример такого распределения трафика приведен на рисунке 16.18, где каждая из трех рабочих станций с одинаковой интенсивностью обращается к каждому из трех серверов сегмента сети.

Однако, если трафик не сбалансирован, то даже самый быстродействующий коммутатор не всегда сможет гарантировать его поддержание.

Так, если в предыдущем примере все три рабочие станции обмениваются данными только с одним из серверов с максимально возможной скоростью, то на порт этого сервера данные будут поступать с интенсивностью в 30 Мб/с, в то время как порт может их принимать со скоростью 10 Мб/с. Поэтому коммутатор будет помещать избыточные кадры для этого порта в свой внутренний буфер, и какого бы размера буфер не был, все равно наступит такой момент времени, когда буфер полностью заполнится, и коммутатор будет вынужден отбрасывать поступающие пакеты.

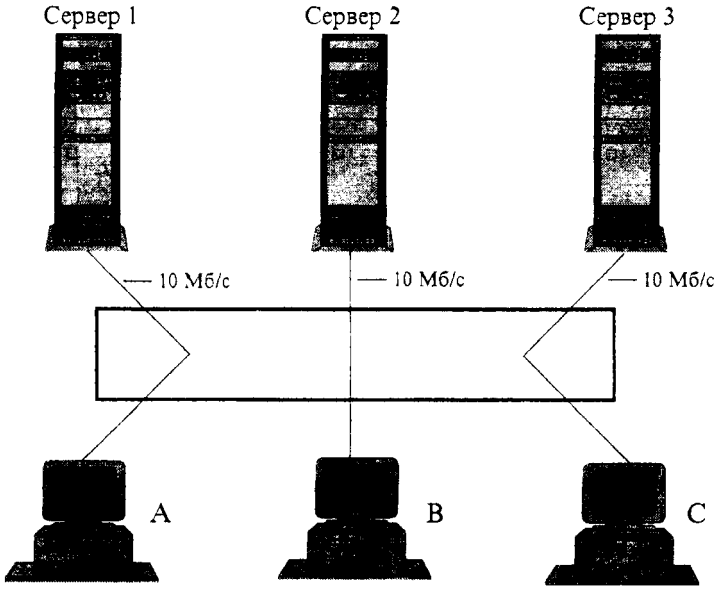


Рис. 16.18. Применение динамического переключателя портов

Такая ситуация возникает из-за того, что мосты и коммутаторы не поддерживают между сегментами базовые алгоритмы доступа к общей среде - метод случайного доступа протоколов Ethernet и Fast Ethernet или метод доступа по токену протоколов Token Ring или FDDI. Методы доступа гарантируют за счет замедления доступа к общей среде, что кадры не будут потеряны из-за неспособности среды и концентраторов поддерживать трафик слишком высокой интенсивности. Таким образом, методы доступа протоколов локальных сетей выполняют роль алгоритмов управления интенсивностями потоков, которые реализуются в протоколах глобальных сетей, предотвращая сеть от перенасыщения кадрами.

Мосты и коммутаторы (и маршрутизаторы также) не поддерживают для межсегментного трафика методы, ограничивающие доступ при слишком высокой интенсивности обмена, поэтому их применение всегда связано с риском потерь кадров данных на канальном уровне. Если же такие потери будут происходить слишком часто, то производительность сети, построенной на коммутаторах, может не повыситься, а упасть, так как потерянные кадры будут повторно передаваться протоколами более верхних уровней, которые работают с более длительными тайм-аутами по сравнению с временами передачи кадров на канальном уровне.

Более четко с графиком работает технология АТМ, в которой предусмотрены процедуры предварительного заказа каждой станцией требуемой полосы пропускания. Коммутаторы сети АТМ могут принять такой заказ, если они видят, что с большой степенью вероятности смогут его выполнить, а могут и отказаться, если в сети наблюдается переполнение или новое соединение может вызвать переполнение. При таком подходе поведение транспортной системы становится более предсказуемым.

При дисбалансе трафика можно применять коммутаторы с различными по скорости портами. В предыдущем примере, можно решить проблему за счет применения коммутатора с низкоскоростными портами для рабочих станций и высокоскоростным портом для сервера. Однако, если рабочие станции совсем не общаются между собой, то такой коммутатор не даст выигрыша в общей

производительности по сравнению с концентратором, у которого все порты высокоскоростные. Стоимость же такого концентратора может оказаться значительно ниже, чем коммутатора.

Применение коммутаторов для соединения не конечных станций, а целых сегментов, состоящих из десятка станций, повышает вероятность равномерного распределения трафика между сегментами, особенно, если в каждом сегменте имеется свой сервер.

Основные и дополнительные функции коммутаторов.

По функциям любой коммутирующий концентратор является быстродействующим мостом, поэтому его основными характеристиками являются скорость фильтрации и скорость продвижения пакетов.

Как и обычный мост, коммутирующий мост работает с протоколами канального уровня и может выполнять и дополнительные функции, такие как фильтрация пакетов по пользовательским маскам, поддержка алгоритма покрывающего дерева, трансляция одного протокола в другой.

На возможности реализации дополнительных функций существенно сказывается способ передачи пакетов - "на лету" (применяются термины on-the-fly и cut-through) или с буферизацией (buffering). Сравнение этих двух способов коммутации приведено в таблице 16.3.

Средняя величина задержки коммутаторов "на лету" при высокой нагрузке объясняется тем, что в этом случае выходной порт часто бывает занят приемом другого пакета, поэтому вновь поступивший пакет для данного порта все равно приходится буферизовать.

Обычно недорогие коммутаторы работают по алгоритму "на лету", а дорогие коммутаторы, выполняющие большое количество дополнительных функций, всегда буферизуют пакеты. Появились и коммутаторы, которые работают в режиме "на лету" до тех пор, пока не обнаруживается слишком большая интенсивность "плохих" пакетов, то есть пакетов некорректной длины или с неверной контрольной суммой. После этого они переходят на режим работы с буферизацией.

Таблица 16.3

Функция	Налету	С буферизацией
Защита от плохих кадров	Нет	Да
Поддержка разнородных сетей (Ethernet, Token Ring)	Нет	Да
Задержка передачи пакетов	Низкая (~ 40 мксек) при низкой нагрузке, средняя при высокой нагрузке	Средняя при любой нагрузке
Поддержка резервных связей	Нет	Да
Функция анализа трафика	Нет	Да
Переход на Fast Ethernet и ATM	Нет	Да

Поддержка виртуальных сегментов.

Кроме своего основного назначения - повышения пропускной способности связей в сети - коммутатор позволяет локализовать потоки информации в сети, а также контролировать эти потоки и управлять ими, образуя виртуальные сегменты. Так как динамический коммутатор передает пакет только между источником и адресатом, то он, как и обычный мост, локализует трафик, что уменьшает нагрузку в сети и повышает конфиденциальность информации. Кроме того, многие коммутаторы позволяют контролировать передачу пакетов и разрешать ее только для определенных сочетаний адресов источника и адресата. Разрешенные пары адресов образуют *виртуальный сегмент* сети, доступ внутрь которого остальным адресам запрещен. Таким образом легко реализуются различные права доступа пользователей сети на уровне MAC-адресов их станций. Каждая станция может входить в несколько виртуальных сегментов, соответствующих связям работников предприятия между собой.

Очевидно, что при подключении к порту коммутатора не отдельной станции, а целого сегмента традиционной технологии с разделяемой средой, например, сегмента коаксиального кабеля со станциями Ethernet 10Base-2, администратор сети будет ограничен в выборе станций для образования виртуальных рабочих групп. Все станции, принадлежащие разделяемому кабелю, необходимо помещать в одну группу, так как все равно они будут видеть все пакеты, помещаемые на этот кабель. Таким образом, количество виртуальных рабочих групп коммутатора не может превышать количества его портов.

Если же к каждому порту подключена только одна станция, то виртуальные рабочие группы могут образовываться произвольно. Обычно каждый коммутатор снабжается специальным программным обеспечением фирмы-производителя, с помощью которого администратор может в удобной графической форме создавать и изменять виртуальные рабочие группы.

Если сеть образуется с помощью нескольких коммутаторов, то рабочие группы можно создавать, не принимая во внимание, к порту какого коммутатора подключена станция или сегмент. Пример таких сегментов, принадлежащих нескольким коммутаторам, приведен на рисунке 16.19.

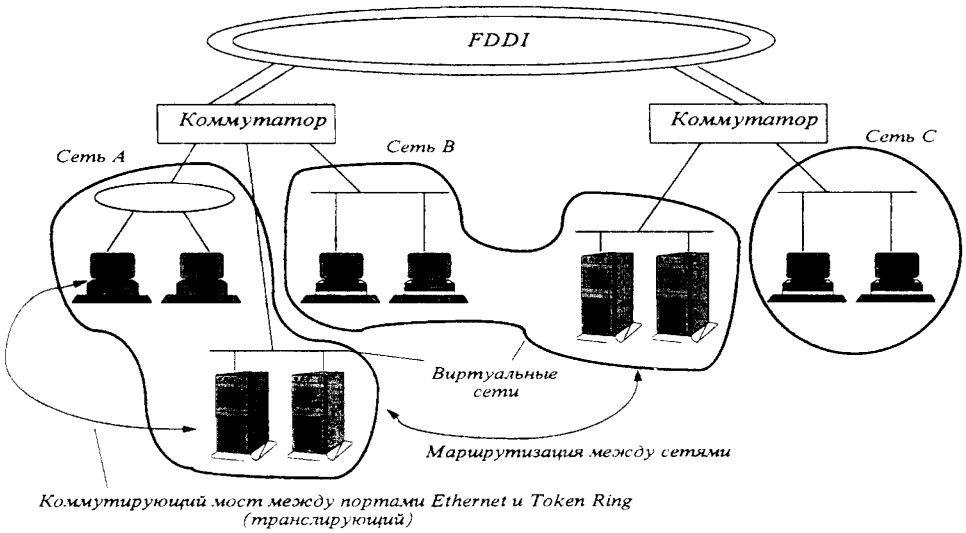


Рис. 16.19. Виртуальные сегменты и сети, образованные несколькими коммутаторами, поддерживающими функции маршрутизации

Однако, при использовании коммутаторов, реализующих алгоритм моста, невозможно обеспечить взаимодействие между изолированными виртуальными сегментами. Для объединения виртуальных сегментов нужно использовать маршрутизатор. Это может быть отдельный традиционный маршрутизатор, к каждому порту которого подключен соответствующий порт коммутатора, или же это может быть коммутатор, который наряду с функциями моста поддерживает и функции маршрутизатора.

Лекция .4. Сетевой уровень как средство объединения локальных сегментов.

16.4.1. Принципы работы составных сетей.

Сетевой уровень в вычислительных сетях служит доя образования единой транспортной системы, объединяющей несколько сетей с различными принципами передачи информации между конечными узлами.

Как видно из описания стандартов канального уровня локальных сетей, сосуществование различных стандартов и технологий передачи пакетов - норма жизни любой вычислительной сети средних и крупных размеров.

Появление новых технологий не означает мгновенного исчезновения старых, таких как 10-Мбитный Ethernet, Token Ring или. FDDI из-за огромной базы капиталовложений в эти технологии. Поэтому трудно рассчитывать в обозримом будущем на вытеснение всех технологий какой-либо одной, хотя бы и такой многообещающей как АТМ.

Кроме того, локальные сети необходимо объединять с помощью глобальных связей друг с другом в территориально распределенные корпоративные сети, так как быстрый доступ ко всей корпоративной информации, разбросанной по многочисленным филиалам, стал сегодня одним из условий выживания предприятий в жесткой конкурентной борьбе. Так как глобальные связи - это не только выделенные линии, соединяющие локальные сети по топологии "точка-точка", но и связи через сети со своими методами передачи информации (например, сети X.25, ISDN, frame relay, SMDS и т.д.), то задача объединения их всех в одну сеть, прозрачную для транспортных операций конечных узлов, еще больше усложняется.

Часто термин *internetworking* используют для обозначения составной сети, включающей связи локальных сетей через глобальные, то есть как термин *внешнее межсетевое взаимодействие,* а для составной локальной сети используют термин *intranetworking,* то есть *внутреннее межсетевое взаимодействие.*

Мосты, описанные в предыдущих разделах, представляют собой хорошее средство для построения структурированных сетей, но их возможности ограничиваются в основном соединением фрагментов сетей одной или близких технологий. Соединение таких разнородных сетей, как X.25 и Ethernet для моста становится неразрешимой задачей по самому принципу его работы, так как для передачи пакетов через сеть X.25 ему необходимо выполнять ряд несвойственных для прозрачного моста операций: операцию сборки-разборки пакетов Ethernet с максимальным размером поля данных в 1500 байтов в 128-байтовые пакеты X.25, операцию установления соединения, операцию выбора моста для передачи пакетов в сеть X.25. Последняя операция необходима в том случае, если локальная сеть соединена с сетью X.25 в нескольких точках несколькими мостами, то есть необходимо выбрать наиболее подходящий мост для сокращения маршрута дальнейшего следования. Если эти функции реализовать в мосте, то это будет уже не мост, а устройство другого класса, а

именно маршрутизатор (или шлюз в традиционной терминологии пользователей сети Internet).

Основная идея введения сетевого уровня состоит в том, чтобы оставить в объединяемых сетях все особенности их технологий в неизменном в виде, но инкапсулировать в пакеты всех сетей единообразную информацию, позволяющую находить на ее основании адресата в сети любого типа.

Если провести хорошо работающую в неоднородном сетевом мире аналогию с общением людей, говорящих на разных языках, то сетевая информация - это общепринятый индекс страны, добавленный к письму, адрес назначения которого написан на одном из сотни языков земного шара, например, на хинди. И даже если это письмо должно пройти через множество стран, почтовые работники которых не знают хинди, понятный им индекс страны-адресата подскажет, через какие промежуточные страны лучше передать письмо, чтобы оно кратчайшим путем попало в Индию. А уже там работники местных почтовых отделений смогут прочитать точный адрес, указывающий город, улицу, дом и индивидуума и доставить письмо конечному пользователю, так как адрес написан на языке и в форме, принятой для данной страны.

Единообразная информация и составляет заголовок пакета сетевого уровня, который вставляется в пакеты любых форматов сетей, которые могут входить в интерсеть.

Основным полем заголовка сетевого уровня является номер сети-адресата. В рассмотренных нами ранее протоколах локальных сетей такого поля в кадрах предусмотрено не было - предполагалось, что все узлы принадлежат одной сети. Явная нумерация сетей позволяет протоколам сетевого уровня составлять точную карту межсетевых связей и выбирать рациональные маршруты при любой их топологии, используя альтернативные маршруты, если они имеются, что не умеют делать мосты.

Прежде, чем приступить к рассмотрению межсетевого взаимодействия, уточним, что понимается под термином "сеть".

Этот термин может употребляться в широком смысле (сеть - это совокупность связанных между собой компьютеров) и в узком смысле (сеть - это совокупность компьютеров, соединенных между собой в соответствии с одной из стандартных типовых топологий - шина, звезда, кольцо - и использующих для передачи пакетов внутри этого сообщества свой набор протоколов). В протоколах сетевого уровня термин "сеть" используется в узком смысле.

Кроме номера сети заголовок сетевого уровня должен содержать и другую информацию, необходимую для успешного перехода пакета из сети одного типа в сеть другого типа. К такой информации может относиться, например:

- номер фрагмента пакета, нужный для успешного проведения операций сборки-разборки фрагментов при соединении сетей с разными максимальными размерами пакетов,
- время жизни пакета, указывающее, как долго он путешествует по интерсети и которое может использоваться для уничтожения заблудившихся пакетов,
- информация о наличии и состоянии связей между сетями, помогающая узлам сети рационально выбирать межсетевые маршруты,
- информация о загруженности сетей, также помогающая согласовать темп посылки пакетов в сеть конечными узлами с реальными возможностями сетей на пути следования пакетов,
- качество сервиса - критерий выбора маршрута при межсетевых передачах - например, узел-отправитель может потребовать передать пакет с максимальной надежностью, возможно, в ущерб времени доставки.

На рисунке 16.20 приведена гипотетическая интерсеть, иллюстрирующая идею использования сетевого протокола. Интерсеть состоит из 6 сетей, к каждой из которых присоединены ее узлы, которые в соответствии с терминологией ISO называются конечными системами - ES (End System). Терминология ISO здесь используется для удобства, так как сети разных типов используют различные термины для обозначения одних и тех же понятий, что вносит путаницу при рассмотрении механизма межсетевого взаимодействия с общих позиций. Внутренняя структура каждой сети не показана, так как она не имеет значения с точки зрения сетевого протокола. Сети соединяются маршрутизаторами, которые ISO называет промежуточными системами - IS (Intermediate System).

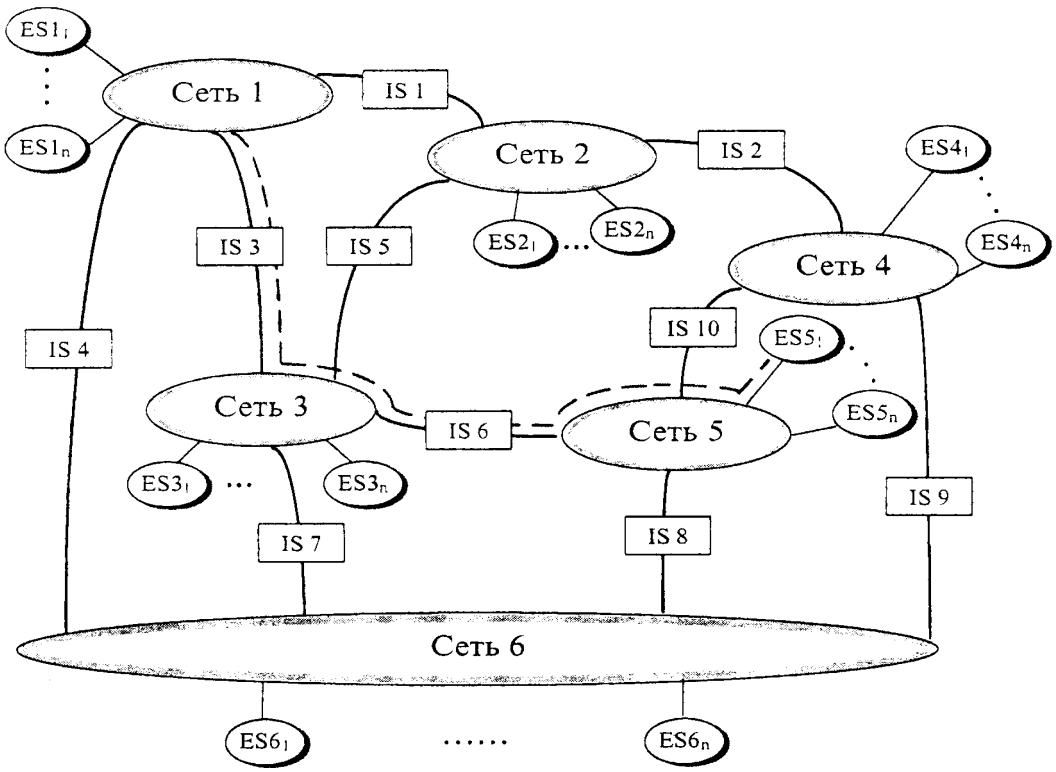


Рис. 16.20. Гипотетическая интерсеть.

ISN - промежуточная система/шлюз /маршрутизатор N,

ESN_n - конечная система /узел /хост n.

Каждая промежуточная система присоединена к нескольким сетям (по крайней мере к двум) и имеет в каждой такой сети локальный адрес, как и остальные конечные системы этой сети. Соответственно, промежуточная система должна поддерживать все протоколы, используемые в каждой из сетей, к которым она непосредственно присоединена.

Узел ES также обязан принимать участие в работе протокола сетевого уровня. Именно конечный узел формирует заголовок сетевого уровня с необходимой информацией, в том числе и адресом сети назначения, и вкладывает его в протокол своей сети, который для локальных сетей является протоколом канального уровня, таким как Ethernet или Token Ring. В служебном заголовке канального уровня конечный узел указывает локальный адрес маршрутизатора, подключенного к его сети, и отправляет ему кадр с вложенным пакетом сетевого уровня (если на канальном уровне протокольные блоки данных чаще называются кадрами, то на сетевом - пакетами, хотя принципиальной разницы между ними нет).

Маршрутизатор, получив кадр, извлекает из него заголовок сетевого уровня и решает, каким маршрутом лучше далее отправить этот пакет, если сеть назначения не подключена к нему непосредственно. Принятие решения о маршруте для него равнозначно принятию решения о выборе следующего маршрутизатора. После того, как выбор сделан, он упаковывает пакет в кадр сети, которая связывает его с выбранным маршрутизатором, указывает в кадре локальный адрес маршрутизатора и отправляет кадр по этой сети. В конце концов пакет приходит в сеть назначения, где маршрутизатор направляет его в соответствии с локальным адресом узлу назначения.

Важным вопросом является схема адресации узлов в отдельных сетях.

Описанный подход не требует наличия уникальных адресов и единой схемы адресации для внутрисетевой доставки пакета. После того, как пакет доставлен в нужную сеть за счет использования ее уникального номера, доставка в пределах этой сети осуществляется по ее правилам, и адрес узла внутри этой сети может быть традиционного для нее формата. Однако различия в форматах адресов узлов не очень удобны для реализации сетевого протокола, так как адрес узла назначения необходимо
поместить в заголовок сетевого уровня - в заголовке канального уровня в случае пути, проходящего через несколько сетей, указывается локальный адрес маршрутизатора, который должен передать пакет в другую сеть. Поэтому в некоторых сетевых протоколах, например, IP, локальные адреса узлов имеют единый формат, не зависящий от локального формата адреса сети. Другие же сетевые протоколы, например. IPX, используют в качестве адреса узла в сетевом заголовке локальный адрес, но это ограничивает использование протокола IPX только такими сетями, адрес которых умещается в отведенные ему 6 байтов.

Маршрутизатор выбирает маршрут на основании его представления о текущей конфигурации сети и соответствующего критерия выбора маршрута. Обычно в качестве критерия выступает время прохождения маршрута, которое в локальных сетях совпадает с длиной маршрута, измеряемой в количестве пройденных узлов маршрутизации (в глобальных сетях это не так, там принимается в расчет и время передачи пакета по каждой линии связи).

В сложных составных сетях почти всегда существует несколько альтернативных маршрутов для передачи пакетов между двумя конечными узлами. Так, в нашем примере для передачи пакетов от узла ESI.I сети 1 узлу ES5.1 сети 5 существует несколько альтернативных маршрутов, из которых наиболее очевидными представляются:

ES1.1→ IS3 → СЕТЬ 3 → IS 6 → СЕТЬ 5 → ES5.1

ES1.1 → IS4 → СЕТЬ 6 → IS 8 → СЕТЬ 5 → ES5.1

ES1.1 → IS1 → СЕТЬ 2 → IS 2 → СЕТЬ 4 → IS 10 → СЕТЬ 5 → ES5.1,

если считать, что все маршрутизаторы и сети работоспособны, и производительность и надежность сетей и связей между ними одинакова.

Хотя мы смогли достаточно легко определить несколько возможных маршрутов просто при рассмотрении топологии интерсети, для того, чтобы на практике конечные узлы и маршрутизаторы смогли решить поставленную задачу, необходимо найти ответы на ряд вопросов:

- Как конечный узел может узнать локальный адрес маршрутизатора или маршрутизаторов, присоединенных к его сети?
- Как маршрутизатор может определить локальный адрес конечных узлов, присоединенных к его сетям?

• Каким образом конечный узел может выбрать подходящий маршрутизатор в своей сети для отправки пакета через интерсеть, если таких маршрутизаторов несколько?

• Каким образом маршрутизатор может узнать локальный адрес других маршрутизаторов, присоединенных к его сетям?

• Каким образом маршрутизатор выбирает следующий маршрутизатор при выборе рационального маршрута пакета?

Существует большое количество протоколов сетевого уровня, каждый из которых по своему отвечает на эти вопросы.

Для облегчения решения поставленных задач разработчики сетей разделили протоколы сетевого уровня на три класса. Протоколы первого класса называют собственно протоколами сетевого уровня. Эти протоколы (например, IP, IPX, AppleTalk) переносят пользовательские данные вместе со служебным заголовком сетевого уровня, который включает информацию об адресе сети и узла, а также некоторую дополнительную информацию, описанную выше.

Протоколы второго класса называют протоколами маршрутизации, и они выполняют служебные функции для маршрутизаторов - переносят в своем поле данных информацию о топологии связей интерсети. С помощью этих протоколов маршрутизаторы составляют карту связей сети той или иной степени подробности и принимают решение о том, какому следующему маршрутизатору нужно передать пакет для образования рационального пути. Примерами таких протоколов являются протоколы IPX RIP, IP RIP, EGP, BGP, OSPF, IS-IS.

Служебная информация протоколов маршрутизации, иногда называемых также протоколами обмена маршрутной информацией, хранится в поле данных пакета сетевого уровня и имеет еще и свой собственный служебный заголовок, поэтому с точки зрения вложенности пакетов протоколы маршрутизации следует отнести к более высокому уровню, чем сетевой. Но функционально они решают общую задачу на сетевом уровне - доставляют кадры отдельных сетей нужному адресату через разнородную составную сеть.

Протоколы третьего класса отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети. Очевидно, что они нужны только в случае, если сетевой протокол использует в своих заголовках адреса конечных узлов, отличные от локальных (например, так делает протокол IP). Если же на сетевом уровне используются локальные адреса, то надобность в протоколах этого класса отпадает. Такие протоколы часто называют протоколами разрешения адресов - Address Resolution Protocol. ARP. Иногда их относят не к сетевому уровню, а к канальному, хотя тонкости классификации не изменяют их сути.

Необходимо заострить внимание на том, что существование нескольких протоколов сетевого уровня (IP, IPX, DECnet, AppleTalk, XNS и т.д.) в принципе противоречит идее объединения сетей на основе одного протокола сетевого уровня, который и несет унифицированную для всех сетей адресную информацию - номер сети. Если же в разных частях интерсети будут использоваться разные сетевые протоколы, то эти части взаимодействовать не смогут. По крайней мере средствами сетевого уровня их объединить уже нельзя.

Для объединения сетей с различными сетевыми протоколами используются шлюзы (gateways), которые привлекают для решения этой задачи информацию прикладного уровня. Шлюзы - это продукты, выполняющие функцию согласования работоспособности на всех уровнях, называемую *interoperability*. В то время как термин internetworking обозначает взаимодействие сетей только на

нижних уровнях, непосредственно связанных с транспортировкой пакетов, в понятие interoperability входит обеспечение согласования верхних уровней стека коммуникационных протоколов, реализуемых серверами и редиректорами операционных систем и некоторыми сетевыми приложениями.

Тем не менее и при отсутствии шлюзов можно говорить об общей интерсети, даже если в ее разных сетях работают разные сетевые протоколы. При этом возможны различные варианты работы:

• При наличии многопротокольных маршрутизаторов, то есть таких промежуточных систем, которые одновременно могут обрабатывать пакеты с различными сетевыми заголовками, интерсеть представляет собой совокупность непересекающихся интерсетей, использующих общие каналы связи и общие кадры канального уровня, но никак не взаимодействующих между собой.

• При наличии многопротокольных конечных узлов образуется общая интерсеть, так как конечные узлы принимают и понимают сетевые пакеты любых типов.

Очевидно, что для каждого сетевого протокола конечный узел будет адресоваться оригинальным способом. Так, для протокола IP у него будет один номер сети и узла, а для протокола IPX это будет совсем другая пара чисел.

Большинство современных маршрутизаторов почти всегда поддерживает несколько протоколов сетевого уровня, являясь мультипротокольными, что облегчает построение гетерогенных сетей.

Несмотря на большое разнообразие протоколов сетевого уровня, обусловленное длительной историей развития сетевых технологий, в последнее время наметился явный лидер - протокол IP сети Internet, который имеет хорошие перспективы по оценкам многих специалистов стать на ближайшие 4 - 5 лет основным объединяющим протоколом сетей всех типов - и локальных, и глобальных. Поэтому мы наиболее подробно рассмотрим именно этот протокол, реализованный во всех маршрутизаторах и популярных сетевых операционных системах, включая Novell NetWare, традиционно ориентировавшуюся на протокол IPX.

16.4.2. Протоколы сетевого и транспортного уровней IP, TCP, UDP, IPX

Протокол IP

Протокол IP (Internet Protocol) является наиболее эффективным на сегодняшний день протоколом образования больших интерсетей. Особенно он эффективен при построении сетей на основе медленных глобальных связей, так как он изначально разрабатывался для работы в таких условиях. Многолетняя проверка и усовершенствования этого протокола в сети Internet гарантируют его высокую степень отлаженности.

Основные характерные черты протокола IP:

•Стандарты протокола IP принимаются на основании открытого обсуждения сообществом Internet так называемых "Запросов для комментария" - Request For Comment (RFC). Каждый стандарт имеет порядковый номер, например, RFC-791 является общим описанием протокола IP, а RFC-1624 описывает порядок вычисления контрольной суммы IP-пакета.

•Протокол IP является протоколом дейтаграммного типа.

•Гибкая система адресации. Как адрес сети, так и адрес узла задаются администратором для каждого компьютера как параметры при конфигурировании стека TCP/IP в операционной системе, независимо от MAC-адреса сетевого

адаптера. Преимущества - независимость адреса узла от адреса используемого в нем оборудования. Недостаток - трудоемкость ручного конфигурирования адресов в больших сетях. Для IP-сетей разработан протокол DHCP, позволяющий автоматизировать процесс раздачи IP-адресов узлам сети с одного сервера. Существует 5 классов IP-адресов, отличающихся границей между номером сети и номером узла в 4-х байтовом общем адресном поле. Классы различаются по значению нескольких старших битов первого байта адреса. Небольшая длина IP-адреса определяет небольшую длину IP-заголовка - 20 байтов, что при максимальной длине IP-пакета в 64 Кбайта дает небольшие накладные расходы на служебную информацию. Примеры IP-адресов: 192.33.81.15,100.15.23.34.

• Отсутствие широковещательного адреса для сети (широковещательность поддерживается только для узлов одной определенной сети) позволяет избежать широковещательных штормов без участия администратора.

• Наличие класса групповых адресов - multicast - с помощью которых один пакет доставляется всем узлам - членам группы с заданным адресом.

• Возможность гибкого задания границы между номером сети и номером узла при использовании в маршрутизаторах и компьютерах масок. Например, адрес 101.23.45.16 с маской 255.255,255 соответствуют сети 101.23.45 и номеру узла 16. Маски помогают делить одну сеть на подсети без приобретения у поставщика услуг Internet новых IP-адресов сетей.

• Использование иерархических символьных имен компьютеров, например www. ibm. com, понятных пользователю. Каждая часть имени соответствует одному административному домену, находящемуся под управления какого-либо административного органа сети Internet или ее поставщика услуг.

• Использование иерархической службы имен DNS для предоставления компьютерам справок о соответствии символьных имен IP-адресам, используемым в IP-пакетах. Служба DNS не использует широковещательные рассылки при своей работе, а основана на распределенной иерархической базе данных с прозрачным доступом. Каждый административный домен имеет свой DNS-сервер или DNS-серверы, в которых хранится их часть базы данных имен, При разрешении имени серверы DNS взаимодействуют прозрачным для клиента образом. Пока служба DNS не взаимодействует с сервисом назначения адресов DHCP, хотя разработка нового протокола Dynamic DNS, который будет взаимодействовать с DNS, уже идет.

• Инкапсуляция IP-пакетов в кадры локальных или глобальных сетей определена соответствующими стандартами Internet, например, стандарт RFC-1226 определяет

инкапсуляцию IP в пакеты сетей X.25, стандарт RFC-1490 - инкапсуляцию в кадры frame relay, а стандарт RFC-894 - инкапсуляцию в кадры Ethernet.

• Соответствие IP-адресов MAC-адресам сетевых адаптеров устанавливается протоколами семейства ARP (Address Resolution Protocol), которые определяются отдельно для каждого вида сетей, которые переносят IP-пакеты.

• Возможность фрагментации пакетов верхних уровней (то есть разбиения их на части без дублирования заголовков) обеспечивается за счет наличия специальных полей в заголовке IP-пакета, позволяющих разбивать пакеты на части при переходе в сеть с меньшим максимально допустимым размером кадра, а затем собирать из отдельных частей исходный пакет протокола верхнего уровня, например, TCP.

• Возможность указания класса обслуживания IP-пакетов маршрутизаторами: с низкой задержкой, с максимальной производительностью и с наивысшей надежностью.

• Достаточно большое максимальное значение поля "Время жизни" IP-пакета, определяемое его форматом в один байт. Это позволяет пакету пересечь

до 254 маршрутизаторов и не быть удаленным из сети, что важно для сверхбольших сетей. Реальное используемое начальное значение этого поля зависит от настройки конкретной операционной системы в компьютере-источнике.

Протоколы TCP и UDP

Протоколы транспортного уровня не используются для маршрутизации пакетов, а служат для повышения надежности доставки данных протоколов прикладного уровня, а также мультиплексируют протокол сетевого уровня с различными протоколами прикладного уровня.

Протокол UDP (User Datagram Protocol) так же, как IP является дейтаграммным протоколом, поэтому надежности при передаче данных прикладных протоколов он не прибавляет, а является просто мультиплексором между протоколом IP и такими протоколами как TFTP, BOOTP и др. Мультиплексирование происходит на основании таких полей пакета UDP, как порт источника данных и порт назначения данных. Номер порта соответствует определенному протоколу прикладного уровня или же определенной функции какого-либо протокола. Например, порт 67 закреплен за сервером протокола BOOTP, а порт 68 - за клиентом этого протокола.

Протокол TCP также выполняет роль мультиплексора между протоколом IP и протоколами прикладного уровня, за которыми также закреплены соответствующие значения портов пакета TCP. Однако TCP выполняет и вторую функцию протоколов транспортного уровня - он обеспечивает надежную передачу пакетов за счет установления соединения и нумерации пакетов по алгоритму скользящего окна. Номером соединения является пара конечных точек соединения, где конечная точка сама образуется из пары (номер узла, номер порта) приложения.

По сравнению с образованием виртуального канала, когда каждому соединению присваивается номер виртуального канала, который затем указывается в пакетах транспортного уровня для маршрутизации пакетов, использование обозначения соединений парой конечных точек позволяет стеку TCP/IP маршрутизировать каждый
IP-пакет отдельно, что повышает производительность и отказоустойчивость сети, и в то же время нумеровать TCP пакеты внутри, каждого соединения, обеспечивая их надежную доставку.

Маршрутизаторы для выполнения своих функций обычно работают только с заголовками пакетов сетевого уровня, то есть с IP-заголовками, но при выполнении функций фильтрации трафика могут просматривать и заголовки пакетов транспортного уровня, что позволяет использовать номер порта как условие фильтрации и в гораздо более удобной форме, чем при использовании мостов, запрещать использование того или иного сервиса (идентифицируемого номером порта) всем пользователям или определенному пользователю (на основании его IP-адреса).

Протокол IPX

Протокол IPX, так же, как и IP, является протоколом дейтаграммного типа. Однако он разрабатывался для применения в локальных сетях и поэтому некоторые возможности, имеющиеся в протоколе IP, не поддерживает.

Адрес получателя в протоколе IPX - это межсетевой адрес, который содержит три поля, а именно: номер сети (32 бита), номер узла (48 битов) и номер сокета (16 битов).

• Номер сети идентифицирует каждый сегмент в общем случае многосерверной сети; эти номера назначают администраторы сети, когда инициализируют файл-серверы.

• Адрес узла является MAC-адресом узла, то есть в данном случае на сетевом уровне используется локальный адрес узла.

• Сокет (socket - гнездо или разъем) определяет собственно прикладную программу-получатель, работающую на станции назначения. Прикладные программы открывают и закрывают сокеты во многом так же, как они открывают и закрывают файлы.

Наличие поля сокета (аналога порта протоколов UDP и TCP) в пакете IPX говорит о том, что этот протокол поддерживает не только маршрутизацию в составных сетях, но и выполняет роль мультиплексора по отношению к протоколам прикладного уровня. В стеке Novell это свойство явным образом используется при работе файлового сервиса -протокол NCP непосредственно работает с протоколом IPX, минуя транспортный протокол SPX, что уменьшает накладные расходы, связанные с многоуровневостью.

Протокол IPX является одним из наиболее легко настраиваемых протоколов сетевого уровня. Номер сети задается администратором только на серверах, а номер узла вообще вручную не задается, так как он автоматически считывается из сетевого адаптера компьютера. Административные издержки при конфигурировании сети сводятся из-за этого к минимуму. При этом отпадает необходимость в использовании протокола типа ARP. выясняющего соответствие между сетевыми адресами узлов и их MAC-адресами. Однако при смене сетевого адаптера нужно скорректировать адрес узла, если для его выяснения используется справочная служба типа NDS.

В версии стека IPX для локальных сетей соответствие символьных имен серверов их сетевым адресам устанавливалось с помощью широковещательного протокола Service Advertising Protocol (SAP), поэтому проблем при смене у сервера сетевого адаптера не возникало, Однако широковещательные рассылки - не очень хороший способ взаимодействия в глобальной сети, недаром в стеке TCP/IP они для выяснения соответствия символьных имен IP-адресам не используются. Модернизируя свой стек для применения в глобальных сетях, компания Novell использует теперь справочную службу NDS для нахождения разнообразной информации о имеющихся в сети ресурсах и сервисах, в том числе и о соответствии имени сервера его сетевому адресу. Так как служба NDS поддерживается только серверами с версией NetWare 4 и выше, то для работы с версиями NetWare 3.x маршрутизаторы распознают пакеты SAP по номеру их определенного сокета и передают их на все порты, имитируя широковещательные рассылки локальной сети, что, конечно, съедает значительную часть пропускной способности медленных глобальных линий.

Еще несколько особенностей протокола IPX ограничивают его применение в глобальных сетях.

• Отсутствие полей, поддерживающих фрагментацию пакетов верхнего уровня, требует задания такого размера пакета **IPX,** который бы гарантированно уложился бы во все кадры локальных и глобальных сетей на всем пути следования по составной сети. Возможно поэтому длина поля данных пакета **IPX** ограничена 546 байтами. При заголовке в 30 байтов (его большая длина связана с большим размером адреса, включающего 6-байтовый MAC-адрес узла) накладные расходы на служебную информацию оказываются достаточно большими.

• Время жизни пакета ограничено числом 15, что может оказаться недостаточным для большой сети.

• Отсутствие поля качества сервиса не позволяет маршрутизаторам автоматически подстраиваться к требованиям приложения по передаче трафика.

Следующее ограничение относится к протоколу NCP, так как именно он обеспечивает надежную передачу данных между клиентом и сервером, являясь протоколом с установлением соединения. Этот протокол не использует метод скользящего окна при передаче своих пакетов, а просто не отправляет очередной пакет до прихода подтверждения о приеме предыдущего пакета. Такой метод нормально работает в быстродействующих локальных сетях, но очень медленно передает данные на медленных глобальных связях.

В последних версиях NetWare компания Novell произвела много необходимых модификаций в своем стеке для его успешной работы в глобальных сетях:

• Имеется NLM для реализации метода скользящего окна - так называемый Burst Mode Protocol NLM.

• Имеется NLM для поддержки длинных IPX-пакетов - Large Internet Packet NLM.

• Использование службы NDS позволяет отказаться от широковещательного протокола SAP.

Кроме того, постоянное повышение скорости глобальных сервисов уменьшает недостатки оригинальных протоколов стека IPX, что позволяет некоторым обозревателям говорить об успешной работе операционной системы NetWare в глобальных сетях и без указанных нововведений.

16.4.3. Протоколы маршрутизации RIP и OSPF.

Протоколы маршрутизации позволяют маршрутизаторам в составной сети получать информацию о топологии связей в сети, на основе которой можно принимать решения о выборе рационального пути прохождения пакетов через сеть.

Протоколы маршрутизации работают на основании различных алгоритмов, которые можно разделить на три больших класса:

• алгоритмы фиксированной маршрутизации,
• алгоритмы простой маршрутизации,
• алгоритмы адаптивной маршрутизации,

Независимо от того, на основании какого протокола и в какой форме получена маршрутизатором информация о топологии связей в сети, почти у всех алгоритмов маршрутизации имеется одна и та же конечная цель - *таблица маршрутов,* которая говорит о том, какому маршрутизатору, непосредственно связанному с данным, нужно передать пакет с определенным адресом сети назначения.

Следующая таблица (табл. 16.4.) представляет собой типичный пример таблицы маршрутов, использующей IP-адреса сетей:

Таблица маршрутов используется при принятии решения о передаче пакета - если в ней имеется несколько строк для одной и той же сети, то выбирается та, в которой расстояние до конечной сети меньше.

При этом под расстоянием понимается любая метрика, используемая в соответствии с заданным в сетевом пакете классом сервиса. Это может быть и время прохождения пакета по линиям связи, и надежность линий связи, и загруженность линий связи в данный момент времени и любая другая величина, определенная в соответствующем сетевом протоколе. Если маршрутизатор

Таблица 16.4.

Адрес сети назначения	Номер выходного порта	Расстояние до конечной сети
129.13.0.0	1	20
116.0.0.0	2	30
202.101.45.0	1	1450
213.34.6.0	3	2150
56.0.0.0	2	40
56.0.0.0	1	1300
default	1	

поддерживает несколько классов сервиса пакетов, то таблица маршрутов составляется и применяется отдельно для каждого вида сервиса.

Очевидно, что если алгоритм маршрутизации вырабатывает в результате своей работы подобную таблицу, то принятие решения о выборе маршрута разбивается на несколько этапов - каждый маршрутизатор выбирает только один шаг составного маршрута. Тем не менее, в зависимости от принятого алгоритма маршрутизации, он может это делать на основании общей картины всех связей в сети.

Обычно в каждом маршрутизаторе существует порт, на который пакеты передаются по умолчанию, если адрес сети назначения не присутствует в явном виде в таблице (default port или default route). Часто порт по умолчанию связан с магистралью сети, так что пакеты, попав на магистраль, попадут в конце концов в маршрутизатор, знающий их сеть назначения.

Фиксированная маршрутизация.

Этот алгоритм применяется в сетях с простой топологией связей и основан на ручном составлении таблицы маршрутизации администратором сети. Алгоритм часто эффективно работает также для магистралей крупных сетей, так как сама магистраль может иметь простую структуру с очевидными наилучшими путями следования пакетов в подсети, присоединенные к магистрали.

Различают однопутевые таблицы, в которых для каждого адресата задан один путь, и многопутевые таблицы. В многопутевых таблицах имеется несколько альтернативных путей для каждого адресата и правило выбора одного из них. Чаще всего один путь является основным, а остальные - резервными.

Простая маршрутизация.

Алгоритмы простой маршрутизации подразделяются на три подкласса:

• Случайная маршрутизация - пакеты передаются в любом, случайном направлении, кроме исходного.

• Лавинная маршрутизация - пакеты передаются во всех направлениях, кроме исходного (применяется в мостах для пакетов с неизвестным адресом доставки).

• Маршрутизация по предыдущему опыту - таблицы маршрутизации составляются на основании данных проходящих через маршрутизатор пакетов. Именно так работают прозрачные мосты (единственное, что отличает их работу - отсутствие информации о расстоянии до адресата). Приспособление в этом виде маршрутизации к изменениям топологии сети достаточно медленное.

Адаптивная маршрутизация.

Это основной вид алгоритмов маршрутизации, применяющихся в современных сетях со сложной топологией. Основан на периодическом обмене маршрутизаторами специальной топологической информацией о имеющихся в интерсети сетях, а также о связях между маршрутизаторами. Обычно учитывает не только топологию связей, но и их производительность и состояние.

Адаптивные протоколы обмена маршрутной информацией, применяемые в настоящее время в вычислительных сетях, основаны на двух различных группах алгоритмов - *дистанционно-векторных алгоритмах (Distance Vector Algorithms, DVA) и алгоритмах состояния связей (Link State Algorithms, LSA).*

Это динамические распределенные протоколы, которые позволяют всем маршрутизаторам собрать информацию о топологии связей в сети, адаптивно отрабатывая все изменения конфигурации связей. Распределенность их состоит в том, что в сети отсутствует один или несколько выделенных маршрутизаторов, которые собирают и обобщают топологическую информацию, эта работа распределена между всеми маршрутизаторами.

В алгоритмах *дистанционно-векторного типа* каждый маршрутизатор периодически и широковещательно рассылает по сети вектор расстояний от себя до всех известных ему сетей. Под расстоянием обычно понимается число промежуточных маршрутизаторов (число так называемых "хопов", то есть прыжков, от английского hop), через которые, пакет должен пройти, прежде чем попадет в соответствующую сеть (может использоваться и другая метрика, учитывающая не только число перевалочных пунктов, но и время прохождения пакетом по связи между соседними маршрутизаторами). Получив вектор от соседнего маршрутизатора, каждый маршрутизатор добавляет к нему информацию об известных ему других сетях, о которых он узнал непосредственно (если они подключены 1 к его портам) или из аналогичных объявлений других маршрутизаторов, а затем рассылает новое значение вектора снова по сети, В конце концов каждый маршрутизатор узнает информацию об имеющихся в интерсети сетях и о расстоянии до них через соседние маршрутизаторы.

Дистанционно-векторные алгоритмы хорошо работают только в небольших сетях. В больших сетях они засоряют линии связи интенсивным широковещательным трафиком, к тому же изменения конфигурации могут отрабатываться по этому алгоритму не всегда корректно, так как маршрутизаторы не имеют точного представления о топологии связей в сети, а располагают только обобщенной информацией - вектором дистанций, к тому же полученной из вторых рук.

Наиболее распространенным протоколом, основанным на дистанционно-векторном алгоритме, является протокол RIP, который распространен в двух версиях - RIP IP, работающий с протоколом IP, и RIP IPX, работающий с протоколом IPX.

Алгоритмы состояния связей обеспечивают каждый маршрутизатор информацией, достаточной для построения точного графа связей сети. Все маршрутизаторы работают на основании одинаковых графов, что делает процесс маршрутизации более устойчивым к изменениям конфигурации. Широковещательная рассылка используется здесь только при изменениях состояния связей, что происходит в надежных сетях не так часто.

Для того, чтобы понять, в каком состоянии находятся линии связи, подключенные к его портам, маршрутизатор периодически обменивается

короткими пакетами со своими ближайшими соседями. Этот трафик также широковещательный, но он циркулирует только между соседями и не так засоряет сеть.

Протоколами, основанными на алгоритме состояния связей, являются протоколы IS-IS (Intermediate System to Intermediate System) стека OSI, OSPF (Open Shortest Path First) стека TCP/IP и NLSP стека Novell, реализованный совсем недавно.

Протокол OSPF имеет ряд особенностей, специально ориентированных на использование в больших корпоративных сетях. К ним относятся:

• Применение процедур аутентификации маршрутизаторов, исключающих внедрение в сеть "злоумышленников", отводящих трафик с помощью нелегальных маршрутизаторов.

• Использование поля качества сервиса в пакете IP для автоматической балансировки загрузки параллельных линий,

• Отказ от обязательного присваивания IP-адресов портам, работающим на выделенные линии, что упрощает работу администратора при конфигурировании маршрутизатора и экономит IP адреса.

• Возможность разбиения большой сети на области администрирования. Области импортируют только конечные таблицы маршрутизации других областей, а не детальные сведения о топологии связей каждой области. Это позволяет существенно уменьшить размер базы данных топологической информации, с которой работает каждый маршрутизатор большой сети.

• Возможность импорта таблиц маршрутизации из частей сети, называемых автономными системами, в которых работают отличные от OSPF протоколы маршрутизации. Это дает возможность оставлять в неизменном виде маршрутизаторы небольших сетей, работающие по протоколу RIP, применяя в остальной части корпоративной сети протокол OSPF.

16.4.4. Типы и характеристики маршрутизаторов

Основная функция маршрутизатора - чтение заголовков пакетов сетевых протоколов, принимаемых и буферизуемых по каждому порту (например, IPX, IP, AppleTalk или DECnet), и принятие решения о дальнейшем маршруте следования пакета по его сетевому адресу, включающему, как правило, номер сети и номер узла.

Маршрутизатор выбирает наилучший маршрут в сети, используя различные критерии и различные алгоритмы маршрутизации, часто достаточно сложные с математической точки зрения (интенсивных вычислений требуют протоколы, основанные на алгоритме LSA, вычисляющие оптимальный путь на графе - протоколы OSPF, NLSP, IS-IS). Поэтому маршрутизатор является обычно мощным вычислительным устройством с одним или даже несколькими процессорами, чаще всего RISC-архитектуры, со сложным программным обеспечением. То есть сегодняшний маршрутизатор - это специализированный компьютер, имеющий скоростную внутреннюю шину или шины (с пропускной способностью 600 - 2000 Мб/с), часто использующий симметричное или ассиметричное мультипроцессирование и работающий под управлением специализированной операционной системы, относящейся к классу систем реального времени.

Маршрутизаторы могут поддерживать только один протокол сетевого уровня, например, IPX или DECnet, а могут поддерживать и большое количество таких протоколов. Чем больше протоколов сетевого уровня поддерживает маршрутизатор, тем лучше он подходит для использования в корпоративной сети.

Большая вычислительная мощность позволяет маршрутизаторам наряду с основной работой по выбору оптимального маршрута выполнять и ряд вспомогательных высокоуровневых функций.

Практика применения маршрутизаторов разделяет их по областям применения на три класса:

Магистральные маршрутизаторы (backbone routers) предназначены для построения центральной сети корпорации и соединения их с помощью магистральных высокоскоростных и многопротокольных связей с сетями региональных отделений корпораций.

Центральная сеть может состоять из большого количества локальных сетей, разбросанных по разным зданиям и использующих самые разнообразные сетевые технологии, типы компьютеров и операционных систем.

Маршрутизаторы региональных отделений соединяют региональные отделения между собой и с центральной сетью. Сеть регионального отделения, также как и центральная сеть, может состоять из нескольких локальных сетей.

Маршрутизаторы удавленных офисов соединяют как правило единственную локальную сеть удаленного офиса с центральной сетью или сетью регионального отделения.

Различные области применения предъявляют различные требования к основным и дополнительным функциям маршрутизаторов.

На рисунке 16.21 показана упрощенная схема областей использования маршрутизаторов основных трех типов.

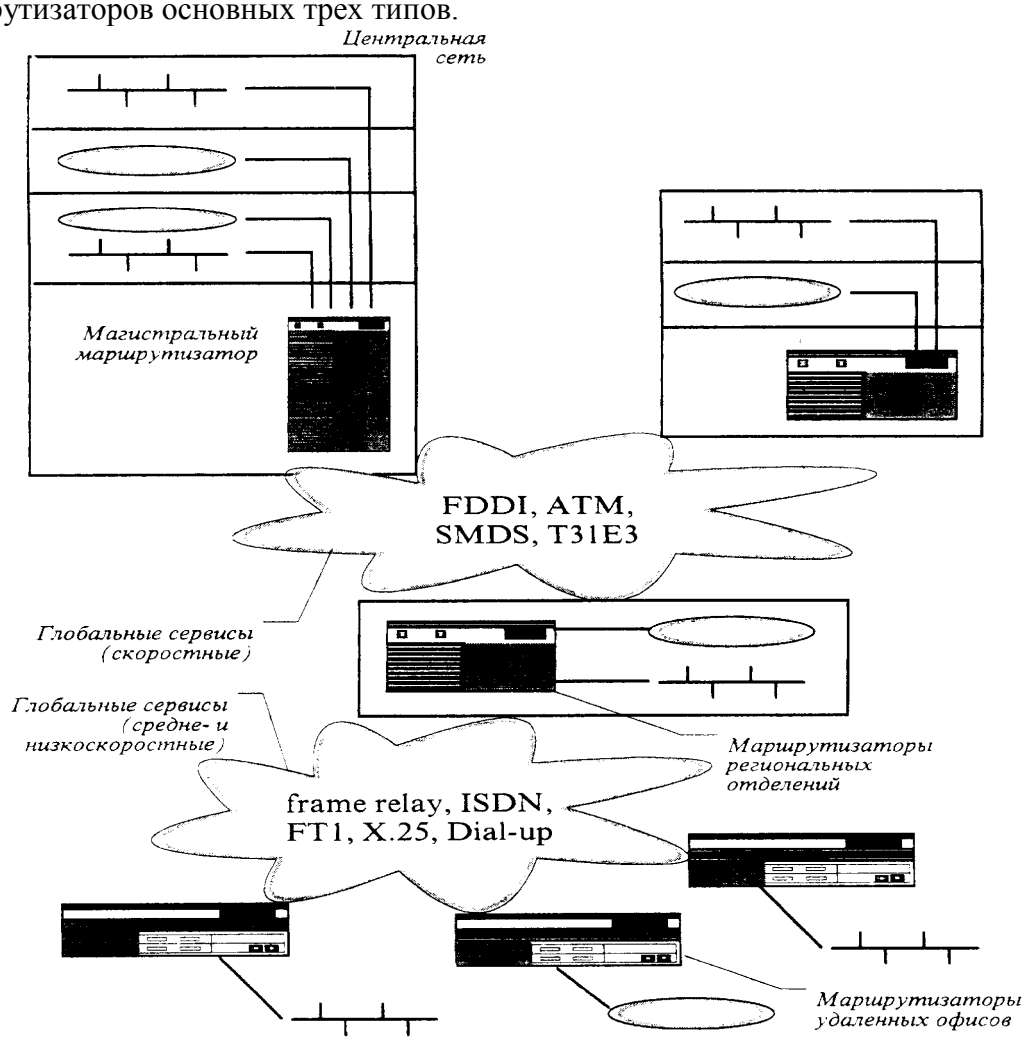


Рис. 16.21. Упрощенная схема использования маршрутизаторов различных типов.

В отношении основной функции маршрутизатора можно выделить **несколько основных характеристик,** определяющих возможности и сферу применения маршрутизатора.

Перечень поддерживаемых сетевых протоколов.

Магистральный маршрутизатор должен поддерживать большое количество сетевых протоколов и протоколов маршрутизации, чтобы поддерживать трафик всех существующих на предприятии вычислительных систем (в том числе и устаревших, но все еще успешно эксплуатирующихся), а также систем, которые могут появиться на предприятии в ближайшем будущем. Если центральная сеть связывается с региональными отделениями через Internet, то, возможно, потребуется поддержка и специфических протоколов маршрутизации этой сети, таких как EGP и BOP. Программное обеспечение магистральных маршрутизаторов обычно строится по модульному принципу, поэтому при возникновении потребности можно докупать и добавлять модули, реализующие недостающие протоколы.

Перечень поддерживаемых сетевых протоколов обычно включает протоколы IP, CONS и CLNS OSI, IPX, AppleTalk, DECnet, Banyan VINES, Xerox XNS.

Перечень протоколов маршрутизации: IP RIP, IPX RIP, NLSP, OSPF, IS-IS OSI, EGP, BGP, VINES RTP, AppleTalk RTMP.

Перечень поддерживаемых интерфейсов локальных и глобальных сетей для передачи пакетов по сетям, непосредственно подключенным к портам маршрутизатора.

Для локальных сетей - это интерфейсы, реализующие физические и канальные протоколы сетей Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN и ATM.

Для глобальных связей - это интерфейсы физического уровня для связи с аппаратурой передачи данных, а также протоколы канального и сетевого уровня, необходимые для подключения к глобальным сетям с коммутацией каналов и пакетов (набор этих протоколов часто называется глобальным сервисом).

Поддерживаются интерфейсы последовательных линий (serial lines) RS-232, RS-449/422. V. 35 (для передачи данных со скоростями до 2 - 6 Мб/с), высокоскоростной интерфейс HSSI. обеспечивающий скорость до 52 Мб/с, а также интерфейсы с цифровыми глобальными каналами T1/E1, T3/E3 и ISDN BRI и PRI. Некоторые маршрутизаторы включают аппаратуру связи с цифровыми глобальными каналами, что исключает необходимость использования внешних устройств сопряжения с этими каналами.

В набор поддерживаемых глобальных сервисов обычно входят сервисы сетей X.25, frame relay, ISDN и коммутируемых аналоговых телефонных сетей, сетей ATM, а также поддержка протокола канального уровня PPP.

Общая производительность маршрутизатора, измеряемая в 64-байтовых пакетах в секунду.

Высокая производительность маршрутизации важна для работы с высокоскоростными локальными сетями, а также для поддержки новых высокоскоростных глобальных технологий, таких как frame relay, T3/E3 и ATM. Общая производительность маршрутизатора зависит от многих факторов, наиболее важными из которых являются: тип используемых процессоров, эффективность программной реализации протоколов, архитектурная организация вычислительных и интерфейсных модулей. Общая производительность

маршрутизаторов колеблется от нескольких десятков тысяч пакетов в секунду до сотен тысяч (верхний предел, достигнутый на сегодня - миллион пакетов в секунду). Наиболее производительные маршрутизаторы имеют мультипроцессорную архитектуру, сочетающую симметричные и асимметричные свойства - несколько мощных центральных процессоров по симметричной схеме выполняют функции вычисления маршрутной таблицы, а менее мощные процессоры в интерфейсных модулях занимаются передачей пакетов на подключенные к ним сети и пересылкой пакетов на основании части таблицы маршрутизации, кэшированной в локальной памяти интерфейсного модуля.

Магистральные маршрутизаторы обычно поддерживают максимальный набор протоколов и интерфейсов и обладают высокой общей производительностью. Маршрутизаторы удаленных офисов поддерживают один-два протокола локальных сетей и низкоскоростные глобальные сервисы, общая производительность таких маршрутизаторов обычно составляет от 5 до 20-30 тысяч пакетов в секунду.

Маршрутизаторы региональных отделений занимают промежуточное положение, и их поэтому иногда не выделяют в отдельный класс устройств.

Наряду с функцией маршрутизации, интеллектуальные маршрутизаторы обладают следующими важными расширенными возможностями:

Приоритеты протокола. Можно установить приоритет одного протокола сетевого уровня над другими. Это бывает полезно в случае недостаточной полосы пропускания кабельной системы и существования трафика, чувствительного к временным задержкам, например, трафика SNA.

Защита от "штормов" широковещательных пакетов (broadcast storm).

Одна из характерных неисправностей сетевого оборудования - самопроизвольная генерация с высокой интенсивностью широковещательных пакетов. Обычный мост слепо передает такие пакеты во все стороны, засоряя таким образом сеть. Борьба с широковещательным штормом в сети, соединенной мостами, требует от администратора отключения портов, генерирующих широковещательные пакеты.

Маршрутизатор не распространяет такие поврежденные пакеты, потому что в его обязанности не входит копирование широковещательных пакетов во все объединяемые им сети.

Поддержка немаршрутизируемых протоколов, таких как NetBIOS, NetBEUI или LAT, которые не оперируют с таким понятием, как сеть. Маршрутизаторы могут обрабатывать пакеты таких протоколов двумя способами. В первом случае они могут работать с пакетами этих протоколов как мосты, то есть передавать их на основании изучения MAC-адресов. Другим способом передачи пакетов немаршрутизируемых протоколов является *инкапсуляция* этих пакетов в пакеты какого-либо сетевого протокола. Некоторые производители маршрутизаторов разработали собственные протоколы, специально предназначенные для инкапсуляции немаршрутизируемых пакетов. Кроме того, существуют стандарты для инкапсуляции некоторых протоколов в другие, в основном в IP.

Примером такого стандарта является протокол DLSw, определяющий методы инкапсуляции пакетов SDLC в пакеты IP.

Трансляция протоколов канального *уровня.* Эта важная функция была одной из основных причин применения маршрутизаторов для объединения сетей с разными протоколами канального уровня, например Ethernet и Token Ring,

Совмещение функций моста и маршрутизатора. Удобно, когда по желанию администратора одно и то же устройство может выполнять по отношению к некоторым протоколам или портам функции моста, образуя сегменты, а по

отношению к другим протоколам или портам - функции маршрутизатора. Такой мост/маршрутизатор (иногда называемый brouter) удобно использовать на магистрали сети.

Разделение функций построения таблицы маршрутов и использования таблицы маршрутов. Основная вычислительная работа проводится маршрутизатором при составлении таблицы маршрутов ко всем известным ему сетям. Эта работа состоит в обмене пакетами протоколов маршрутизации, таких как RIP или OSPF, и вычислении оптимального пути к каждой целевой сети по некоторому критерию. Вычисление оптимального пути на графе, как это требуют протоколы состояния связей, требует привлечения значительной вычислительной мощности.

После того, как таблица маршрутов составлена, маршрутизация (если не заданы сложные дополнительные условия фильтрации) происходит весьма просто - осуществляется просмотр таблицы и поиск совпадения с адресом целевой сети. Если совпадение есть, то пакет передается на соответствующий порт маршрутизатора. В последнее время наметилась тенденция разделения этих двух видов работ между различными устройствами сети. Вычисление таблицы маршрутизации возлагается на так называемый сервер маршрутов - это устройство централизует в сети или области сети обработку пакетов RIP и OSPF и построение таблицы маршрутов, но не занимается собственно продвижением пакетов. Этим занимаются другие устройства, которые запрашивают у сервера маршрутов информацию о интересующих их сетях, кэшируют ее и на ее основании маршрутизируют пакеты. Эти устройства получаются гораздо проще традиционных маршрутизаторов и проще конфигурируются. Иногда их называют коммутаторами третьего уровня, иногда маршрутизаторами. Преимущество схемы с сервером маршрутов проявляется также при работе большого количества локальных сетей через глобальную сеть, не поддерживающую, как правило, широковещательность. При использовании традиционных маршрутизаторов, в каждом маршрутизаторе, общающемся с другими через глобальную сеть, нужно вручную задавать глобальный адрес всех маршрутизаторов-соседей. При использовании сервера маршрутов в коммутаторах третьего уровня нужно вручную задать только глобальный адрес сервера маршрутов, а остальные адреса можно узнать у сервера, который, в свою очередь, будет получать их автоматически при регистрации в нем каждого коммутатора. На рисунке 16.22 показана схема использования первого коммерческого сервера маршрутов NAS

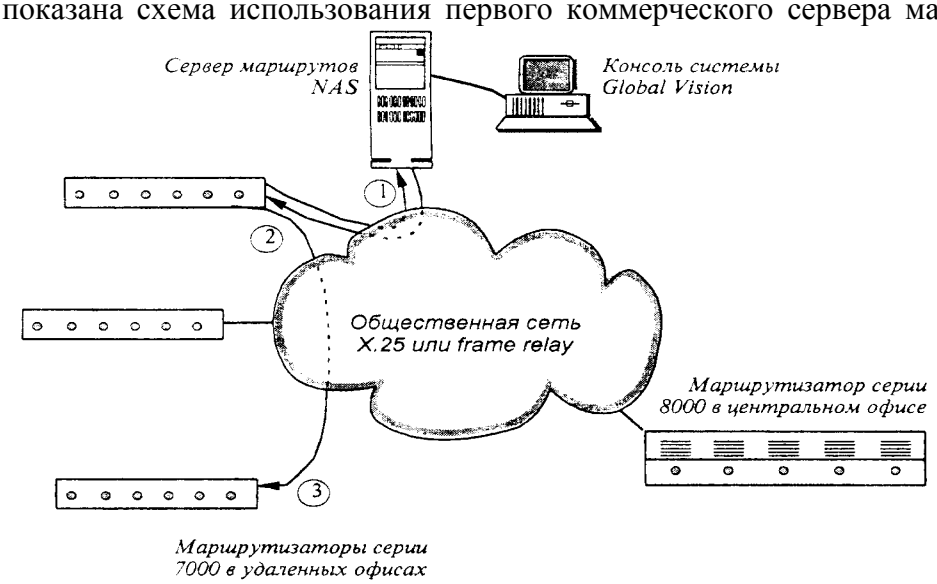


Рис. 16.22. Сервер маршрутов компании Hughes Network Systems

компании Hughes Network Systems, работающего через глобальную сеть frame relay с маршрутизаторами серий 7000 и 8000 этой же компании, которые выполняют роль коммутаторов третьего уровня.

16.4.5. Типовые структуры интрасетей.

Очевидно, что архитектура сети, стек коммуникационных протоколов, тип кабельной системы зависят в конечном счете от специфики предприятия и выбранных приложений.

Однако, существуют проверенные временем стратегические решения, которые можно считать в некоторой степени типовыми, так как они подходят на уровне идей для большинства предприятий. К таким решениям для коммуникационного слоя корпоративной сети относятся: использование на уровне отделов звездообразной иерархической структуры кабельной сети на витой паре для сегментов Ethernet и Token Ring, применение оптоволоконного кабельного кольца FDDI для связи сетей отделов в сеть кампуса, сегментация сетей отделов и кампусов с помощью мостов и маршрутизаторов. Такое разбиение хорошо отражает и функциональную структуру предприятия, и пространственную структуру зданий.

По мере продвижения снизу вверх по иерархии подсетей изменяются и используемые устройства образования локальных связей. Для образования связей в отделах и рабочих группах используются обычно простые концентраторы-повторители, которые с помощью мостов или маршрутизаторов подключаются к вертикальному позвоночнику сети здания. Сети зданий объединяются в позвоночник кампуса с помощью маршрутизаторов, которые используются и как устройства соединения локальных сетей с глобальными.

Распределенная магистраль.

Одной из типичных структур для сети небольшого здания является структура, представленная на рисунке 16.23. Здесь на каждом этаже для соединения рабочих

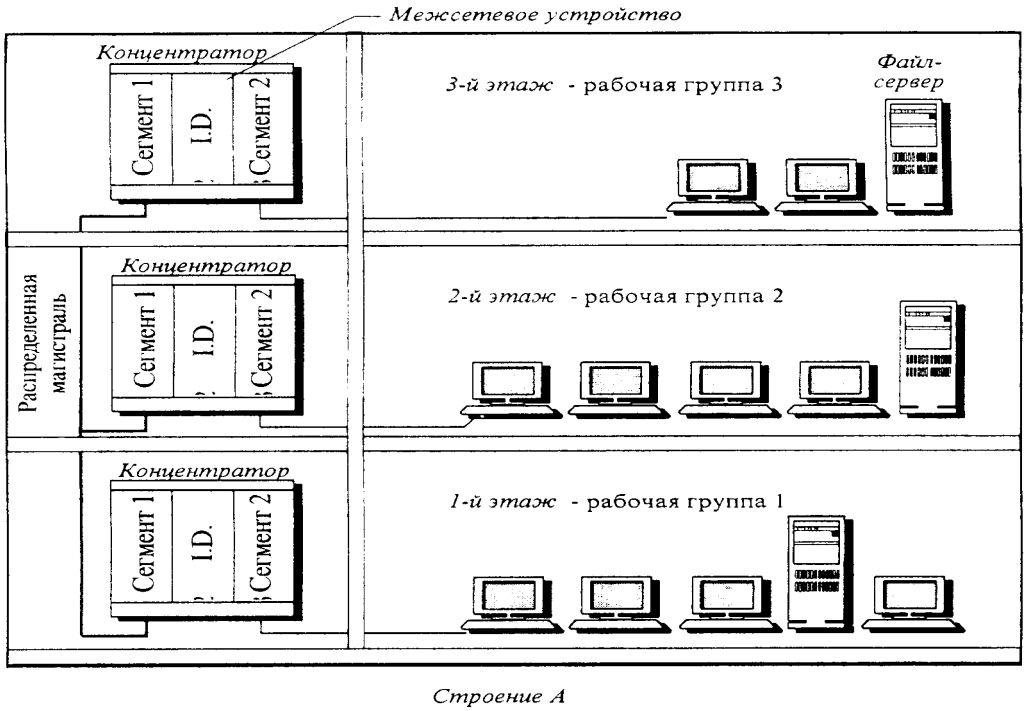


Рис. 16.23. Распределенная магистраль.

станций и серверов используются концентраторы-повторители для сегментов Ethernet и колец Token Ring. Для локализации графика в подсетях этажей они присоединяются к кабелю вертикального позвоночника через устройства межсетевого взаимодействия - мосты, коммутаторы или маршрутизаторы. Такая схема обладает хорошей масштабируемостью, но имеет и недостатки. Во-первых, это достаточно дорогое решение, так как устройство межсетевого взаимодействия применяется на каждом этаже. Во-вторых, трафик, общий для всех сетей, складывается на вертикальной магистрали, поэтому ее производительность должна быть достаточна для его общей интенсивности. Во многих случаях 10-Мбитный Ethernet из-за своей низкой производительности не сможет служить распределенной магистралью. Использование сети FDDI или Fast Ethernet в качестве вертикальной магистрали улучшит пропускную способность магистрали, но удорожит сеть.

Применение мостов для подключения сегментов на этажах к магистрали интрасети является хорошим решением только для сетей сравнительно небольших размеров с большой однородностью, где не требуется поддержка различных сетевых протоколов, не нужны жесткие меры по возведению между сетями защитных барьеров и не нужна развитая связь через глобальные сети с удаленными локальными сетями.

Поэтому для более сложных сетей, объединяющих различные канальные протоколы. используется другое базовое решение, в котором вместо мостов применяются маршрутизаторы, решающие задачи согласования различных канальных протоколов, защищающие корпоративную сеть от широковещательных штормов и обеспечивающие другие высокоуровневые функции управления трафиком. Кроме того, они могут использоваться для образования избыточных связей как между этажами, так и между зданиями, то есть такая структура сети может проще развиваться, чем структура, построенная полностью на мостах. Структура такой сети соответствует структуре сети, образованной с помощью мостов.

Стянутая в точку магистраль (collapsed backbone)

В этой модели магистралью сети является внутренняя шина устройства межсетевого взаимодействия. Все сегменты сети, образованные концентраторами, подключаются индивидуальными линиями связи к одному устройству межсетевого взаимодействия, обладающему достаточной внутренней производительностью для поддержки межсегментного трафика.

Эту модель иногда называют также моделью с вырожденным позвоночником.

Сейчас не редкостью являются коммутаторы с производительностью внутренней шины в несколько Гб или маршрутизаторы с шинами до 1 Гб, поэтому при увеличении требований к производительности магистрали эту проблему можно решить, просто заменив или модернизировав коммутатор или маршрутизатор, образующий магистраль, а не заменяя технологию сети, служащей распределенной магистралью.

Еще более гибким решением будет использование в качестве устройства с вырожденной магистралью корпоративного модульного концентратора с функциями повторителя, коммутатора и маршрутизатора. Для многих предприятий такой концентратор позволит подобрать нужный набор модулей - мостов, маршрутизаторов или коммутируемых мостов - для нужной связи подсетей друг с другом на скоростной магистрали концентратора. Для не

слишком больших сетей на этажах можно отказаться от концентраторов на этажах, и использовать модули-повторители для прямой связи подсетей с центральным концентратором.

Модель с вырожденной магистралью может применяться и в масштабах сети здания. Наиболее просто она организуется в случае, когда сегменты сети (то есть рабочие группы) не выходят за пределы этажей (рисунок 16.24).

Кабели от станций на этаже подключаются к концентратору. Концентратор может поддерживать и несколько рабочих групп на этаже) если его шасси имеет несколько независимых внутренних шин. В приводимом примере от каждого сегмента к общему концентратору, расположенному на первом этаже, идет один вертикальный кабель. К центральному концентратору подключаются и общие серверы, возможно, образуя отдельные, выделенные сегменты.

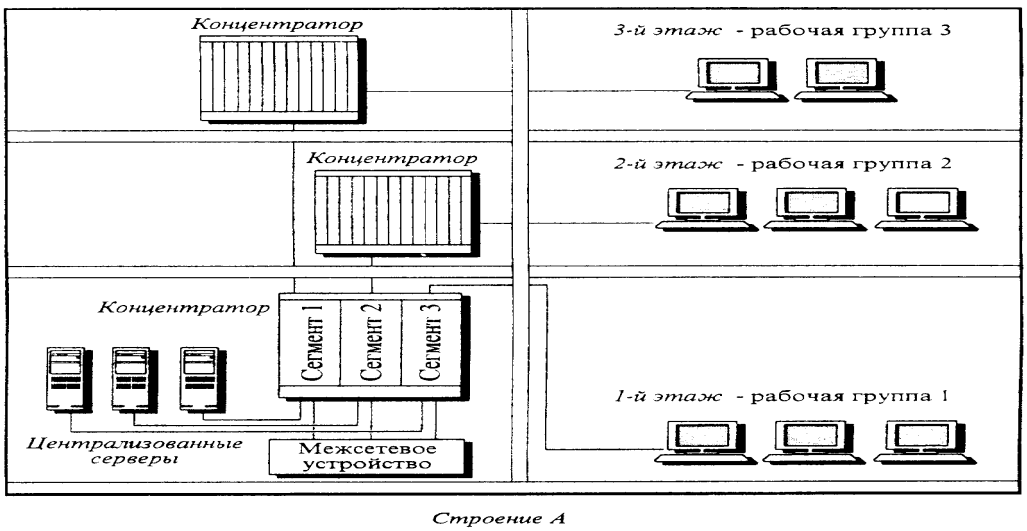


Рис. 16.24. Структура сети с коллапсированной магистралью

Объединение сегментов осуществляет маршрутизатор (коммутатор), к портам которого подключаются выходы сегментов центрального концентратора.

Более сложные межэтажные соединения возникают при существовании параллельных рабочих групп, то есть рабочих групп, члены которых распределены по этажам (рисунок 16.25).

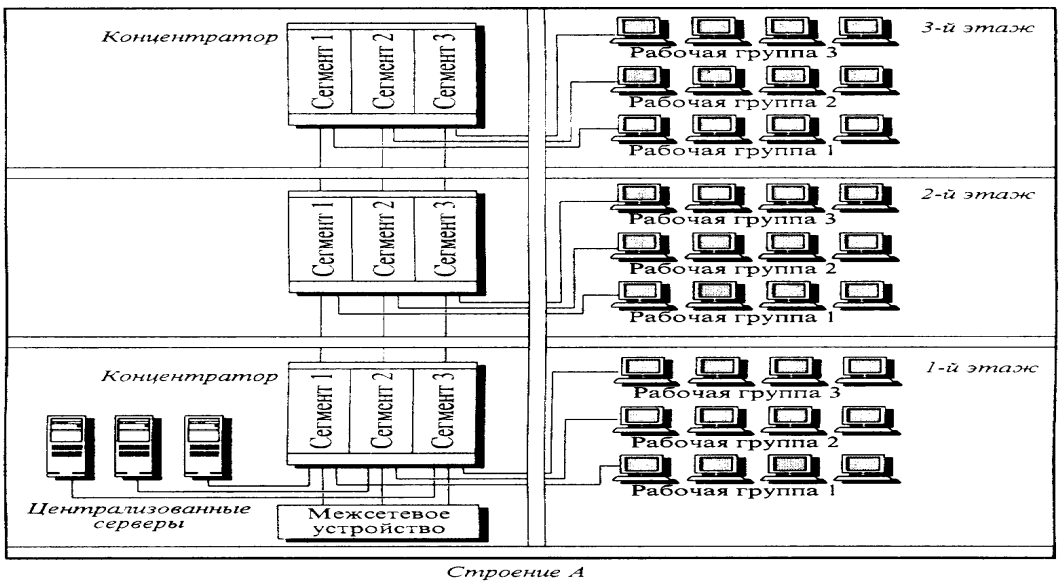


Рис. 16.25. Структура сети с коллапсированной магистралью и распределенными по этажам группами.

Каждый концентратор этажа соединяется с другими концентраторами этажей отдельными кабелями для отдельных рабочих групп, С маршрутизатором или коммутатором непосредственно соединяются порты только того концентратора, который находится на одном с ним этаже. При применении оптоволокна стоимость такой сложной вертикальной разводки увеличивается за счет большого количества ответвлений и разъемов.

В последнее время ведутся оживленные дебаты по поводу того, какое устройство межсетевого взаимодействия должно использоваться в центре интрасети - коммутатор или маршрутизатор. И тот и другой подход имеют свои преимущества и недостатки.

Коммутатор не требует сложного предварительного конфигурирования, поддерживает любые сетевые протоколы (так как просто не обращает внимания, какие протоколы он переносит в кадрах канального уровня, с которыми он имеет дело) и объединяет сегменты сети быстро и за существенно меньшую цену, чем маршрутизатор. Кроме того, многие коммутаторы поддерживают виртуальные сегменты, поэтому распределение компьютеров по сегментам можно осуществлять на программном уровне, причем сегменты не должны быть локализованы внутри одного корпуса, как это происходит при использовании корпоративного модульного концентратора с несколькими внутренними сегментными шинами, или же внутри одного стека концентраторов. Многие коммутаторы поддерживают образование виртуальных сегментов в распределенной системе коммутаторов, соединенных обычными связями, то есть, например, отрезками витой пары длиной до 100 метров.

Однако, защита одного сегмента от другого с помощью коммутатора выполняется не без проблем. Если в сети нет виртуальных сегментов, которые полностью непроницаемы друг для друга, в том числе и по широковещательному трафику, то защита сегмента одного отдела от сегмента другого отдела может происходить толькона основе пользовательских фильтров, установленных администратором сети, а с ними могут быть связано несколько проблем. Во-первых, пользовательские фильтры коммутаторов устанавливать достаточно сложно, так как от администратора требуется хорошее знание структуры пакетов сетевого, транспортного и прикладного уровня. Во-вторых, фильтрация может резко снизить скорость коммутации, являющейся одним из главных преимуществ коммутатора по сравнению с маршрутизатором. Из-за этого некоторые высокопроизводительные коммутаторы, например, Lattis System 28115 компании Bay Networks, не поддерживают пользовательские фильтры.

Маршрутизатор, образующий коллапсированную магистраль сети здания, выполняет в основном функцию защиты сетей друг от друга, а не функцию маршрутизации трафика между сетями, так как при древовидной топологии проблема выбора маршрута отпадает, И некоторые специалисты именно из-за этой функции, которая у маршрутизатора вытекает из его алгоритма работы, предпочитают ставить маршрутизатор в вершину дерева сети здания. Дополнительная фильтрация также осуществляется маршрутизатором гораздо эффективней и проще с точки зрения конфигурирования. Однако, если от такого центрального устройства требуется очень высокая производительность, измеряемая сотнями тысяч продвигаемых пакетов в секунду, то здесь выбор оказывается невелик. Пока очень немного марок маршрутизаторов самого высокого класса может справиться с такой работой - в основном это маршрутизаторы Bay Networks с **симметричной мультипроцессорной организацией** (маршрутизатор BCN этой компании способен обработать свыше

1000000 пакетов в секунду) или маршрутизаторы Cisco Systems с **асимметричной мультипроцессорной организацией** семейства 7500. При этом стоимость такого маршрутизатора может составить несколько сотен тысяч долларов.

Как видно, ни одно из решений не является идеальным. На рисунках 16.26 и 16.27 показаны оба варианта сети здания. Естественно, использование коммутатора или маршрутизатора в вершине дерева не исключает применения конкурирующих устройств на нижних уровнях сети.

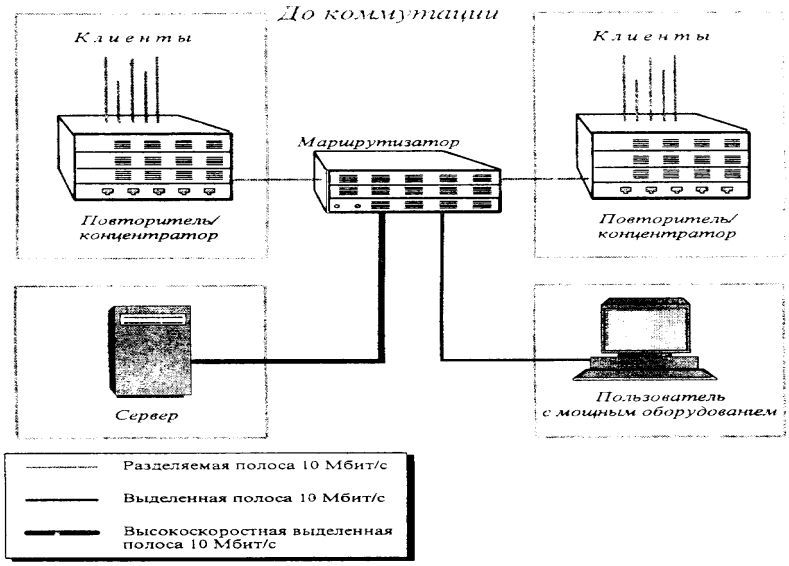


Рис. 16.26. Сеть с симметричной мультипроцессорной организацией.

Если на вершине оказывается маршрутизатор, то коммутаторы очень полезны на следующем уровне иерархии, где они могут образовывать виртуальные сегменты. Объединение виртуальных сегментов внешним маршрутизатором приводит к тому, что сейчас называют виртуальными сетями (Virtual LAN, VLAN).

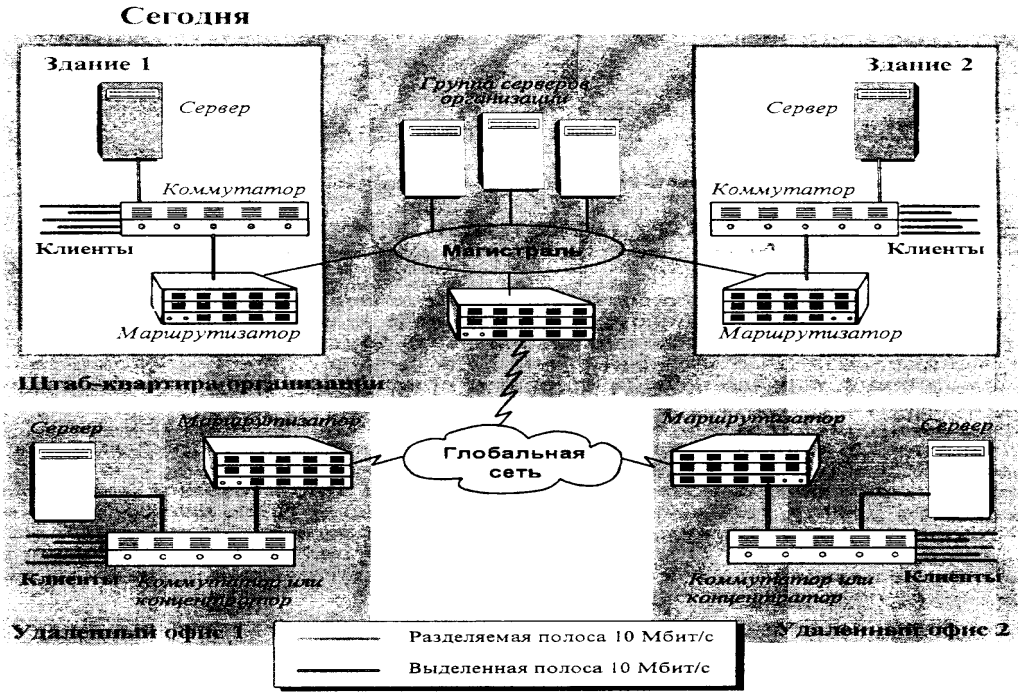


Рис. 16.27. Сеть с асимметричной мультипроцессорной организацией.

Роль самого маршрутизатора при этом не отличается от классического случая, когда сегменты образованы за счет их физического разделения.

Если на вершине оказывается коммутатор, то маршрутизатор отодвигается на периферию сети, и становится пограничным устройством, соединяющим и одновременно отделяющим сеть здания от внешних сетей, которые, в основном, оказываются глобальными сетями.

Существует и третий вариант, когда в вершину сети помещается коммутатор, способный одновременно выполнять и функции маршрутизатора. Если при этом коммутатор поддерживает виртуальные сегменты, которые внутри него же объединяются программным способом по алгоритмам маршрутизатора, то виртуальность таких сетей становится более очевидной. Однако пока это не самый работоспособный вариант из-за того, что современные коммутаторы высшего класса, такие как Catalist 5000 компании Cisco Systems или MMAC Plus компании Cabletron резко снижают производительность при выполнении одновременно функций коммутации и маршрутизации.

Методические рекомендации для преподавателей.

Для проведения данного занятия рекомендуется следующий расчет времени и методика его проведения.

I. Вводная часть - 10 мин.

- проверка наличия обучаемых студентов;
- объявление темы, цели занятия, перечня учебных пособий и учебных вопросов.

II. Основная часть –330 мин.

1. Архитектура и протоколы - 90 мин.

Рассмотреть традиционные локальные сети Ethernet и Token Ring и локальные сети на быстрых протоколах: FDDI, Fast Ethernet и 100VG-AnyLAN.

2. Кабельные системы для локальных сетей - 60 мин.

Рассмотреть концепцию и преимущества структурированной кабельной системы, выбор кабеля для различных подсистем, примеры промышленных структурированных кабельных систем.

2. Многосегментные локальные сети - 90 мин.

Изучить структуру и средства, применение концентраторов, применение мостов и коммутаторов.

4. Сетевой уровень как средство объединения локальных сегментов – 90 мин.

Дать общие сведения по принципам работы составных сетей, по протоколам сетевого и транспортного уровней (IP, TCP, UDP, IPX), по протоколам маршрутизации (RIP и OSPF), по типам и характеристикам маршрутизаторов, по типовым структурам интрасетей.

II. Заключительная часть – 20 мин.

- контрольный опрос;
- ответы на вопросы обучаемых студентов;
- подведение итогов занятия;
- задание на самоподготовку.