Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет телекоммуникаций

Кафедра защиты информации

Л. М. Лыньков, В. П. Ширинский

ПРОЕКТИРОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ

*Рекомендовано УМО по образованию в
области информатики и радиоэлектроники
в качестве учебно-методического пособия
по курсовому проектированию для
специальности 1-45 01 03 «Сети телекоммуникаций»*

Минск БГУИР 2015

УДК 004.7(076)
ББК 32.973.202.я73
Л88

Р е ц е н з е н т ы:
кафедра телекоммуникационных систем
учреждения образования «Высший государственный
колледж связи» (протокол №10 от 20.06.2013 г.);

профессор кафедры менеджмента учреждения
образования «Минский университет управления»,
доктор технических наук, профессор В. А. Вишняков;

заведующий кафедрой программного обеспечения
сетей телекоммуникаций учреждения образования
«Высший государственный колледж связи»,
кандидат физико-математических наук,
доцент Н. Н. Буснюк;

доцент кафедры сетей и устройств телекоммуникаций учреждения
образования «Белорусский государственный университет
информатики и радиоэлектроники»,
кандидат технических наук, доцент В. Ю. Цветков

Лыньков, Л. М.

Л88 Проектирование компьютерных систем : учеб.-метод. пособие / Л. М. Лыньков, В. П. Ширинский. – Минск : БГУИР, 2015. – 62 с. : ил.
ISBN 978-985-543-047-7.

Содержит краткие сведения для проектирования компьютерных сетей.
Предназначено для студентов высших учебных заведений, изучающих дисциплину «Системы подвижной радиосвязи и компьютерные сети».

УДК 004.7(076)
ББК 32.973.202.я73

ISBN 978-985-543-047-7

СОДЕРЖАНИЕ

1. ПРОГРАММНЫЕ КОМПОНЕНТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ.....5
1.1. Сетевые операционные системы 5
1.2. Структура сетевой операционной системы.....5
1.3. Серверное программное обеспечение.....6
1.4. Средства предоставления собственных ресурсов и услуг в общее пользование 7
1.5. Коммуникационные средства ОС.....10
1.6. Компоненты прикладного уровня HTTP, FTP, SMTP, SNMP, Telnet 14
1.7. DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) 15
1.8. DNS (англ. Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах 16
1.9. Active Directory – активные директории, AD – реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT. 18
2. АППАРАТНЫЕ СРЕДСТВА ДЛЯ ПОСТРОЕНИЯ СЕТИ.....19
2.1. Сетевые адаптеры 19
2.2. Классификация сетевых адаптеров.....20
2.3. Повторители и концентраторы.....21
2.4. Многосегментные концентраторы.....22
2.5. Мосты и коммутаторы 23
2.6. Техническая реализация и дополнительные функции коммутаторов.....25
2.7. Маршрутизаторы и шлюзы.....26
2.8. Оборудование для сетей Wi-Fi.....28
2.9. Wi-Fi точки доступа 29
2.10. Средства обеспечения защиты информации в сети 29
2.11. Типы сетевых экранов разных уровней.....32
3. ТЕХНОЛОГИИ ДОСТУПА В ИНТЕРНЕТ 34
4. ПРОЕКТИРОВАНИЕ СЕТИ.....36
4.1. Выбор размера и структуры сети.....36
4.2. Иерархия и основные части сети 36
4.3. Распределение IP-адресов.....39
4.4. Планирование сети с концентратором 41

4.5. Оценка производительности сети.....42
4.6. Выбор оборудования.....45
4.7. Проектирование кабельной системы 46
4.8. Обеспечение защиты информации в сети на основе сетевых экранов 49
4.9. Обслуживание сети, контроль ее безопасности и безотказности 52
4.10. Выбор сетевых программных средств 55
ЛИТЕРАТУРА.....61

1. ПРОГРАММНЫЕ КОМПОНЕНТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Сетевые операционные системы

Сетевые операционные системы – это комплекс программ, обеспечивающих обработку, хранение и передачу данных в сети.

Сетевая операционная система (СОС) составляет основу любой компьютерной сети. Каждый компьютер в сети автономен. Поэтому под ***сетевой операционной системой*** в широком смысле можно понимать совокупность операционных систем отдельных компьютеров, взаимодействующих с целью обмена сообщениями и разделения ресурсов по единым правилам – протоколам. В узком смысле **сетевая ОС** – это операционная система отдельного компьютера, обеспечивающая ему возможность работать в сети.

Сетевая ОС выполняет функции прикладной платформы, предоставляет разнообразные виды сетевых служб и поддерживает работу прикладных процессов, выполняемых в абонентских системах. Сетевые ОС используют клиент-серверную либо одноранговую архитектуру. Компоненты сетевой ОС располагаются на всех рабочих станциях, включенных в сеть.

Сетевая ОС определяет взаимосвязанную группу протоколов верхних уровней, обеспечивающих выполнение основных функций сети. К ним в первую очередь относятся:

- адресация объектов сети;
- функционирование сетевых служб;
- обеспечение безопасности данных;
- управление сетью.

При выборе сетевой ОС необходимо рассматривать множество факторов. Среди них:

- набор сетевых служб, которые предоставляет сеть;
- механизм рассредоточения ресурсов по сети;
- способ модификации сети и сетевых служб;
- надежность функционирования и быстродействие сети;
- используемые или выбираемые физические средства соединения;
- типы компьютеров, объединяемых в сеть, их операционные системы;
- предлагаемые системы, обеспечивающие управление сетью;
- используемые средства защиты данных.

1.2. Структура сетевой операционной системы

В сетевой операционной системе отдельной машины можно выделить несколько частей.

1. *Средства управления локальными ресурсами компьютера*: функции распределения оперативной памяти между процессами, планирования и диспетчеризации процессов, управления процессорами, управления периферийными устройствами и т. д.

2. *Средства предоставления собственных ресурсов и услуг в общее пользование* – серверная часть ОС (сервер).

3. *Средства запроса доступа к удаленным ресурсам*. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат, так что для приложения выполнение локальных и удаленных запросов неразличимо.

4. *Коммуникационные средства ОС*, с помощью которых происходит обмен сообщениями в сети. Эта часть обеспечивает адресацию и буферизацию сообщений, выбор маршрута передачи сообщения по сети, надежность передачи и прочее, т. е. является средством транспортировки сообщений.

1.3. Серверное программное обеспечение

Для того чтобы компьютер мог выступать в роли сетевого сервера, необходимо установить серверную часть сетевой ОС, которая позволяет поддерживать ресурсы и распространять их среди сетевых клиентов. Важным вопросом для сетевых серверов является возможность ограничить доступ к сетевым ресурсам. Это называется *сетевой защитой* (network security). Она предоставляет средства управления над тем, к каким ресурсам могут получить доступ пользователи, степень этого доступа, а также сколько пользователей смогут получить такой доступ одновременно. Этот контроль обеспечивает конфиденциальность и защиту и поддерживает эффективную сетевую среду.

В дополнение к обеспечению контроля над сетевыми ресурсами сервер выполняет следующие функции [3]:

- предоставляет проверку регистрационных имен *(logon identification)* для пользователей;
- управляет пользователями и группами;
- хранит инструменты сетевого администрирования для управления, контроля и аудита;
- обеспечивает отказоустойчивость для защиты целостности сети.

Некоторые из сетевых ОС, в том числе Windows, имеют программные компоненты, обеспечивающие компьютеру как клиентские, так и серверные возможности. Это позволяет компьютерам поддерживать и использовать сетевые ресурсы. В общем этот тип сетевых операционных систем не так мощен и надежен, как законченные сетевые операционные системы.

1.4. Средства предоставления собственных ресурсов и услуг в общее пользование

Функции верхних уровней эталонной модели OSI выполняют сетевые программные средства. Для установки сети достаточно иметь набор сетевого оборудования, его драйверы, а также сетевое программное обеспечение. От выбора программного обеспечения зависит очень многое: допустимый размер сети, удобство использования и контроля сети, режимы доступа к ресурсам, производительность сети в разных режимах и т. д. Правда, заменить одну программную систему на другую значительно проще, чем сменить оборудование.

С точки зрения распределения функций между компьютерами сети все сети можно разделить на две группы:

• *одноранговые сети*, состоящие из равноправных (с точки зрения доступа к сети) компьютеров;

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

Согласно с этим выделяют и типы программных средств, реализующих данные виды сетей.

Одноранговые сети

Одноранговые сети и соответствующие программные средства, как правило, используются для объединения небольшого количества компьютеров. Каждый компьютер такой сети может одновременно являться и сервером и клиентом сети.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки (к тому же количество компьютеров обычно невелико). Установка одноранговых сетей довольно проста, и не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей по доступу к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. К тому же выход из строя любого компьютера-сервера приводит к потере части общей информации, т. е. все такие компьютеры должны

быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети.

В настоящее время считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедлят работу компьютеров и создадут множество других проблем. Тем не менее для небольшого офиса одноранговая сеть – оптимальное решение.

Сети на основе сервера

Сети на основе сервера применяются в тех случаях, когда в сеть должно быть объединено много пользователей, поэтому в сеть включается специализированный компьютер – сервер, который обслуживает только сеть и не решает никаких других задач. Такой сервер называется выделенным. Сервер может быть и специализирован на решении одной задачи, например сервер печати. В сети может быть и несколько серверов, каждый из которых решает свою задачу.

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

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

Для обеспечения надежной работы сети при авариях электропитания применяется бесперебойное электропитание сервера. В данном случае это гораздо проще, чем при одноранговой сети, где желательно оснащать источниками бесперебойного питания все компьютеры сети. Для администрирования сети (т. е. управления распределением ресурсов, контроля прав доступа, защиты данных,

файловой системы, резервирования файлов и т. д.) [3] в случае сети на основе сервера необходимо выделять специального человека, имеющего соответствующую квалификацию. Централизованное администрирование облегчает обслуживание сети и позволяет оперативно решать все вопросы. Особенно это важно для надежной защиты данных от несанкционированного доступа. В случае же одноранговой сети можно обойтись и без специалиста-администратора, правда, при этом все пользователи сети должны иметь хоть какое-то представление об администрировании.

Процесс установки серверной сетевой операционной системы гораздо сложнее, чем в случае одноранговой сети. Так, он включает в себя следующие обязательные процедуры [10]:

- форматирование и разбиение на разделы жесткого диска компьютера-сервера;
- присвоение индивидуального имени серверу;
- присвоение имени сети;
- установка и настройка сетевого протокола;
- выбор сетевых служб;
- ввод пароля администратора.

Сетевая операционная система на базе сервера Windows Server 2003 предоставляет пользователям гораздо больше возможностей, чем в случае одноранговой сети.

Настройка операционной системы

В Windows предусмотрена поддержка совместного использования дисков (в том числе гибких дисков и CD), а также принтеров. Имеется возможность объединения всех пользователей в рабочие группы для более удобного поиска требуемых ресурсов и организации доступа к ним. Пользователи имеют доступ ко встроенной системе электронной почты. Это означает, что все пользователи сети получают возможность совместно применять многие ресурсы ОС своего компьютера.

При настройке сети пользователь должен выбрать тип сетевого протокола. По умолчанию используется протокол TCP/IP, но возможно применение IPX/SPX (NWLink), а также NetBEUI. При выборе **TCP/IP** можно задавать адреса IP вручную или с помощью автоматической настройки адресации (в этом случае компьютер сам присвоит себе адрес из диапазона, не используемого в Интернете).

Кроме того, надо задать индивидуальное имя компьютера и определить рабочую группу, к которой он относится.

После этого можно разрешить доступ по сети к ресурсам каждого компьютера сети, к его файлам, папкам, принтерам, сканерам, доступу в Интернет.

Каждому серверу необходимо назначить роль, которую он будет выполнять в сети [10]:

• контроллер домена (управляет работой домена);

• файловый сервер (хранит совместно используемые файлы);

• сервер печати (управляет сетевым принтером);

• веб-сервер (содержит сайт, доступный по сети Интернет или по локальной сети);

• коммуникационный сервер (обеспечивает работу электронной почты и конференций);

• сервер удаленного доступа (обеспечивает удаленный доступ).

Каждому пользователю сети необходимо присвоить свое учетное имя и пароль, а также права доступа к ресурсам (полномочия). Права доступа могут задаваться как индивидуально, так и целой рабочей группе пользователей. Windows Server 2003 обеспечивает следующие виды полномочий для папок:

• полный контроль (просмотр, чтение, запись, удаление папки, подпапок, файлов, запуск на исполнение, установка прав доступа к папке);

• изменение (просмотр, чтение, запись, удаление подпапок и файлов, запуск на исполнение);

• чтение и исполнение (просмотр, чтение, запуск на исполнение);

• просмотр содержимого папки;

• запись нового содержимого в папку;

• чтение информации из папки.

1.5. Коммуникационные средства ОС

Стандартные сетевые протоколы

Протоколы – это набор правил и процедур, регулирующих порядок осуществления связи.

О протоколах нижних уровней (физического и канального) можно прочесть в литературе [1]. В частности, к ним относятся методы кодирования и декодирования, а также управления обменом информацией в сети.

Связь сетевого адаптера с сетевым программным обеспечением осуществляют драйверы сетевых адаптеров. Именно благодаря драйверу компьютер может «не знать» никаких аппаратных особенностей адаптера (его адресов, правил обмена с ним, его характеристик). Драйвер унифицирует, делает единообразным взаимодействие программных средств высокого уровня с любым адаптером данного класса. Сетевые драйверы, поставляемые вместе с сетевыми адаптерами, позволяют сетевым программам одинаково работать с платами разных поставщиков и

даже с платами разных локальных сетей (Ethernet, Arcnet, Token-Ring и т. д.).

Протоколы высоких уровней

Существует несколько стандартных наборов (или, как их еще называют, стеков) протоколов, получивших широкое распространение:

- набор протоколов ISO/OSI;
- IBM System Network Architecture (SNA);
- Digital DECnet;
- Novell NetWare;
- Apple AppleTalk;
- набор протоколов глобальной сети Интернет, TCP/IP.

Включение в этот список протоколов глобальной сети вполне объяснимо, ведь, как уже отмечалось, модель OSI используется для любой открытой системы: на базе как локальной, так и глобальной сети или комбинации локальной и глобальной сетей.

Протоколы перечисленных наборов делятся на три основных типа:

• прикладные протоколы (выполняющие функции трех верхних уровней модели OSI – прикладного, представительского и сеансового);

• транспортные протоколы (реализующие функции средних уровней модели OSI – транспортного и сеансового);

• сетевые протоколы (осуществляющие функции трех нижних уровней модели OSI).

Прикладные протоколы обеспечивают взаимодействие приложений и обмен данными между ними. Наиболее популярны:

• SMTP (Simple Mail Transfer Protocol) – протокол глобальной сети Интернет для обмена электронной почтой;

• FTP (File Transfer Protocol) – протокол глобальной сети Интернет для передачи файлов;

• SNMP (Simple Network Management Protocol) – протокол для мониторинга сети, контроля за работой сетевых компонентов и управления ими;

• Telnet – протокол глобальной сети Интернет для регистрации на удаленных серверах и обработки данных на них.

Транспортные протоколы поддерживают сеансы связи между компьютерами и гарантируют надежный обмен данными между ними. Наиболее популярны из них следующие:

• TCP (Transmission Control Protocol) – часть набора протоколов TCP/IP для гарантированной доставки данных, разбитых на последовательность фрагментов;

• SPX – часть набора протоколов IPX/SPX (Internetwork Packet Exchange/Sequential Packet Exchange) для гарантированной доставки данных, разбитых на последовательность фрагментов, предложенных компанией Novell.

Сетевые протоколы управляют адресацией, маршрутизацией, проверкой ошибок и запросами на повторную передачу. Широко распространены следующие из них:

• IP (Internet Protocol) – TCP/IP-протокол для негарантированной передачи пакетов без установления соединений;

• IPX (Internetwork Packet Exchange) – протокол компании NetWare для негарантированной передачи пакетов и маршрутизации пакетов.

Методы взаимодействия абонентов в сети

Модель OSI допускает два основных метода взаимодействия абонентов в сети:

• метод взаимодействия без логического соединения (или метод дейтаграмм);

• метод взаимодействия с логическим соединением.

Метод дейтаграмм – простейший метод, в котором каждый пакет рассматривается как самостоятельный объект.

Пакет при этом методе передается без установления логического канала, т. е. без предварительного обмена служебными пакетами для выяснения готовности приемника, а также без ликвидации логического канала, т. е. без пакета подтверждения окончания передачи. Дойдет пакет до приемника или нет – неизвестно (проверка факта получения переносится на более высокие уровни).

Метод дейтаграмм предъявляет повышенные требования к аппаратуре (так как приемник всегда должен быть готов к приему пакета). Достоинства метода в том, что передатчик и приемник работают независимо друг от друга, к тому же пакеты могут накапливаться в буфере и затем передаваться вместе. Можно также использовать широковещательную передачу, т. е. адресовать пакет всем абонентам одновременно. Недостатки метода – возможность потери пакетов, а также бесполезной загрузки сети пакетами в случае отсутствия или неготовности приемника.

Метод с логическим соединением разработан позднее, чем метод дейтаграмм, и отличается усложненным порядком взаимодействия.

При этом методе пакет передается только после того, как будет установлено логическое соединение (канал) между приемником и передатчиком. Каждому информационному пакету сопутствует один или несколько служебных пакетов (установка соединения, подтверждение получения, запрос повторной передачи, разрыв соединения). Логический канал может устанавливаться на время передачи одного или нескольких пакетов.

Метод с логическим соединением, как уже говорилось, более сложен, чем метод дейтаграмм, но гораздо надежнее, поскольку к моменту ликвидации логического канала передатчик уверен, что все его пакеты дошли до места назначения, причем дошли успешно. Не бывает при данном методе и перегрузки сети из-за бесполезных пакетов.

Примеры протоколов, работающих по методу дейтаграмм – это протоколы IP и IPX.

Примеры протоколов, работающих по методу с логическим соединением, – это TCP и SPX.

Именно для того, чтобы объединить достоинства обоих методов, эти протоколы используются в виде связанных наборов: TCP/IP и IPX/SPX, в которых протокол более высокого уровня (TCP, SPX), работающий на базе протокола более низкого уровня (IP, IPX), гарантирует правильную доставку пакетов в требуемом порядке.

Протоколы IPX/SPX, разработанные компанией Novell, образуют набор (стек), используемый в сетевых программных средствах довольно широко распространенных локальных сетей Novell (NetWare). Это сравнительно небольшой и быстрый протокол, поддерживающий маршрутизацию.

Набор (стек) протоколов TCP/IP был специально разработан для глобальных сетей и для межсетевого взаимодействия. Он изначально ориентирован на низкое качество каналов связи, на большую вероятность ошибок и разрывов связей. Этот протокол принят во всемирной компьютерной сети Интернет, значительная часть абонентов которой подключается по коммутируемым линиям (т. е. обычным телефонным линиям). Как и протокол IPX/SPX, протокол TCP/IP также поддерживает маршрутизацию. На его основе работают протоколы высоких уровней, такие, как SMTP, FTP, SNMP. Недостаток протокола TCP/IP – более низкая скорость работы, чем у IPX/SPX. Однако сейчас протокол TCP/IP используется и в локальных сетях, чтобы упростить согласование протоколов локальных и глобальных сетей. В настоящее время он считается основным в самых распространенных операционных системах.

В стек протоколов TCP/IP часто включают и протоколы всех верхних уровней. И тогда уже можно говорить о функциональной полноте стека TCP/IP.

Как протокол IPX, так и протокол IP являются самыми низкоуровневыми протоколами, поэтому они непосредственно инкапсулируют свою информацию, называемую дейтаграммой, в поле данных передаваемого по сети пакета. При этом в заголовок дейтаграммы входят адреса абонентов (отправителя и получателя) более высокого уровня, чем MAC-адреса, – это IPX-адреса для протокола IPX или IP-адреса для протокола IP. Эти адреса включают номера сети и узла, хоста (индивидуальный

идентификатор абонента). При этом IPX-адреса более простые и имеют всего один формат, а в IP-адрес могут входить три формата (класса A, B и C) [2], различающиеся значениями трех начальных битов.

Интересно, что IP-адрес не имеет никакой связи с MAC-адресами абонентов. Номер узла в нем присваивается абоненту независимо от его MAC-адреса. В качестве идентификатора станции IPX-адрес включает в себя полный MAC-адрес абонента.

Номер сети – это код, присвоенный каждой конкретной сети, т. е. каждой *широковещательной области* общей, единой сети. Под широковещательной областью понимают часть сети, которая прозрачна для широковещательных пакетов и пропускает их беспрепятственно.

1.6. Компоненты прикладного уровня HTTP, FTP, SMTP, SNMP, Telnet

На прикладном уровне работает множество стандартных утилит и служб TCP/IP, к числу которых относятся:

- **протокол HTTP** – используется для организации доступа к общим данным, расположенным на веб-серверах, с целью публикации и чтения общедоступной информации. Протокол HTTP описывает взаимодействие между HTTP-серверами (веб-серверами) и HTTP-клиентами (веб-браузерами);
- **протокол FTP** – служба Интернета, обеспечивающая передачу файлов между компьютерами;
- **протокол SMTP** – применяется почтовыми серверами для передачи электронной почты;
- **протокол Telnet** – протокол эмуляции терминала, применяемый для подключения к удаленным узлам сети. Te1net позволяет клиентам удаленно запускать приложения, кроме того, он упрощает удаленное администрирование. Реализации Telnet, доступные практически для всех ОС, облегчают интеграцию в разнородных сетевых средах;
- **протокол SNMP** – позволяет централизованно управлять узлами сети, например серверами, рабочими станциями, маршрутизаторами, мостами и концентраторами. Кроме того, SNMP можно использовать для конфигурирования удаленных устройств, мониторинга производительности сети, выявления ошибок сети и попыток несанкционированного доступа, а также для аудита использования сети.

1.7. DHCP (англ. Dynamic Host Configuration Protocol – протокол динамической конфигурации узла)

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это *сетевой протокол*, протокол, позволяющий компьютерам автоматически получать *IP-адрес* и другие параметры, необходимые для работы в сети TPC/IP.

Для нормальной работы сети каждому сетевому интерфейсу компьютера и маршрутизатора должен быть назначен IP-адрес.

Процедура присвоения адресов происходит в ходе **конфигурирования** компьютеров и маршрутизаторов. Назначение IP-адресов может происходить вручную в результате выполнения процедуры конфигурирования интерфейса, для компьютера сводящейся, например, к заполнению системы экранных форм. При этом администратор должен помнить, какие адреса из имеющегося множества он уже использовал для других интерфейсов, а какие еще свободны. При конфигурировании помимо IP-адресов сетевых интерфейсов (и соответствующих масок) устройству сообщается ряд других **конфигурационных параметров**. При конфигурировании администратор должен назначить клиенту не только IP-адрес, но и другие параметры стека TCP/IP, необходимые для его эффективной работы, например, маску и IP-адрес маршрутизатора по умолчанию, IP-адрес DNS-сервера, доменное имя компьютера и т. п. Даже при не очень большом размере сети эта работа представляет для администратора утомительную процедуру.

Протокол динамического конфигурирования хостов (Dynamic Host Configuration Protocol, DHCP) автоматизирует процесс конфигурирования сетевых интерфейсов, обеспечивая отсутствие дублирования адресов за счет централизованного управления их распределением. Работа DHCP описана в RFC 2131 и 2132.

Режимы DHCP

Протокол DHCP работает в соответствии с моделью *клиент-сервер*. Во время старта системы компьютер, являющийся DHCP-клиентом, посылает в сеть широковещательный запрос на получение IP-адреса. DHCP-сервер откликается и посылает сообщение-ответ, содержащее IP-адрес и некоторые другие конфигурационные параметры.

При этом сервер DHCP может работать в разных режимах, включая:

- ручное назначение статических адресов;
- автоматическое назначение статических адресов;
- автоматическое распределение динамических адресов.

Во всех режимах работы администратор при конфигурировании DHCP-сервера сообщает ему один или несколько диапазонов IP-адресов, причем все

эти адреса относятся к одной сети, т. е. имеют одно и то же значение в поле номера сети. В **ручном** режиме администратор, помимо пула доступных адресов, снабжает DHCP-сервер информацией о жестком соответствии IP-адресов физическим адресам или другим идентификаторам клиентских узлов. DHCP-сервер, пользуясь этой информацией, *всегда* выдаст определенному DHCP-клиенту *один и тот же* назначенный ему администратором IP-адрес (а также набор других конфигурационных параметров).

В режиме автоматического назначения статических адресов DHCP-сервер самостоятельно без вмешательства администратора произвольным образом выбирает клиенту IP-адрес из пула наличных IP-адресов. Адрес дается клиенту из пула в постоянное пользование, т. е. между идентифицирующей информацией клиента и его IP-адресом по-прежнему как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первого назначения DHCP-сервером IP-адреса клиенту. При всех последующих запросах сервер возвращает клиенту тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, называемое сроком аренды. Когда компьютер, являющийся DHCP-клиентом, удаляется из подсети, назначенный ему IP-адрес автоматически освобождается. Когда компьютер подключается к другой подсети, то ему автоматически назначается новый адрес. Ни пользователь, ни сетевой администратор не вмешиваются в этот процесс.

Это дает возможность впоследствии повторно использовать этот IP-адрес для назначения другому компьютеру. Таким образом, помимо основного преимущества DHCP – автоматизации рутинной работы администратора по конфигурированию стека TCP/IP на каждом компьютере, режим динамического распределения адресов в принципе позволяет строить IP-сеть, количество узлов в которой превышает количество имеющихся в распоряжении администратора IP-адресов.

1.8. DNS (англ. Domain Name System – система доменных имен) – компьютерная распределенная система для получения информации о доменах

Для идентификации компьютеров аппаратное и программное обеспечение в сетях TCP/ IP полагается на IP-адреса. Например, команда ftp://192.45.66.17 будет устанавливать сеанс связи с нужным ftp-сервером, а команда http://203.23.106.33 откроет начальную страницу на корпоративном веб-сервере. Однако пользователи обычно предпочитают работать с более удобными **символьными** именами компьютеров.

Символьные идентификаторы сетевых интерфейсов в пределах составной

сети строятся по иерархическому принципу. Составляющие полного символьного (или доменного) имени в IP-сетях разделяются точкой и перечисляются в следующем порядке: сначала простое имя хоста, затем имя группы хостов (например, имя организации), потом имя более крупной группы (домена) и так до имени домена самого высокого уровня (например, домена, объединяющего организации по географическому принципу: RU – Россия, UK – Великобритания, US – США). Примером доменного имени может служить имя base2.sales.zil.ru.

Между **доменным именем** и IP-адресом узла нет никакой функциональной зависимости, поэтому единственный способ установления соответствия – это таблица. В сетях TCP/IP используется специальная система доменных имен (Domain Name System, DNS), которая устанавливает это соответствие на основании создаваемых администраторами сети таблиц соответствия. Поэтому доменные имена называют также **DNS-именами**.

Чаще всего DNS используется для получения IP-адреса по имени хоста (компьютера или устройства).

DNS обладает следующими характеристиками:

1. *Распределенность администрирования. Ответственность* за разные части иерархической структуры несут разные люди или организации.
2. *Распределенность хранения информации.* Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его *зону ответственности* .
3. *Кеширование информации.* Узел *может* хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
4. *Иерархическая структура,* в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или *делегировать* (передавать) их другим узлам.
5. *Резервирование.* За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделенных как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, ибо для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например HTTP-серверы, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла hosts, который составлялся централизованно и автоматически рассылался на каждую из машин в своей локальной сети. С ростом сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

1.9. Active Directory – активные директории, AD – реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT

Active Directory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, развертывать программное обеспечение на множестве компьютеров через групповые политики или посредством *System Center Configuration Manager* (ранее *Microsoft Systems Management Server*), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления *Windows Server*. *Active Directory* хранит данные и настройки среды в централизованной базе данных. Сети *Active Directory* могут быть различного размера: от нескольких сотен до нескольких миллионов объектов.

Ключевым решением при проектировании *Active Directory* является решение о разделении информационной инфраструктуры на иерархические домены и подразделения верхнего уровня.

2. АППАРАТНЫЕ СРЕДСТВА ДЛЯ ПОСТРОЕНИЯ СЕТИ

2.1. Сетевые адаптеры

Сетевые адаптеры – это сетевое оборудование, обеспечивающее функционирование сети на физическом и канальном уровнях.

Сетевой адаптер относится к периферийному устройству компьютера, непосредственно взаимодействующему со средой передачи данных, которая прямо или через другое коммуникационное оборудование связывает его с другими компьютерами. Как и любой контроллер компьютера, сетевой адаптер работает под управлением *драйвера* операционной системы.

Сетевой адаптер вставляется в гнездо *материнской платы*. Карты сетевых адаптеров устанавливаются на каждой рабочей станции и на файловом сервере. Сетевые адаптеры преобразуют параллельные коды, используемые внутри компьютера и представленные маломощными сигналами, в последовательный поток мощных сигналов для передачи данных по внешней сети.

Физический интерфейс между самой сетевой картой и сетью называют трансивером (transceiver) – устройство, которое как получает, так и посылает данные.

Сетевые адаптеры различаются также по типу принятой в сети технологии – Ethernet, Token Ring, FDDI и т. п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае, когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Различные типы сетевых адаптеров отличаются не только методами доступа к среде и протоколами, но еще и следующими параметрами:

– скорость передачи;
– объем буфера для пакета;
– тип шины;
– быстродействие шины;
– совместимость с различными микропроцессорами;
– использование прямого доступа к памяти (DMA);
– адресация портов ввода/вывода и запросов прерывания;
– конструкция разъема.

2.2. Классификация сетевых адаптеров

В качестве примера классификации адаптеров можно использовать подход фирмы 3Com, имеющей репутацию лидера в области адаптеров Ethernet. Фирма 3Com считает, что сетевые адаптеры Ethernet прошли в своем развитии три поколения.

Сетевые адаптеры *первого поколения* были выполнены на дискретных логических микросхемах, в результате чего обладали низкой надежностью. Они имели буферную память только на один кадр, что приводило к низкой производительности адаптера, так как все кадры передавались из компьютера в сеть или из сети в компьютер последовательно. Кроме этого, задание конфигурации адаптера первого поколения происходило вручную с помощью перемычек. Для каждого типа адаптеров использовался свой драйвер, причем интерфейс между драйвером и сетевой операционной системой не был стандартизирован.

В сетевых адаптерах *второго поколения* для повышения производительности стали применять метод *многокадровой буферизации.* При этом следующий кадр загружается из памяти компьютера в буфер адаптера одновременно с передачей предыдущего кадра в сеть. В режиме приема, после того как адаптер полностью принял один кадр, он может начать передавать этот кадр из буфера в память компьютера одновременно с приемом другого кадра из сети.

В сетевых адаптерах второго поколения широко используются микросхемы с высокой степенью интеграции, что повышает надежность адаптеров. Кроме того, драйверы этих адаптеров основаны на стандартных спецификациях. Адаптеры второго поколения обычно поставляются с драйверами, работающими как в стандарте NDIS *(спецификация интерфейса сетевого драйвера),* разработанном фирмами 3Com и Microsoft и одобренном IBM, так и в стандарте ODI *(интерфейс открытого драйвера),* разработанном фирмой Novell.

В сетевых адаптерах *третьего поколения* (к ним фирма 3Com относит свои адаптеры семейства EtherLink III) осуществляется *конвейерная схема обработки кадров.* Она заключается в том, что процессы приема кадра из оперативной памяти компьютера и передачи его в сеть совмещаются во времени. Таким образом, после приема нескольких первых байт кадра начинается их передача. Это существенно (на 25–55 %) повышает производительность цепочки *оперативная память – адаптер – физический канал – адаптер – оперативная память.* Такая схема очень чувствительна к порогу начала передачи, т. е. к количеству байт кадра, которое загружается в буфер адаптера перед началом передачи в сеть. Сетевой адаптер третьего поколения осуществляет самонастройку этого параметра путем анализа рабочей среды, а также методом расчета без участия администратора сети. Самонастройка обеспечивает максимально возможную производительность для конкретного соче-

тания производительности внутренней шины компьютера, его системы прерываний и системы прямого доступа к памяти.

Адаптеры третьего поколения базируются на специализированных интегральных схемах (ASIC), что повышает производительность и надежность адаптера при одновременном снижении его стоимости. Компания 3Com назвала свою технологию конвейерной обработки кадров Parallel Tasking, другие компании также реализовали похожие схемы в своих адаптерах. Повышение производительности канала *адаптер – память* очень важно для повышения производительности сети в целом, так как производительность сложного маршрута обработки кадров, включающего, например, концентраторы, коммутаторы, маршрутизаторы, глобальные каналы связи и т. п., всегда определяется производительностью его самого медленного элемента. Следовательно, если сетевой адаптер сервера или клиентского компьютера работает медленно, никакие быстрые коммутаторы не смогут повысить скорость работы сети.

Выпускаемые в настоящее время сетевые адаптеры можно отнести к *четвертому поколению.* В эти адаптеры обязательно входят элементы ASIC, выполняющие функции MAC-уровня, а также большое количество высокоуровневых функций. В набор таких функций может входить *поддержка агента удаленного мониторинга* RMON, схема приоритезации кадров, функции дистанционного управления компьютером и т. п. В серверных вариантах адаптеров почти обязательно наличие мощного процессора, разгружающего центральный процессор. Примером сетевого адаптера четвертого поколения может служить адаптер компании Intel – Intel PRO/1000 MT Desktop или Hardlink HA-32G фирмы MAS Elektronik AG.

2.3. Повторители и концентраторы

Основная функция повторителя (repeater), как это следует из его названия, – повторение сигналов, поступающих на его порт. Повторитель улучшает электрические характеристики сигналов и их синхронность, и за счет этого появляется возможность увеличивать общую длину кабеля между самыми удаленными в сети узлами.

Многопортовый повторитель часто называют *концентратором* (concentrator), или *хабом* (hub), что отражает тот факт, что данное устройство реализует не только функцию повторения сигналов, но и концентрирует в одном центральном устройстве функции объединения компьютеров в сеть.

Концентратор представляет собой сетевое устройство, действующее на физическом уровне сетевой модели OSI.

Ядром концентратора является *процессор.* Для объединения входной информации чаще всего используется *множественный доступ с разделением времени.* Функции, выполняемые концентратором, близки к задачам, возложенным на мультиплексор.

Современные концентраторы имеют порты для подключения к разнообразным локальным сетям.

Концентратор является активным оборудованием, служит центром (шиной) звездообразной конфигурации сети и обеспечивает подключение сетевых устройств.

Концентраторы образуют из отдельных физических отрезков кабеля общую среду передачи данных – логический сегмент.

Логический сегмент также называют *доменом коллизий,* поскольку при попытке одновременной передачи данных любых двух компьютеров этого сегмента, хотя бы и принадлежащих разным физическим сегментам, возникает блокировка передающей среды. Следует особо подчеркнуть, что, какую бы сложную структуру ни образовывали концентраторы, например, путем иерархического соединения, все компьютеры, подключенные к ним, образуют единый логический сегмент, в котором любая пара взаимодействующих компьютеров полностью блокирует возможность обмена данными для других компьютеров.

2.4. Многосегментные концентраторы

При рассмотрении некоторых моделей концентраторов возникает вопрос: зачем в этой модели имеется такое большое количество портов, например 192 или 240? Имеет ли смысл разделять среду в 10 или 100 Мбит/с между таким большим количеством станций? В таких концентраторах имеется несколько несвязанных внутренних шин, которые предназначены для создания нескольких разделяемых сред. Например, концентратор имеет три внутренние шины Ethernet. Если в таком концентраторе 72 порта, то каждый из этих портов может быть связан с любой из трех внутренних шин. Между собой компьютеры, подключенные к разным сегментам, общаться через концентратор не могут, так как шины внутри концентратора никак не связаны.

Многосегментные концентраторы нужны для создания разделяемых сегментов, состав которых может легко изменяться. Большинство многосегментных концентраторов, например System 5000 компании Nortel Networks или PortSwitch Hub компании 3Com, позволяют выполнять операцию соединения порта с одной из внутренних шин чисто программным способом, например, с помощью локального конфигурирования через консольный порт. В результате администратор сети может присоединять компьютеры пользователей к любым портам концентратора, а затем с помощью программы конфигурирования концентратора управлять составом каждого сегмента. Если вдруг сегмент 1 станет перегруженным, то его компьютеры можно распределить между оставшимися сегментами концентратора.

Многосегментные концентраторы – это программируемая основа больших сетей.

Возможность многосегментного концентратора программно изменять связи портов с внутренними шинами называется **конфигурационной коммутацией** (configuration switching).

Для соединения сегментов между собой нужны устройства другого типа – *мосты* или *коммутаторы*. Такое межсетевое устройство должно подключаться к нескольким портам многосегментного концентратора, подсоединенным к разным внутренним шинам, и выполнять передачу кадров или пакетов между сегментами точно так же, как если бы они были образованы отдельными устройствами-концентраторами.

Для крупных сетей многосегментный концентратор играет роль *интеллектуального кроссового шкафа,* который выполняет новое соединение не за счет механического перемещения вилки кабеля в новый порт, а за счет программного изменения внутренней конфигурации устройства.

2.5. Мосты и коммутаторы

Мосты

Мост (bridge) – ретрансляционная система, соединяющая каналы передачи данных.

В соответствии с базовой эталонной моделью взаимодействия открытых систем мост описывается протоколами физического и канального уровней, над которыми располагаются канальные процессы. Мост опирается на пару связываемых им физических средств соединения, которые в этой модели представляют физические каналы. Мост преобразует физический и канальный уровни различных типов. Что касается канального процесса, то он объединяет разнотипные каналы передачи данных в один общий.

Мост, а также его быстродействующий аналог *коммутатор* (switching hub) делят общую среду передачи данных на логические сегменты.

Логический сегмент образуется путем объединения нескольких физических сегментов (отрезков кабеля) с помощью одного или нескольких концентраторов. Каждый логический сегмент подключается к отдельному порту моста/коммутатора. При поступлении кадра на какой-либо из портов мост/коммутатор повторяет этот кадр, но не на всех портах, как это делает концентратор, а только на том порту, к которому подключен сегмент, содержащий компьютер-адресат.

Мосты могут соединять сегменты, использующие разные типы носителей, например, 10BaseT, 100BaseT, l000BaseT (витая пара), 10Base2 (тонкий коаксиальный кабель) и l000BaseFX (оптоволокно). Они могут соединять сети с разными методами доступа к каналу, например, сети Ethernet (метод доступа CSMA/CD) и Token Ring (метод доступа TDMA).

Коммутатор

Коммутатор (switch) – устройство, осуществляющее выбор одного из возможных вариантов направления передачи данных.

Общая структура коммутатора аналогична структуре моста.

В коммуникационной сети коммутатор является ретрансляционной системой (система, предназначенная для передачи данных или преобразования протоколов), обладающей свойством прозрачности (т. е. коммутация осуществляется здесь без какой-либо обработки данных). Коммутатор не имеет буферов и не может накапливать данные. Поэтому при использовании коммутатора скорости передачи сигналов в соединяемых каналах передачи данных должны быть одинаковыми. Канальные процессы, реализуемые коммутатором, выполняются специальными интегральными схемами. В отличие от других видов ретрансляционных систем, здесь, как правило, не используется программное обеспечение.

Коммутатор может соединять серверы в кластер и служить основой для объединения нескольких рабочих групп. Он направляет пакеты данных между узлами ЛВС. Каждый коммутируемый сегмент получает доступ к каналу передачи данных без конкуренции и видит только тот трафик, который направляется в его сегмент. Коммутатор должен предоставлять каждому порту возможность соединения с максимальной скоростью без конкуренции со стороны других портов (в отличие от совместно используемого концентратора). Обычно в коммутаторах имеется один или два высокоскоростных порта, а также достаточные инструментальные средства для решения задач управления.

Коммутатором можно заменить маршрутизатор, дополнить им наращиваемый маршрутизатор или использовать коммутатор в качестве основы для соединения нескольких концентраторов. Коммутатор может служить отличным устройством для направления трафика между концентраторами ЛВС рабочей группы и загруженными файл-серверами.

Коммутатор локальной сети (local area network switch) – устройство, обеспечивающее взаимодействие сегментов одной либо группы локальных сетей.

Коммутатор локальной сети, как и обычный коммутатор, обеспечивает взаимодействие подключенных к нему локальных сетей (рис. 2.1).

В дополнение к основной функции он осуществляет преобразование интерфейсов, если **соединяются** различные типы сегментов локальной сети. Чаще всего это сети Ethernet, кольцевые сети IBM, сети с оптоволоконным распределенным интерфейсом данных.

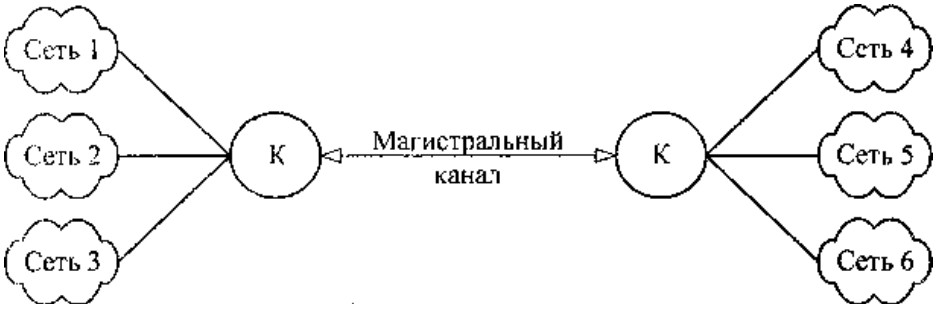

Рис. 2.1. Схема подключения локальных сетей к коммутаторам

В перечень функций, выполняемых коммутатором локальной сети, входят:

- обеспечение сквозной коммутации;
- наличие средств маршрутизации;
- поддержка простого протокола управления сетью;
- имитация моста либо маршрутизатора;
- организация виртуальных сетей;
- скоростная ретрансляция блоков данных.

Необходимо отметить, что, несмотря на сходство мостов и коммутаторов, ключевая разница между ними состоит в том, что *мост в каждый момент времени может осуществлять передачу кадров только между одной парой портов, а коммутатор одновременно поддерживает потоки данных между всеми своими портами.* Другими словами, мост передает кадры последовательно, а коммутатор – параллельно.

2.6. Техническая реализация и дополнительные функции коммутаторов

В настоящее время существует большое разнообразие моделей коммутаторов. Они отличаются как внутренней организацией, так и набором выполняемых дополнительных функций, таких, как трансляция протоколов, поддержка алгоритма покрывающего дерева, образование виртуальных логических сетей и рядом других.

Современные коммутаторы используют в качестве базовой одну из трех схем, на которой строится такой узел обмена:

- коммутационная матрица;
- разделяемая многовходовая память;
- общая шина.

Часто эти три способа взаимодействия комбинируются в одном коммутаторе.

В конструктивном отношении коммутаторы делятся на следующие типы:

- автономные коммутаторы с фиксированным количеством портов;
- модульные коммутаторы на основе шасси;
- коммутаторы с фиксированным количеством портов, собираемые в стек.

Автономный коммутатор обычно предназначен для организации небольших рабочих групп.

Модульные коммутаторы на основе шасси чаще всего предназначены для применения на магистрали сети. Поэтому они выполняются на основе какой-либо комбинированной схемы, в которой взаимодействие модулей организуется по быстродействующей шине или же на основе быстрой разделяемой памяти большого объема. Модули такого коммутатора выполняются на основе технологии «hot swap», т. е. допускают замену на ходу, без выключения коммутатора, так как центральное коммуникационное устройство сети не должно иметь перерывов в работе. Шасси обычно снабжается резервированными источниками питания и резервированными вентиляторами в тех же целях.

С технической точки зрения определенный интерес представляют *стековые коммутаторы.* Эти устройства представляют собой коммутаторы, которые могут работать автономно, так как выполнены в отдельном корпусе, но имеют специальные интерфейсы, которые позволяют их объединять в общую систему, работающую как единый коммутатор. Говорят, что в этом случае отдельные коммутаторы образуют стек.

Обычно такой специальный интерфейс представляет собой высокоскоростную шину, которая позволяет объединить отдельные корпуса подобно модулям в коммутаторе на основе шасси. Так как расстояния между корпусами больше, чем между модулями на шасси, скорость обмена по шине обычно ниже, чем у модульных коммутаторов: 200–400 Мбит/с. Не очень высокие скорости обмена между коммутаторами стека обусловлены также тем, что стековые коммутаторы обычно занимают промежуточное положение между коммутаторами с фиксированным количеством портов и коммутаторами на основе шасси. Стековые коммутаторы применяют для создания сетей рабочих групп и отделов, поэтому сверхвысокие скорости шин обмена им не очень нужны и не соответствуют их ценовому диапазону.

2.7. Маршрутизаторы и шлюзы

Структура маршрутизатора

Маршрутизатор (router) – ретрансляционная система, соединяющая две коммуникационные сети либо их части.

Каждый маршрутизатор реализует протоколы физического, канального и сетевого уровней.

Физический, канальный и сетевой протоколы в разных сетях различны. Поэтому соединение пар коммуникационных сетей осуществляется через маршрутизаторы, которые совершают необходимое преобразование указанных протоколов. Сетевые процессы выполняют взаимодействие соединяемых сетей.

Маршрутизатор работает с несколькими каналами, направляя в какой-нибудь из них очередной блок данных. Маршрутизаторы обмениваются информацией об изменениях структуры сетей, трафике. Благодаря этому выбирается оптимальный маршрут следования блока данных в разных сетях от абонентской системы-отправителя к системе-получателю. Маршрутизаторы обеспечивают также соединение административно независимых коммуникационных сетей.

Различие между маршрутизаторами и мостами

Маршрутизаторы превосходят мосты своей способностью фильтровать и направлять пакеты данных в сети.

Так как маршрутизаторы работают на сетевом уровне, они могут соединять сети, использующие разную сетевую архитектуру, методы доступа к каналам связи и протоколы.

Маршрутизаторы не обладают такой способностью к анализу сообщений как мосты, но зато могут принимать решение о выборе оптимального пути для данных между двумя сетевыми сегментами.

Мосты принимают решение по поводу адресации каждого из поступивших пакетов данных, переправлять его через мост или нет в зависимости от адреса назначения. Маршрутизаторы же выбирают из таблицы маршрутов наилучший для данного пакета.

В «поле зрения» маршрутизаторов находятся только пакеты, адресованные к ним предыдущими маршрутизаторами, в то время как мосты должны обрабатывать все пакеты сообщений в сегменте сети, к которому они подключены.

Тип топологии или протокола уровня доступа к сети не имеет значения для маршрутизаторов, так как они работают на уровень выше, чем мосты (сетевой уровень модели OSI). Маршрутизаторы часто используются для связи между сегментами с одинаковыми протоколами высокого уровня. Наиболее распространенным транспортным протоколом, который используют маршрутизаторы, является IPX фирмы Novell или TCP фирмы Microsoft.

Необходимо помнить, что для работы маршрутизаторов требуется один и тот же протокол во всех сегментах, с которыми он связан. При связывании сетей с различными протоколами лучше использовать мосты. Для управления загруженностью трафика сегмента сети также можно использовать мосты.

Шлюз (gateway) – ретрансляционная система, обеспечивающая взаимодействие информационных сетей.

Шлюз является наиболее сложной ретрансляционной системой, обеспечивающей взаимодействие сетей с различными наборами протоколов всех семи уровней. В свою очередь наборы протоколов могут опираться на различные типы физических средств соединения.

В тех случаях, когда соединяются информационные сети, в них часть уровней может иметь одни и те же протоколы. Тогда сети соединяются не при помощи шлюза, а на основе более простых ретрансляционных систем, именуемых маршрутизаторами и мостами.

Шлюзы оперируют на верхних уровнях модели OSI (сеансовом, представительском и прикладном) и представляют наиболее развитый метод подсоединения сетевых сегментов и компьютерных сетей. Необходимость в сетевых шлюзах возникает при объединении двух систем, имеющих различную архитектуру. Например, шлюз приходится использовать для соединения сети (протокол TCP/IP) и большой ЭВМ со стандартом SNA. Эти две архитектуры не имеют ничего общего, и потому требуется полностью переводить весь поток данных, проходящих между двумя системами.

В качестве шлюза обычно используется выделенный компьютер, на котором запущено программное обеспечение шлюза и производятся преобразования, позволяющие взаимодействовать нескольким системам в сети. Другой функцией шлюзов является преобразование протоколов. При получении сообщения IPX/SPX для клиента TCP/IP шлюз преобразует его в соответствии с протоколом TCP/IP.

2.8. Оборудование для сетей Wi-Fi

Сети Wi-Fi отождествляются с аббревиатурой *WLAN* (Wireless Local Area Network). Для организации *сетей Wi-Fi* (Wireless Fidelity, беспроводное соответствие) необходимы Wi-Fi сетевые карты, точки доступа и антенны. Необходимость в использовании точек доступа отпадает, когда мы говорим об очень малых сетях, размещенных в одном помещении. Использование точек доступа позволяет более гибко настроить сеть, объединить клиентов проводных и беспроводных сетей, а также установить связь с удаленными объектами (внешнее исполнение).

Wi-Fi сетевые карты по сути мало чем отличаются от обычных сетевых карт, за исключением некоторых особенностей настройки. Wi-Fi сетевые карты представлены в трех основных вариантах исполнения – внутренние PCI-карты, CARDBUS и USB адаптеры. Также существуют адаптеры в COMPACT FLASH форм-факторе.

Адаптеры различаются по платформе, в которой они используются: PCI – настольный компьютер; CARDBUS – ноутбук; Compact Flash – карманный компьютер; USB – универсален. Принцип построения и настройки сетей един и не зависит от форм-фактора Wi-Fi адаптера. Необходимо отметить, что тип адаптера влияет лишь на излучаемую мощность передатчика и чувствительность приемника, а также возможность использования внешней антенны.

2.9. Wi-Fi точки доступа

Wi-Fi точки доступа – устройства, позволяющие объединять клиентов сети (как проводной, так и беспроводной) в единую сеть. Другими словами, для Wi-Fi клиентов точка доступа – своеобразный хаб (концентратор). Для клиентов проводной сети – возможность выхода в сеть к беспроводным клиентам.

Wi-Fi точки доступа представлены в двух основных вариантах исполнения – для использования внутри помещений и для внешнего использования. Существуют варианты исполнения точек доступа, совмещенных с панельными антеннами, для внешнего использования.

При рассмотрении точек доступа исполнение играет очень важную роль. То есть внутриофисные точки доступа нельзя использовать на улице, а внешние – крайне нецелесообразно использовать внутри помещений. Также исполнение Wi-Fi точек доступа определяет их функциональные возможности.

Внутриофисные точки доступа служат для объединения Wi-Fi клиентов внутри помещений. Они оснащены функциями фильтров, создания виртуальных сетей и т. д. Но зачастую используются точки доступа с более широкими возможностями: WAN-порт, firewall, Ftp-сервер и т. д.

Внешние Wi-Fi точки доступа служат для объединения Wi-Fi клиентов вне помещений, например в публичных местах. Внешние точки доступа имеют защищенное исполнение, более жесткие эксплуатационные характеристики и т. д. При применении нескольких внешних точек доступа можно соединить достаточно удаленные объекты и создать публичный *хот-спот.* Внешние Wi-Fi точки доступа отличаются и большей излучаемой мощностью. Ко всем внешним точкам доступа можно подключить дополнительные антенны, что позволяет расширить зону покрытия Wi-Fi сети.

Следует обратить внимание на то, что многие точки доступа могут выступать в роли беспроводного клиента, что значительно расширяет область их применения.

2.10. Средства обеспечения защиты информации в сети

Сетевой, или **межсетевой**, **экран –** это комплекс программно-аппаратных средств, осуществляющий информационную защиту одной ча-

сти компьютерной сети от другой путем анализа проходящего между ними трафика.

Для сетевых экранов существуют и другие термины, хорошо отражающие функциональное назначение средств защиты этого типа:

1. Брандмауэр – это слово много лет назад пришло в русский язык из немецкого. Изначально оно обозначало перегородку в поезде, отделяющую область топки паровоза от пассажирского отделения.

2. Файервол и другие транслитерации английского слова firewall, хотя официально не приняты, можно встретить в литературе достаточно часто. Исходным значением этого термина является элемент конструкции дома, а именно стена, сделанная из огнеупорного материала и препятствующая распространению огня между частями дома (обычно принадлежащими разным собственникам).

Для сетевого экрана одна часть сети является *внутренней*, другая – *внешней* (рис. 2.2). Сетевой экран защищает внутреннюю сеть (например, локальную сеть предприятия или, как вырожденный случай, отдельный компьютер пользователя) от угроз, исходящих из внешней сети (мы будем, как правило, подразумевать под такой сетью Интернет).

Защиту границ между локальными сетями предприятия и Интернетом обеспечивают **корпоративные сетевые экраны**, те же функции, но на границе между домашним компьютером и Интернетом выполняют **персональные сетевые экраны.** Для эффективного выполнения сетевым экраном его главной функции – защиты – необходимо, чтобы через него проходил *весь* трафик, которым обмениваются узлы защищаемой части сети с узлами Интернета. Такое расположение позволяет сетевому экрану полностью контролировать (запрещать, ограничивать или протоколировать) доступ внешних пользователей к ресурсам внутренней сети. Сетевой экран защищает сеть не только от несанкционированного доступа внешних злоумышленников, но и от ошибочных действий пользователей защищаемой сети, например таких, как передача во внешнюю сеть конфиденциальной информации.

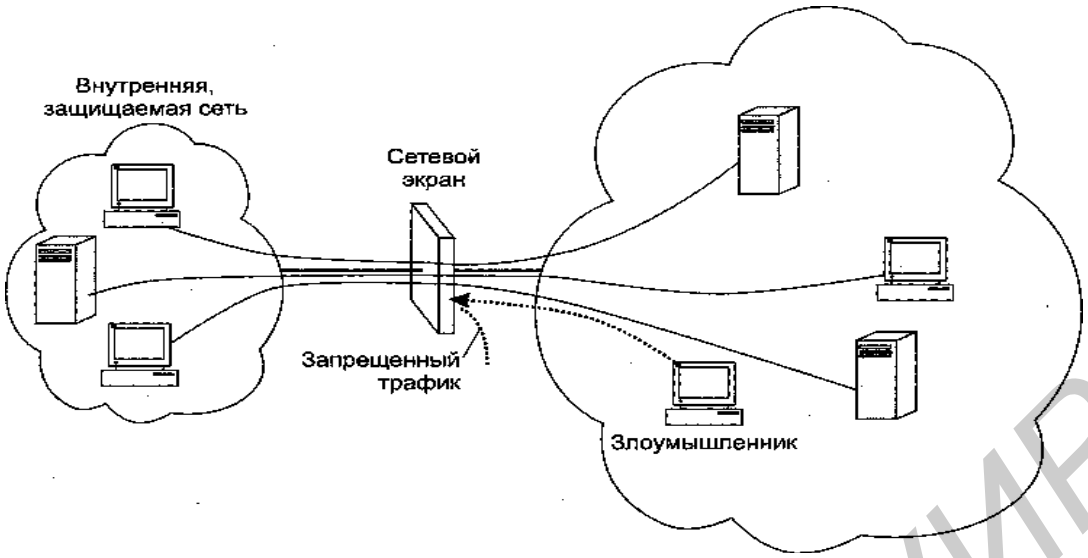

Рис. 2.2. Сетевой экран защищает внутреннюю сеть от угроз, исходящих из внешней сети

Чтобы осуществлять контроль доступа, сетевой экран должен уметь выполнять следующие функции:

- анализировать, контролировать и регулировать трафик (функция фильтрации);
- играть роль логического посредника между внутренними клиентами и внешними серверами (функция прокси-сервера);
- фиксировать все события, связанные с безопасностью (функция аудита).

Наряду с этими базовыми функциями на сетевой экран могут быть возложены и другие вспомогательные функции защиты, в частности:

- антивирусная защита;
- шифрование трафика;
- фильтрация сообщений по содержимому, включая типы передаваемых файлов, имена DNS и ключевые слова;
- предупреждение и обнаружение вторжений и сетевых атак;
- функции VPN;
- трансляция сетевых адресов.

Как можно заметить, большинство из перечисленных функций реализуются в виде отдельных продуктов или в составе систем защиты других типов. Так, функции пакетной фильтрации встроены практически во все маршрутизаторы, задача обнаружения вирусов решается множеством разнообразных программ, шифрование трафика – неотъемлемый элемент технологий защищенных каналов и т. д. Прокси-серверы часто поставляются в виде приложений, более того, они сами часто интегрируют в себе многие функции, свойственные сетевым экранам, такие, например, как аутентификация,

трансляция сетевых адресов или фильтрация по содержимому **(контенту)**.

2.11. Типы сетевых экранов разных уровней

Одной из принятых классификаций сетевых экранов является разделение их на типы в зависимости от уровня модели OSI, на котором они работают.

Сетевые экраны сетевого уровня, называемые также **экранами с фильтрацией пакетов** (packet filtering firewall), в полном соответствии со своим названием решают задачу фильтрации пакетов по IP-адресам и портам приложений на основании списков доступа. Фильтрация на основе статических правил, при которой не отслеживаются состояния соединений, называется **простой фильтрацией** (stateless packet inspection). Этому типу сетевых экранов соответствуют маршрутизаторы. Преимуществами брандмауэров сетевого уровня являются простота, невысокая стоимость и минимальное влияние на производительность сети.

Сетевые экраны сеансового уровня отслеживают состояние соединений. Они фиксируют подозрительную активность, направленную на сканирование портов и сбор другой информации о сети. *Отслеживание состояний соединений* заключается в том, что сетевой экран проверяет, насколько соответствует последовательность обмена сообщениями контролируемому протоколу. Например, если клиент посылает TCP-сообщение *SYN*, запрашивающее TCP-соединение, сервер должен отвечать TCP-сообщением *ЛСК SYN*, а не посылать в ответ свой TCP-запрос *SYN*. После того как сетевой экран установил допустимость TCP-соединения, он начинает работать простым передаточным звеном между клиентом и сервером. Для того чтобы контролировать процесс установления соединения, сетевой экран должен фиксировать для себя текущее состояние соединения, т. е. *запоминать,* какое последнее сообщение отправил клиент и какое сообщение он ожидает получить. Такой подход, когда пропускаются только те пакеты, которые удовлетворяют логике работы соответствующего протокола, называют **фильтрацией с учетом контекста** (stateful packet inspection). Благодаря такой способности брандмауэры сетевого уровня могут защищать серверы внутренней сети от различных видов атак, использующих уязвимости протоколов, в частности от DoS-атак.

Сетевые экраны прикладного уровня способны интерпретировать, анализировать и контролировать содержимое сообщений, которыми обмениваются приложения. К этому уровню относят прокси-серверы, о которых мы будем говорить подробнее далее. Прокси-сервер перехватывает запросы клиентов к внешним серверам за тем, чтобы потом отправить их от своего имени. Этот тип

сетевых экранов обеспечивает самый высокий уровень защиты, хотя и имеет свои недостатки, например, требует больших вычислительных затрат. Кроме того, прокси-серверы могут скрывать адрес «доверившегося» ему клиента, что снижает эффективность других средств защиты.

3. ТЕХНОЛОГИИ ДОСТУПА В ИНТЕРНЕТ

Увеличение потоков информации, передаваемых по сети Интернет компаниями и частными пользователями, а также потребность в организации удаленного доступа к корпоративным сетям, породили потребность в создании недорогих технологий цифровой высокоскоростной передачи данных по самому «узкому» месту цифровой сети – абонентской телефонной линии. Технологии xDSL позволяют значительно увеличить скорость передачи данных по медным парам телефонных проводов без необходимости модернизации абонентских телефонных линий. Именно возможность преобразования существующих телефонных линий в высокоскоростные каналы передачи данных и является главным преимуществом технологий DSL.

ADSL (Asymmetric Digital Subscriber Line) – асимметричная цифровая абонентская линия. Данная технология является асимметричной, т. е. скорость передачи данных от сети к пользователю значительно выше, чем скорость передачи данных от пользователя в сеть. Такая асимметрия в сочетании с состоянием «постоянно установленного соединения» делает технологию ADSL идеальной для организации доступа в сеть Интернет, доступа к локальным сетям. При организации таких соединений пользователи обычно получают гораздо больший объем информации, чем передают. Технология ADSL обеспечивает скорость «нисходящего» потока данных в пределах от 1,5 до 8 Мбит/с и скорость «восходящего» потока данных от 640 Кбит/с до 1,5 Мбит/с. ADSL позволяет передавать данные со скоростью 1,54 Мбит/с на расстояние до 5,5 км по одной витой паре проводов. Скорость передачи порядка 6–8 Мбит/с может быть достигнута при передаче данных на расстояние не более 3,5 км по проводам диаметром 0,5 мм.

R-ADSL (Rate-Adaptive Digital Subscriber Line) – цифровая абонентская линия с адаптацией скорости соединения. Технология R-ADSL обеспечивает такую же скорость передачи данных, что и технология ADSL, но при этом позволяет адаптировать скорость передачи к протяженности и состоянию используемой витой пары проводов. При использовании технологии R-ADSL соединение на разных телефонных линиях будет иметь разную скорость передачи данных. Скорость передачи данных может выбираться при синхронизации линии, во время соединения или по сигналу, поступающему от станции.

IDSL (ISDN Digital Subscriber Line) – цифровая абонентская линия IDSN. Технология IDSL обеспечивает полностью дуплексную передачу данных на скорости до 144 Кбит/с. В отличие от ADSL возможности IDSL ограничиваются только передачей данных. Несмотря на то что IDSL, так же как и ISDN,

использует модуляцию 2B1Q, между ними имеется ряд отличий. В отличие от ISDN линия IDSL является некоммутируемой линией, не приводящей к увеличению нагрузки на коммутационное оборудование провайдера. Также линия IDSL является «постоянно включенной» (как и любая линия, организованная с использованием технологии DSL), в то время как ISDN требует установки соединения.

HDSL (High Bit-Rate Digital Subscriber Line) – высокоскоростная цифровая абонентская линия. Технология HDSL предусматривает организацию симметричной линии передачи данных, т. е. скорости передачи данных от пользователя в сеть и из сети к пользователю равны. Благодаря скорости передачи – 1,544 Мбит/с по двум парам проводов и 2,048 Мбит/с по трем парам проводов – телекоммуникационные компании используют технологию HDSL в качестве альтернативы линиям T1/E1.

SDSL (Single Line Digital Subscriber Line) – однолинейная цифровая абонентская линия. Так же как и технология HDSL, технология SDSL обеспечивает симметричную передачу данных со скоростями, соответствующими скоростям линии T1/E1, но при этом технология SDSL имеет два важных отличия. Во-первых, используется только одна витая пара проводов, а во-вторых, максимальное расстояние передачи ограничено 3 км. В пределах этого расстояния технология SDSL обеспечивает, например, работу системы организации видеоконференций, когда требуется поддерживать одинаковые потоки передачи данных в оба направления. В определенном смысле технология SDSL является предшественником технологии HDSL2.

VDSL (Very High Bit-Rate Digital Subscriber Line) – сверхвысокоскоростная цифровая абонентская линия). Технология VDSL является наиболее «быстрой» технологией xDSL. Она обеспечивает скорость передачи данных «нисходящего» потока в пределах от 13 до 52 Мбит/с, а скорость передачи данных «восходящего» потока в пределах от 1,5 до 2,3 Мбит/с, причем по одной витой паре телефонных проводов. В симметричном режиме поддерживаются скорости до 26 Мбит/с. Технология VDSL может рассматриваться как экономически эффективная альтернатива прокладыванию волоконно-оптического кабеля до конечного пользователя. Однако максимальное расстояние передачи данных для этой технологии составляет от 300 до 1300 м.

4. ПРОЕКТИРОВАНИЕ СЕТИ

4.1. Выбор размера и структуры сети

Под размером сети в данном случае понимают как количество объединяемых в сеть компьютеров, так и расстояния между ними. Надо четко представлять себе, сколько компьютеров (минимально и максимально) нуждается в подключении к сети. При этом необходимо оставлять возможность для дальнейшего роста количества компьютеров в сети, хотя бы на 20–50 %.

Совсем не обязательно раз и навсегда включать в сеть все компьютеры предприятия. Иногда имеет смысл оставить некоторые из них автономными, например, из соображений безопасности информации на их дисках. Количество подключенных к сети компьютеров сильно влияет как на производительность, так и на сложность ее обслуживания. Оно также определяет стоимость требуемых программных средств, поэтому просчеты могут иметь довольно серьезные последствия.

Требуемая длина линий связи сети также играет немалую роль в проектировании сети. Например, если расстояния очень большие, может понадобиться использование дорогого оборудования. К тому же с увеличением расстояния резко возрастает значимость защиты линий связи от внешних электромагнитных помех. От расстояния зависит и скорость передачи информации по сети (выбор между разными типами сетей [1, с. 120]). Целесообразно при выборе расстояний закладывать небольшой запас (хотя бы 10 %) для учета непредвиденных обстоятельств. Преодолеть ограничения по длине иногда можно путем выбора структуры сети, разбиения ее на отдельные части.

Под структурой сети понимают способ разделения сети на части (сегменты), а также способ соединения этих сегментов между собой. Сеть предприятия может включать в себя рабочие группы компьютеров, сети подразделений, опорные сети, средства связи с другими сетями. Для объединения частей сети могут использоваться репитеры, репитерные концентраторы, коммутаторы, мосты и маршрутизаторы. Причем в ряде случаев стоимость этого объединительного оборудования может даже превысить стоимость компьютеров, сетевых адаптеров и кабеля, поэтому выбор структуры сети исключительно важен.

В идеале структура сети должна соответствовать структуре здания или комплекса зданий предприятия.

4.2. Иерархия и основные части сети

Рабочие места группы сотрудников, занимающихся одной задачей (например, бухгалтерия, отдел продаж, инженерная группа), должны размещаться в одной

или рядом расположенных комнатах. Тогда можно компьютеры этих сотрудников объединить в один сегмент, в единую рабочую группу и установить вблизи их комнат сервер, с которым они будут работать, а также концентратор или коммутатор, связывающий все их машины. Точно так же рабочие места сотрудников подразделения, занимающихся комплексом близких задач, лучше расположить на одном этаже здания, что существенно упростит их объединение в сегмент и дальнейшее его администрирование. На этом же этаже удобно расположить коммутаторы, маршрутизаторы и серверы, с которыми работает данное подразделение.

Как и в других случаях, при выборе структуры разумно оставлять возможности для дальнейшего развития сети. Например, лучше приобретать коммутаторы или маршрутизаторы с количеством портов, несколько большим, чем требуется в настоящий момент (хотя бы на 10–20 %). Это позволит при необходимости легко включить в сеть один или несколько сегментов. Ведь любое предприятие всегда стремится к росту (порой совершенно напрасно), и этот рост не должен каждый раз приводить к необходимости проектировать сеть предприятия заново.

Например, небольшое предприятие занимает три этажа, на каждом по пять комнат, и включает в себя три подразделения по три группы. В этом случае можно построить сеть следующим образом (рис. 4.1):

1. Рабочие группы занимают по 1–3 комнаты, их компьютеры объединены между собой репитерными концентраторами. Концентратор может использоваться один на комнату, один на группу или один на весь этаж. Концентратор целесообразно расположить в помещении, в которое имеет доступ минимальное количество сотрудников.

2. Подразделения занимают отдельный этаж. Все три сети рабочих групп каждого подразделения объединяются коммутатором, а для связи с сетями других подразделений используется маршрутизатор. Коммутатор вместе с одним из концентраторов лучше поместить в отдельной комнате.

3. Общая сеть предприятия включает три сегмента сетей подразделений, объединенных маршрутизатором. Этот же маршрутизатор может использоваться для подключения к глобальной сети.

4. Серверы рабочих групп располагаются в комнатах рабочих групп, серверы подразделений – на этажах подразделений.

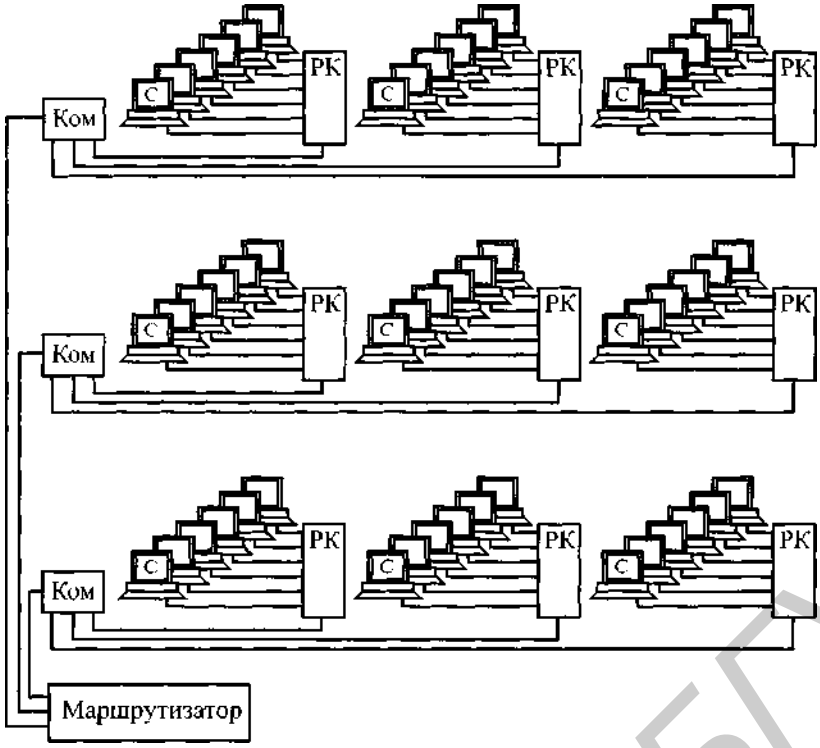

Рис. 4.1. Структура сети предприятия:
С – серверы рабочих групп; РК – репитерные концентраторы;
Ком – коммутаторы

В рассмотренной ситуации области коллизий (зоны конфликта) сети будут включать в себя сегменты, расположенные в комнатах каждой рабочей группы, плюс сегмент, связывающий концентратор рабочей группы с коммутатором подразделения. Всего таких областей коллизий будет девять. Именно для них необходимо проводить расчеты работоспособности сети [4].

Широковещательные области будут включать в себя все сегменты сети каждого подразделения плюс сегмент, связывающий коммутатор подразделения с маршрутизатором предприятия. Таких широковещательных областей будет всего три.

Если предполагаемая интенсивность обмена по проектируемой сети недостаточно велика, компьютеров не слишком много и размеры здания позволяют, то вполне возможно обойтись без маршрутизаторов – довольно сложных и сравнительно дорогих устройств.

Тогда сети подразделений будут связаны концентраторами, а между собой они будут соединяться коммутаторами .

Области коллизий в данном случае будут включать в себя все сегменты сети каждого подразделения плюс сегмент, соединяющий концентратор подразделения и коммутатор предприятия. Таких областей коллизий всего три. Для них надо проводить расчет работоспособности сети, как описано в [4].

В единственную широковещательную область войдет вся сеть предприятия.

В ситуации, когда компьютеров на предприятии немного (до 50), имеет смысл отказаться не только от маршрутизаторов, но и от коммутаторов, оставив только репитерные концентраторы. Более того, при такой малой сети и низкой интенсивности обмена вполне может оказаться подходящей сеть Ethernet на тонком коаксиальном кабеле (сегменты 10BASE2) без концентраторов или с 1–2 простейшими репитерами. Правда, в последнем случае придется компьютеры каждого сегмента разместить на одном этаже из-за ограничений на длину кабеля сегмента 10BASE2. Следует учитывать, что во вновь создаваемых сетях использование коаксиального кабеля не рекомендуется.

В реальности все бывает гораздо сложнее. Например, структура подразделений может вообще не соответствовать структуре комнат и этажей. Предприятие может занимать два разнесенных друг от друга помещения в одном здании или даже 3–4 удаленных здания. Тогда может понадобиться применение оптоволоконных сегментов (в том числе и полнодуплексных, которые обеспечивают максимальную длину кабеля [1, с. 274]). А структура сети при этом обычно чрезвычайно сложна – с множеством областей коллизий и широковещательных областей.

4.3. Распределение IP-адресов

В основе работы протокола TCP/IPv4 лежит принцип использования уникального идентификатора устройства, в качестве которого применяется IP- адрес.

Ключевым понятием в IP-адресации является класс сети. Различают три основных класса сети, которые однозначно идентифицируются первым числом в группе чисел IP-адреса. В таблице 4.1 показано, как распределяются адреса в зависимости от класса сети.

Таблица 4.1

Принцип адресации в сетях различных классов

Класс сети	Диапазон, первый байт	Максимальное число адресов в сети	Пример адреса
A	1–126	16 777 214	101.2.14.192
B	128–191	65 534	150.2.2.1
C	192–223	254	192.168.2.1

Класс сети определяет ее значимость в общей структуре, а также способ определения адреса подсети, адреса узла и количество компьютеров, которое она может обслуживать.

С процессом IP-адресации тесно связаны понятия классовой и бесклассовой

адресации. Классовая адресация основана на определении класса сети с помощью табл. 4.1. Данный способ адресации очень неэффективен и приводит к быстрому истощению свободных IP-адресов. Для примера рассмотрим адреса, приведенные в табл. 4.1:

- 101.2.14.192. Данный адрес означает следующее: узел принадлежит сети класса А, адрес подсети – 101, адрес узла – 0.2.14.192, под адресацию отводится 3 байта, максимальное количество узлов 16 777 214;
- 150.2.2.1. Данный адрес означает следующее: узел принадлежит сети класса В, адрес подсети – 150.2, адрес узла – 0.0.2.1, под адресацию отводится 2 байта, максимальное количество узлов – 65 534;
- 192.168.2.1. Данный адрес означает следующее: узел принадлежит сети класса С, адрес подсети – 192.168.2, адрес узла – 0.0.0.1, под адресацию отводится 1 байт, максимальное количество узлов – 254.

Если у нас малая сеть с 20-ю компьютерами, то, следуя принципу классовой адресации, наша сеть принадлежит классу С. Это означает, что ей необходимо выделить 254 IP-адреса, из которых будут задействованы 20, а остальные 234 – будут незанятыми. Подобное распределение адресов расточительно, и поэтому используется другой способ адресации.

В настоящее время бесклассовая адресация узлов сети применяется все шире и шире. Ее суть в следующем: параллельно с 32-битовым IP-адресом используется 32-битовая маска подсети, которая также состоит из четырех чисел, разделенных точкой. Применение маски базируется на следующем правиле: если рассматривать двоичное представление маски, то на месте адреса узла всегда стоят нули, на месте номера сети – единицы, например:

IP-адрес:
в десятичном представлении: 129.64.134.5;
в двоичном: 1000 0001.0100 0000.1000 0110.0000 0101.
Маска подсети:
в десятичном представлении: 255.255.128.0;
в двоичном: 1111 1111.1111 1111.1000 0000.0000 0000.
Номер подсети: 129.64.128.0.
Номер узла: 0.0.6.5.

Бесклассовый способ адресации позволяет проводить адресацию более экономно [17]. Именно с помощью маски подсети можно разбивать ЛВС на сегменты, используя единственный выделенный IP-адрес.

На практике это выглядит следующим образом. Предположим, имеется IP-адрес 129.64.134.5 и ЛВС из трех сегментов. Согласно правилу маски для

нумерации сегментов придется использовать 2 бита из 8 доступных (00 – 1-й сегмент, 01 – 2-й, 10 – 3-й, 11 – не используется). Это означает, что маска подсети имеет вид 1111 1111.1111 1111.1111 1111.1100 0000, а в десятичной форме – и 255.255.255.192. Шесть бит, которые остались для нумерации компьютеров сети, составят 2^6 или 64 компьютеров.

4.4. Планирование сети с концентратором

При выборе места для установки концентратора следует принять во внимание следующие аспекты:

- местоположение;
- расстояние;
- питание.

Выбор места установки концентратора является наиболее важным этапом планирования небольшой сети. Хаб разумно расположить вблизи геометрического центра сети (на одинаковом расстоянии от всех компьютеров). Такое расположение позволит минимизировать расход кабеля. Длина кабеля от концентратора до любого из подключаемых к сети компьютеров или периферийных устройств не должна превышать 100 м.

Концентратор можно поставить на стол или закрепить его на стене с помощью входящих в комплект хаба скоб. Установка хаба на стене позволяет упростить подключение кабелей, если они уже проложены в офисе.

При планировании сети необходимо предусматривать возможность наращивания (каскадирования) хабов.

Концентраторы имеют много преимуществ. Во-первых, в сети используется топология «звезда» при которой соединения с компьютерами образуют лучи, а хаб является центром «звезды». Такая топология упрощает установку и управление сетью. Любые перемещения компьютеров или добавление в сеть новых узлов при такой топологии совсем несложно выполнить. Кроме того, эта топология значительно надежнее, поскольку при любом повреждении кабельной системы сеть сохраняет работоспособность (перестает работать лишь поврежденный луч). Светодиодные индикаторы хаба позволяют контролировать состояние сети и легко обнаруживать неполадки.

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) в единый логический сегмент;
- автосегментация портов – автоматическое отключение порта при его не-

корректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т. п.);

- поддержка между концентраторами резервных связей, которые используются при отказе основных;
- защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютер с адресом назначения);
- поддержка средств управления сетями – протокола SNMP, баз управляющей информации MIB.

4.5. Оценка производительности сети

Вопрос об оценке производительности сетей, использующих случайный метод доступа CSMA/CD, не очевиден из-за того, что существуют несколько различных показателей. Прежде всего следует упомянуть три связанных между собой показателя, характеризующих производительность сети в идеальном случае – при отсутствии коллизий и при передаче непрерывного потока пакетов, разделенных только межпакетным интервалом IPG. Очевидно, такой режим реализуется, если один из абонентов активен и передает пакеты с максимально возможной скоростью. Неполное использование пропускной способности в этом случае связано, кроме существования интервала IPG, с наличием служебных полей в пакете Ethernet.

Пакет максимальной длины является наименее избыточным по относительной доле служебной информации. Он содержит 12 304 бит (включая интервал IPG), из которых 12 000 являются полезными данными.

Поэтому максимальная скорость передачи пакетов (или иначе – *скорость в кабеле* – wire speed) составит в случае сети Fast Ethernet 10^8 бит/с / 12304 бит = = 8127,44 пакет/с.

Пропускная способность представляет собой скорость передачи полезной информации и в данном случае будет равна 8127,44 пакет/с × 1500 байта = = 12,2 Мбайт/с.

Наконец, *эффективность использования* физической скорости передачи сети в случае Fast Ethernet будет равной 100 Мбит/с и по отношению только к полезным данным составит 8127,44 пакет/с × 12 000 бит/ 10^8 бит/с = 98 %.

При передаче пакетов минимальной длины существенно возрастает скорость в кабеле, что означает всего лишь факт передачи большого числа коротких пакетов. В то же время пропускная способность и эффективность заметно (почти в два раза) ухудшаются из-за возрастания относительной доли служебной информации.

Для реальных сетей, в частности Fast Ethernet, с большим числом активных абонентов N пропускная способность на уровне 12,2 Мбайт/с для какого-либо абонента является пиковым, редко реализуемым значением. При одинаковой активности всех абонентов средняя пропускная способность для каждого из них составит 12,2/N Мбайт/с, а на самом деле может оказаться еще меньше из-за возникновения коллизий, ошибок в работе сетевого оборудования и влияния помех (в случае работы локальной сети в условиях, когда кабельная система подвержена влиянию больших внешних электромагнитных наводок). Влияние помех, так же как и поздних конфликтов (late collision) в некорректных сетях, отслеживается с помощью анализа поля FCS-пакета.

Для реальных сетей более информативен такой показатель производительности, как *показатель использования сети* (network utilization), который представляет собой долю в процентах от суммарной пропускной способности (не поделенной между отдельными абонентами). Он учитывает коллизии и другие факторы. Ни сервер, ни рабочие станции не содержат средств для определения показателя использования сети. Этой цели служат специальные, не всегда доступные из-за высокой стоимости такие аппаратно-программные средства, как анализаторы протоколов.

Считается, что для загруженных систем Ethernet и Fast Ethernet хорошим значением показателя использования сети является 30 %. Это значение соответствует отсутствию длительных простоев в работе сети и обеспечивает достаточный запас в случае пикового повышения нагрузки. Однако, если показатель использования сети значительное время составляет 80...90 % и более, то это свидетельствует о практически полностью используемых (в данное время) ресурсах, но не оставляет резерва на будущее. Впрочем, для реальных сетей, например Fast Ethernet, это скорее гипотетическая ситуация.

На рис. 4.2 приведена зависимость показателя использования сети от времени при условии, что предложенная нагрузка (offered load), т. е. текущий запрос на пропускную способность, линейно возрастает. Зависимость показателя использования сети от времени следующая:

- при линейном увеличении предложенной нагрузки: 1 – наилучшая область работы; 2 – приемлемая; 3 – плохая;
- рассматриваемый показатель достигает максимума (точка полной нагрузки на графике).

При дальнейшем увеличении предложенной нагрузки показатель использования сети начинает уменьшаться, особенно резко после точки насыщения. Это «плохая» область работы сети. Считается, что сеть работает хорошо, если и предложенная нагрузка, и показатель использования сети высоки.

Некоторые авторы предлагают для широко распространенного понятия *«перегрузка»* (overload) сетей на основе метода доступа CSMA/CD следующее определение: сеть перегружена, если она не может работать при полной нагрузке в течение 80 % своего времени (при этом 20 % времени показатель использования сети недопустимо мал из-за коллизий). После точки насыщения наступает крах Ethernet (Ethernet collapse), когда возрастающая предложенная нагрузка заметно превышает возможности сети. Стоит заметить, что реально маловероятно, чтобы предложенная нагрузка постоянно увеличивалась во времени и надолго превышала пропускную способность сети типа Fast Ethernet. Более того, любой детерминированный метод доступа не может обеспечить реализацию сколь угодно большой предложенной нагрузки, существующей в течение продолжительного времени. Если данный вариант детерминированного метода доступа не использует, как и метод CSMA/CD, систему приоритетов, то ни один из абонентов не может захватить сеть более чем на время передачи одного пакета, однако передача данных отдельными пакетами с долгими паузами между ними ведет к снижению скорости передачи для каждого абонента. Преимущество детерминированных методов состоит в возможности простой организации системы приоритетов, что полезно из-за наличия определенной иерархии в любом крупном коллективе.

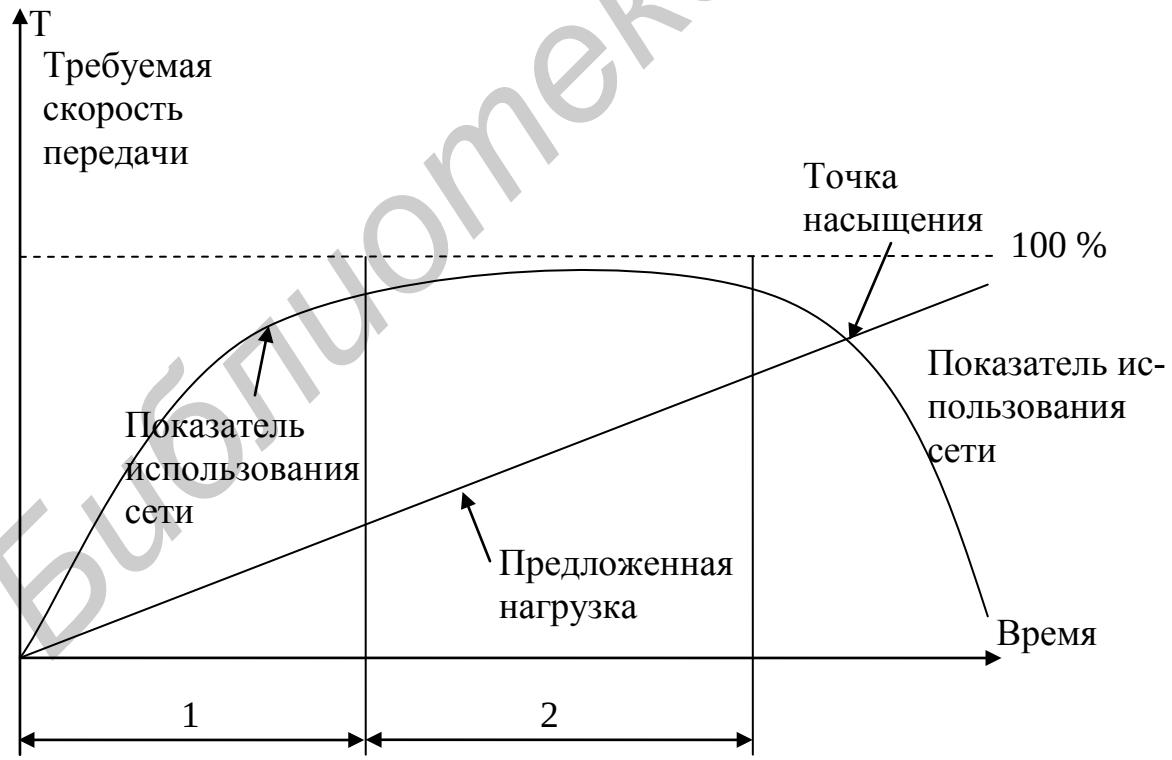

Рис. 4.2. Зависимость показателя использования сети от времени

4.6. Выбор оборудования

При выборе сетевого оборудования надо учитывать множество факторов:

- уровень стандартизации оборудования и его совместимость с наиболее распространенными программными средствами;
- скорость передачи информатизации и возможность ее дальнейшего увеличения;
- метод управления обменом в сети (CSMA/CD или маркерный метод);
- топологии сети (шина, звезда, дерево);
- типы кабеля;
- стоимость и технические характеристики конкретных аппаратных средств.

Следует четко представлять, что замена программного обеспечения проста, а вот замена аппаратных средств и в особенности прокладка кабеля обходится порой очень дорого, а порой и невозможна.

В настоящее время для локальных сетей чаще всего используется неэкранированная витая пара UTP. Экранированная витая пара, оптоволоконные кабели и другие виды соединений применяют только там, где это действительно нужно.

Следующая важная задача – выбор компьютеров. Если для рабочих станций можно использовать те компьютеры, которые уже имеются на предприятии, то для сервера следует приобретать специальный компьютер. Хорошо, если это будет специализированный компьютер, ориентированный для решения задач сети.

Требования к такому компьютеру следующие:

- максимально быстрый в работе;
- большой объем оперативной памяти;
- «быстрые» жесткие диски большого объема.

Для любой сети очень критична проблема устойчивого электропитания.

В идеальном случае от отключения электропитания должны быть защищены все компьютеры в сети.

Однако стоимость бесперебойного источника питания значительна, и часто обеспечивать все компьютеры сети такими источниками обходится хозяевам сети очень дорого.

В этом случае обязательно обеспечить бесперебойными источниками питания следует только серверы.

При проектировании сети приходится выбирать также сетевые адаптеры, репитеры, концентраторы, коммутаторы и маршрутизаторы.

Следует помнить, что быстродействие и надежность сети всегда определяется ее самым низкокачественным компонентом.

4.7. Проектирование кабельной системы

Считается, что к данному этапу проектирования тип кабеля уже определен. Более того, предполагается, что тип локальной сети (Ethernet, Fast Ethernet, FDDI или др.) также выбран. В этом подразделе рассматриваются рекомендации по организации кабельной системы для сетей на основе проводных соединений [11] (витых пар и оптоволокна). При выборе кабеля в первую очередь надо учитывать требуемую длину, а также защищенность от внешних помех и уровень собственных излучений. При большой длине сети и необходимости обеспечить секретность передаваемых данных или высоком уровне помех в помещении незаменим оптоволоконный кабель. Следует отметить, что применение оптоволоконных кабелей вместо электрических даже при достаточно комфортных условиях позволяет существенно (на 10–50 %) поднять производительность сети за счет снижения доли искаженных информационных пакетов.

При проектировании кабельных систем для локальных сетей накоплен большой опыт, на основе которого могут быть сформулированы общие рекомендации по организации таких систем. Более того, существуют стандарты под общим названием «структурированные кабельные системы (СКС)», которые особенно актуальны для вновь создаваемых или реконструируемых относительно больших локальных сетей на уровне предприятия. Для сравнительно небольших локальных сетей создание сертифицированной СКС, которое предполагает работу приглашенных специалистов, резонно рассматривается как излишняя роскошь. Ниже перечислены **общие рекомендации по созданию кабельных систем,** являющиеся фактически «подмножеством» недетализированных требований стандартов СКС:

1. Составить план размещения компьютеров и других сетевых устройств в помещении (или помещениях).

Провести анализ возможности перемещения всех или большей части компьютеров в одно или несколько соседних помещений. Это существенно упростит организацию кабельной системы и исключит необходимость использования излишних активных сетевых устройств. Следует также принять во внимание расширение сети в будущем, для чего предусмотреть наличие точек подключения к сети даже в тех помещениях, где сетевые компьютеры пока отсутствуют.

2. Оценить соответствие длины кабельной системы и ее отдельных частей (сегментов, соединений между данным абонентом и концентратором и т. д.) требованиям выбранной разновидности локальной сети. Для сетей семейства Ethernet необходимо учитывать ограничения на длины сегментов на разных типах кабелей

и задержки сигналов в кабельной системе в соответствии с правилами модели 1 или 2 [9]. Для сетей другого типа (Token Ring, FDDI и т. д.) действуют абсолютные ограничения на длины отдельных участков кабельной системы [9]. В случае если рассчитанная таким образом длина кабельной системы в целом или на отдельных участках превышает предельно допустимую или близка к ней, следует выбрать одно или несколько из следующих решений (в порядке предпочтения по простоте, стоимости и эффективности реализации):

- перейти к более качественному типу кабеля во всей сети или только на критичных участках (переход от неэкранированной витой пары к экранированной или оптоволокну);
- использовать дополнительные репитеры или репитерные концентраторы, позволяющие восстановить амплитуду и форму сигналов, повысив тем самым длину кабельной системы;
- перейти к другому типу сети, имеющему меньшие ограничения на длину кабельной системы (т. е. от сетей на витой паре к сетям на оптоволокне).

Таким образом, выбор конфигурации кабельной системы на данном и предыдущем этапах – итерационный процесс, который может затронуть и более ранние этапы проектирования (вплоть до выбора типов локальной сети и кабеля), если выбор на этих этапах был некорректным.

3. Кабельная система должна быть устойчива к внешним электромагнитным помехам и по возможности не генерировать заметные собственные излучения. В противном случае снижается фактическая скорость работы сети (из-за необходимости повторной передачи искаженных помехами пакетов), а также нарушаются требования защиты информации. Кабельная система должна быть защищена от механических повреждений.

4. Для прокладки кабелей сети лучше всего использовать специальные подвесные кабельные короба, настенные кабелепроводы или фальшполы. В этом случае кабели надежно защищены от механических воздействий. Самое дорогое решение – фальшпол, представляющий собой металлические панели, установленные на подставках и покрывающие весь пол помещения. Зато фальшпол позволяет легко и безопасно проложить огромное количество проводов, что особенно ценно в научных лабораториях, где помимо кабелей локальной сети существует множество других проводов. Для прокладки кабеля между комнатами или этажами обычно пробиваются отверстия в стенах или перекрытиях. По сравнению с прокладкой кабеля через двери комнат и стены коридоров это позволяет существенно сократить общую длину кабелей. Однако надо учитывать, что такое решение усложняет любые дальнейшие изменения в кабельной системе (замену кабелей, прокладку дополнительных кабелей, изменение расположения компью-

теров сети и т. д.). Кабели ни в коем случае не должны самостоятельно удерживать свой вес, так как со временем это может вызвать их обрыв. Их следует подвешивать на стальных тросах, причем для эксплуатации на открытом воздухе необходимы специально предназначенные для этого кабели с оболочкой, устойчивой к атмосферным воздействиям. По возможности надо использовать для соединения далеко разнесенных зданий подземные коллекторы. Но при этом необходимо предпринимать меры по защите кабелей от воздействия влаги.

5. Кабельная система должна иметь «прозрачную» и документированно оформленную структуру. Это необходимо как для обеспечения возможности внесения изменений в эту структуру, так и для поиска неисправностей.

Для объединения концов кабелей часто используются специальные распределительные шкафы, доступ к которым должен быть ограничен. Конечно, их применение оправдано только в том случае, если кабелей много (несколько десятков). Располагать распределительные шкафы целесообразно рядом с концентраторами, коммутаторами или маршрутизаторами.

6. Необходимо проверить целостность кабельной системы.

В сети на коаксиальном кабеле для этого можно было использовать непосредственные измерения омметром сопротивления при наличии и отсутствии согласующих нагрузок. В более современных сетях на витой паре и оптоволокне о целостности кабельной системы можно судить по показаниям индикаторов, расположенных на сетевых картах вблизи сетевых разъемов. Возможно также использование для этой цели специальных приборов – кабельных сканеров [11].

Структурированная кабельная система (СКС) представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. СКС состоит из набора медных и оптических кабелей, кросспанелей, соединительных шнуров, кабельных разъемов, модульных гнезд, информационных розеток и вспомогательного оборудования. Все перечисленные элементы интегрируются в единую систему и эксплуатируются согласно определенным правилам. Основные преимущества (или принципы) СКС:

1. Универсальность: передача данных в ЛВС, видеоинформации или сигналов от датчиков пожарной безопасности либо охранных систем по единой кабельной системе, организация локальной телефонной сети.

2. Гибкость: простота изменения конфигурации кабельной системы и управления перемещениями внутри и между зданиями.

3. Устойчивость: тщательно спланированная СКС устойчива к внештатным ситуациям и гарантирует высокую надежность и защиту данных в течение многих лет. Основным препятствием широкого внедрения СКС является, как уже отмечалось, их высокая стоимость, что делает приемлемым это решение для

относительно масштабных локальных сетей уровня предприятия. Действительно, стандарты на СКС предусматривают проведение наряду с прочими комплекса дорогостоящих строительных работ.

Основными стандартами на СКС являются:

1. Международный стандарт ISO/IEC 11801 Generic Cabling for Customer Premises.
2. Европейский стандарт EN 50173 Information technology – Generic cabling systems.

4.8. Обеспечение защиты информации в сети на основе сетевых экранов

Реализация сетевого экрана так же многовариантна, как и его функциональность. В качестве аппаратной составляющей сетевого экрана может выступать маршрутизатор или комбинация маршрутизаторов, компьютер или комбинация компьютеров, комбинация маршрутизаторов и компьютеров, наконец, это может быть специализированное устройство.

Таким же разнообразием отличается и программная составляющая сетевого экрана, имеющая гибкую структуру и включающая в себя различные модули, функции которых могут широко варьироваться.

Сложная структура аппаратных и программных средств сетевого экрана, разнообразие настраиваемых параметров, наборы правил, регламентирующих работу фильтров разного уровня, списки паролей и другой информации для проведения аутентификации, списки прав доступа пользователей к внутренним и внешним ресурсам сети – все это требует от администратора значительной дополнительной работы по конфигурированию. Только в случае качественной настройки аппаратуры и программных модулей сетевой экран действительно может стать краеугольным камнем системы защиты сети предприятия. «Умные» сетевые экраны позволяют администратору упростить эту работу, потому что они требуют только задания высокоуровневых правил политики безопасности сети, которые затем автоматически транслируются в низкоуровневые операции по конфигурированию отдельных функциональных подсистем сетевого экрана.

Архитектура

Простейшей архитектурой сети с сетевым экраном является вариант, когда все функции сетевого экрана реализуются *одним* программно-аппаратным устройством, например маршрутизатором, или, как показано на рис. 4.3, универсальным компьютером. Такой способ построения защиты логически самый

простой, однако он имеет очевидный недостаток, заключающийся в полной зависимости системы защиты от работоспособности одного звена, в данном случае – компьютера-брандмауэра.

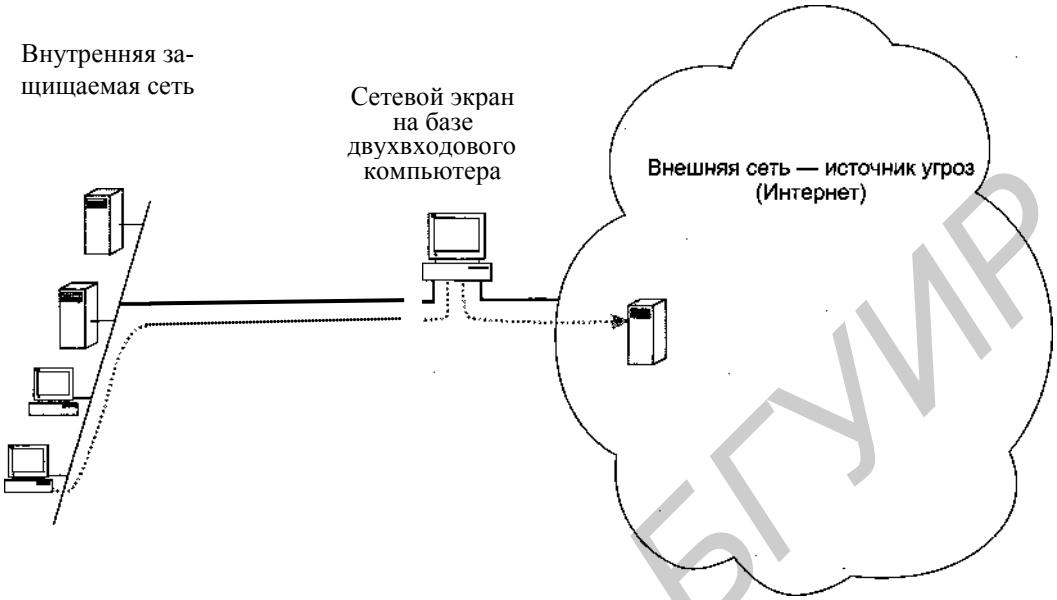

Рис. 4.3. Сетевой экран на базе двухвходового компьютера

Компьютер, играющий роль сетевого экрана, должен иметь по крайней мере два сетевых интерфейса, к одному из которых подключается внутренняя, к другому – внешняя сеть. Двухвходовой компьютер выполняет функции программного маршрутизатора, а также те функции сетевого экрана, конкретный перечень которых определяется установленным на данном компьютере программным обеспечением.

Более надежные схемы сетевых экранов включают несколько элементов. В сети, показанной на рис. 4.4, на рубеже защиты установлено два маршрутизатора, между которыми располагается так называемая сеть периметра.

Сеть периметра, или **сеть демилитаризованной зоны** (DMZ), – это сеть, которую *для* добавления еще одного уровня защиты внутренней сети размещают между внутренней и внешней сетями в качестве буфера. В сети периметра обычно располагаются компьютеры, которые предоставляют общедоступные сервисы, например почтовый сервер, внешний сервер DNS или внешний веб-сервер предприятия. В этой зоне могут быть размещены также прокси-серверы. Учитывая, что само назначение этих компьютеров предполагает практически никак не ограничиваемый доступ к ним внешних пользователей (а значит, и злоумышленников), их необходимо защищать особенно тщательно. Главными задачами при защите этих компьютеров (называемых иногда компьютерами-бастионами) является обеспечение целостности и доступности размещен-

ных на них данных для пользователей внешней сети. Эту задачу решают «индивидуальные» средства защиты, устанавливаемые на компьютерах-бастионах, такие, например, как антивирусные программы или фильтры спама.

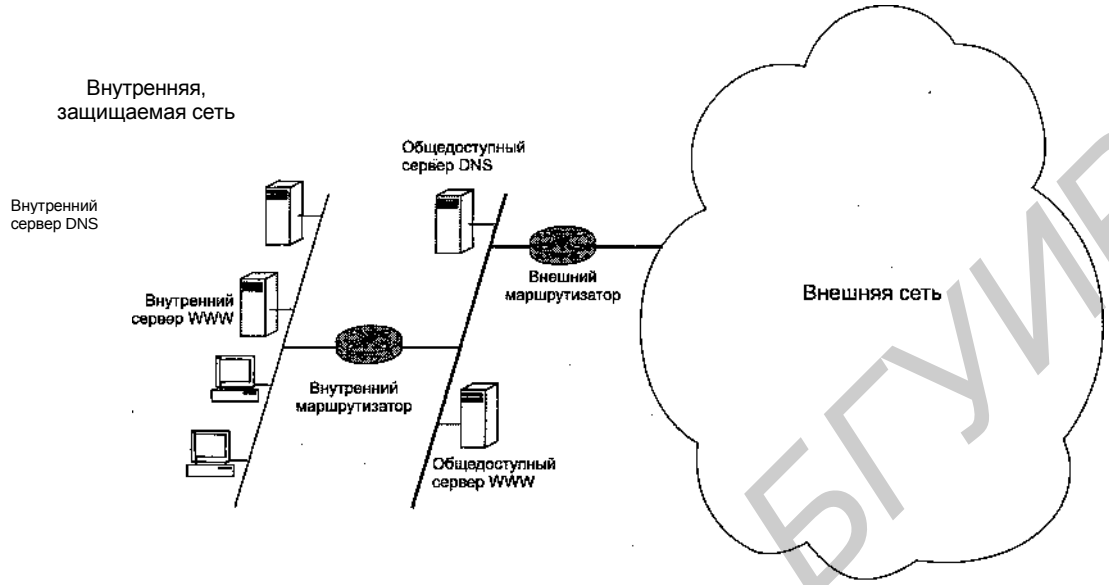

Рис. 4.4. Сетевой экран на базе двух маршрутизаторов

Чтобы пояснить, каким образом сеть периметра усиливает защиту внутренней сети, посмотрим, что произойдет, если какой-либо злоумышленник сможет «взломать» первый рубеж защиты – внешний маршрутизатор – и начнет прослушивать трафик подключенной к нему сети периметра. Очевидно, что он получит доступ только к трафику общедоступных серверов, который не является секретным.

Внешний маршрутизатор призван фильтровать трафик с целью защиты сети периметра и внутренней сети. Однако строгая фильтрация в этом случае оказывается невостребованной. Общедоступные серверы по своей сути предназначены для практически неограниченного доступа. Что касается защиты внутренней сети, правила фильтрации для доступа к ее узлам и сервисам являются одними и теми же для обоих маршрутизаторов, поэтому внешний маршрутизатор может просто положиться в этом деле на внутренний маршрутизатор.

Обычно внешний маршрутизатор находится в зоне ведения *провайдера*, и администраторы корпоративной сети ограничены в возможностях его оперативного реконфигурирования. Это является еще одной причиной, по которой функциональная нагрузка на внешний маршрутизатор обычно невелика. Основная работа по обеспечению безопасности локальной сети возлагается на *внутренний маршрутизатор*, который защищает ее как от внешней сети, так и

от сети периметра. Правила, определенные для узлов сети периметра по доступу к ресурсам внутренней сети, часто бывают более строгими, чем правила, регламентирующие доступ к этим ресурсам внешних пользователей. Это делается для того, чтобы в случае взлома какого-либо компьютера-бастиона уменьшить число узлов и сервисов, которые впоследствии могут быть атакованы с этого компьютера. Именно поэтому внутренний маршрутизатор должен отбрасывать все пакеты, следующие во внутреннюю сеть из сети периметра, исключая пакеты нескольких протоколов (например HTTP, SMTP, DNS), абсолютно необходимых пользователям внутренней сети для обращения к внешним серверам соответственно веб-службы, электронной почты и DNS, установленным в сети периметра.

4.9. Обслуживание сети, контроль, ее безопасности и безотказности

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

Следует заметить, что наряду с термином «защита информации» (применительно к компьютерным сетям) широко используется, как правило, в близком значении термин «компьютерная безопасность».

Переход от работы на персональных компьютерах к работе в сети усложняет защиту информации по следующим причинам:

1. Большое число пользователей в сети и их переменный состав. Защита на уровне имени и пароля пользователя недостаточна для предотвращения входа в сеть посторонних лиц.

2. Значительная протяженность сети и наличие многих потенциальных каналов проникновения в сеть, в их числе неидеальные встроенные средства защиты информации даже в таких известных и «мощных» сетевых ОС, как Windows NT или NetWare. В сети имеется много физических мест и каналов несанкционированного доступа к информации в сети. Каждое устройство в сети является потенциальным источником электромагнитного излучения из-за того, что соответствующие поля, особенно на высоких частотах, экранированы неидеально. Система заземления вместе с кабельной системой и сетью электропитания может служить каналом доступа к информации в сети, в том числе на участках, находящихся вне зоны контролируемого доступа и потому особенно уязвимых. Кроме электромагнитного излучения, потенциаль-

ную угрозу представляет бесконтактное электромагнитное воздействие на кабельную систему. Безусловно, в случае использования проводных соединений типа коаксиальных кабелей или витых пар, называемых часто медными кабелями, возможно и непосредственное физическое подключение к кабельной системе. Если пароли для входа в сеть стали известны или подобраны, становится возможным несанкционированный вход в сеть с файл-сервера или с одной из рабочих станций. Наконец, возможна утечка информации по каналам, находящимся вне сети:

• хранилище носителей информации;

• элементы строительных конструкций и окна помещений, которые образуют каналы утечки конфиденциальной информации за счет так называемого микрофонного эффекта;

• телефонные, радио-, а также иные проводные и беспроводные каналы (в том числе каналы мобильной связи).

Любые дополнительные соединения с другими сегментами или подключение к Интернету порождают новые проблемы. Атаки на локальную сеть через подключение к Интернету для того, чтобы получить доступ к конфиденциальной информации, в последнее время получили широкое распространение, что связано с недостатками встроенной системы защиты информации в протоколах TCP/IP. *Сетевые атаки* через Интернет могут быть классифицированы следующим образом:

1. Сниффер пакетов (sniffer – в данном случае в значении *фильтрация*) – прикладная программа, которая использует сетевую карту, работающую в режиме promiscuous (не делающий различия) mode (в этом режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки).

2. IP-спуфинг (spoof – обман, мистификация) – происходит, когда хакер, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя.

3. Отказ в обслуживании (Denial of Service – DoS). Атака DoS делает сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

4. Парольные атаки – попытка подбора пароля легального пользователя для входа в сеть.

5. Атаки типа Man-in-the-Middle – непосредственный доступ к пакетам, передаваемым по сети.

6. Атаки на уровне приложений.

7. Сетевая разведка – сбор информации о сети с помощью общедоступных данных и приложений.

8. Злоупотребление доверием внутри сети.

9. Несанкционированный доступ (НСД), который не может считаться отдельным типом атаки, так как большинство сетевых атак проводится ради получения несанкционированного доступа.

10. Вирусы и приложения типа «троянский конь».

Классификация средств защиты информации

Защита информации в сети может быть улучшена за счет использования специальных генераторов шума, маскирующих побочные электромагнитные излучения и наводки, помехоподавляющих сетевых фильтров, устройств зашумления сети питания, скремблеров (шифраторов телефонных переговоров), подавителей работы сотовых телефонов и т. д. Кардинальным решением является переход к соединениям на основе оптоволокна, свободным от влияния электромагнитных полей и позволяющим обнаружить факт несанкционированного подключения.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую – упоминавшиеся выше генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

2. Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Шифрование данных представляет собой разновидность программных средств защиты информации и имеет особое значение на практике как единствен-

ная надежная защита информации, передаваемой по протяженным последовательным линиям, от утечки. Шифрование образует последний, практически непреодолимый «рубеж» защиты от НСД. Понятие «шифрование» часто употребляется в связи с более общим понятием криптографии. **Криптография** включает способы и средства обеспечения конфиденциальности информации (в том числе с помощью шифрования) и аутентификации. **Конфиденциальность** – защищенность информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В свою очередь **аутентификация** представляет собой установление подлинности различных аспектов информационного взаимодействия: сеанса связи, сторон (идентификация), содержания (имитозащита) и источника (установление авторства с помощью цифровой подписи).

3. Смешанные *аппаратно-программные* средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.

4. Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки – высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства.

4.10. Выбор сетевых программных средств

В процессе проектирования сети совершенно невозможно выделить те проблемы, которые должны быть решены в начале, и те, которые можно отложить на потом. Выбор программных средств не стоит считать чем-то второстепенным, совершенно не влияющим ни на размер и структуру сети, ни на характеристики требуемого оборудования. Поэтому принимать решение о том, какие программные средства надо использовать или хотя бы к какому классу они должны принадлежать, необходимо в самом начале проектирования.

При выборе сетевого программного обеспечения (ПО) надо в первую очередь учитывать следующие факторы:

• какую сеть поддерживает сетевое ПО: одноранговую, сеть на основе сервера или оба этих типа;

• максимальное количество пользователей (лучше брать с запасом не менее 20 %);

• количество серверов и возможные их типы;

• совместимость с разными операционными системами и компьютерами, а также с другими сетевыми средствами;

• уровень производительности программных средств в различных режимах работы;

• степень надежности работы, разрешенные режимы доступа и степень защиты данных;

• какие сетевые службы поддерживаются;

• и, возможно, главное – стоимость программного обеспечения, его эксплуатацию и модернизацию.

Наконец, еще до установки сети необходимо решить вопрос об управлении сетью. Даже в случае одноранговой сети лучше выделить для этого отдельного специалиста (администратора), который будет владеть информацией о конфигурации сети и распределении ресурсов и следить за корректным использованием сети всеми пользователями. Если сеть большая, то одного сетевого администратора недостаточно – нужна группа, возглавляемая системным администратором. После установки и запуска сети решать эти вопросы, как правило, слишком поздно.

Только после всего вышеперечисленного можно переходить к установке выбранного программного обеспечения, если таковое требуется. Следует заметить, что в большинстве случаев непосредственно установкой программных средств занимаются работники специализированных компьютерных фирм. Но принимать решение о том, что нужно конкретному предприятию, должны все-таки те, кто будет с этой сетью работать в дальнейшем.

Затем необходимо провести конфигурирование сети, т. е. задать ее логическую конфигурацию, настроить на работу в конкретных условиях. В обязанности системного администратора сети, который осуществляет контроль и управление, входит:

• создание групп пользователей различного назначения;

• определение прав доступа пользователей;

• обучение новых пользователей и оперативная помощь в случае необходимости;

• контроль дискового пространства всех серверов сети;

• защита и резервное копирование данных, борьба с компьютерными вирусами;

• модернизация программного обеспечения и сетевой аппаратуры;

• настройка сети для получения максимальной производительности.

Системный администратор, как правило, получает максимальные права по доступу ко всем сетевым ресурсам и служебным программам. Все остальные пользователи в идеале не должны замечать сети: просто у них появляются новые диски, расположенные на файл-серверах, новые принтеры, сканеры, модемы, программы, специально ориентированные на сеть, например электронная почта.

Создаваемые группы пользователей должны по возможности совпадать с реальными группами сотрудников предприятия, занимающимися одной или несколькими близкими проблемами. Для каждой группы системный администратор может установить свои права доступа к сетевым ресурсам. Гораздо удобнее создать группу с установленными правами, а затем включить в нее нужных пользователей, чем определять права каждого пользователя в отдельности. В этом случае при необходимости изменения прав пользователя достаточно перевести его в другую группу. Желательно, чтобы каждой группой управлял свой сетевой администратор (если, конечно, группы достаточно большие). Например, сетевая ОС Windows Server 2000 позволяет создавать четыре типа групп:

• локальные группы регистрируются на локальном компьютере;

• глобальные группы регистрируются на главном контроллере домена;

• специальные группы (обычно используются для внутрисистемных нужд);

• встроенные группы делятся на три категории: администраторы, операторы и другие пользователи.

Свои права доступа можно установить и каждому пользователю в отдельности. В идеале пользователь должен иметь столько прав доступа, сколько ему действительно нужно. Если прав меньше, чем нужно, это мешает работе пользователя и требует постоянного вмешательства сетевого администратора. Если же прав больше, чем необходимо, то пользователь может вольно или невольно уничтожить или исказить ценную информацию.

Каждая сетевая операционная система или оболочка имеет свой набор разрешенных прав доступа к каталогам и файлам. Это характеризует ее гибкость, надежность, возможность развития сети.

Время от времени рекомендуется делать копии всех дисков сервера. Это позволит в случае аварии восстановить недавнее состояние сети, потеряв не слишком много данных. При этом системный администратор должен сохранить на диске рабочей станции информацию о пользователях и их правах доступа, чтобы при восстановлении сети не пришлось все это задавать заново. Целесообразно иметь две копии дисков серверов. Для контроля работы сети системный администратор

пользуется специальными программными средствами. Современные сетевые ОС, как правило, имеют программы-утилиты, которые позволяют наблюдать в реальном времени за деятельностью процессоров, работой дисков, использованием памяти, а также сети. Анализируя параметры реального обмена в сети, администратор может установить такие режимы, которые обеспечивают наибольшую эффективность обмена. Выявив тенденции развития сети, он может вовремя принять решение о необходимости модернизации программных или аппаратных средств.

В последнее время наблюдается устойчивая тенденция к сокращению количества фирм, производящих сетевые программные средства. Причем даже остающиеся на этом рынке поставщики стараются минимизировать количество своих продуктов. В результате выбор у пользователя не так уж и велик. Выбирать приходится между Novell и Microsoft, причем количество основных, базовых продуктов у обеих компаний невелико (2–3). Все другие фирмы либо вообще прекратили производство новых сетевых продуктов, либо их доля в рынке несравнимо меньше, чем у этих двух гигантов.

Выбирая между продуктами компаний Microsoft и Novell, необходимо иметь в виду, что традиционно преимуществами продуктов Novell (сетевые ОС NetWare) считаются:

- более совершенная архитектура сетевой ОС;
- универсальность и функциональная полнота программных средств.

Прикладное программное обеспечение:

- Microsoft office 2007 – для работы с офисными документами;
- платформа 1с – для постановки бизнес процессов;
- WinRAR – работа с архивами;
- антивирус Касперского – программа защиты от вирусов.

Операционные системы семейства Windows

Являются на сегодняшний день признанными лидерами среди операционных систем персональных компьютеров и компьютерных сетей [13].

Windows 2000 Server [14] обладает полной поддержкой TCP/IP. Этот протокол может рассматриваться как основной протокол операционной системы, а также основа всей службы каталогов Active Directory, являющейся ключевым элементом сетей Windows 2000. На стороне клиентов протокол TCP/IP обеспечивает полную поддержку соединений с другими клиентами и серверами, поддерживающими TCP/IP и Internet.

На стороне сервера Windows 2000 Server обеспечивает поддержку всевозможных инструментов конфигурирования и управления, включая поддержку динамического назначения адресов с помощью службы DHCP, разрешения имен с помощью службы DNS .

В состав Windows 2000 входит новое средство, такое, как совместный доступ к Internet ICS (Internet Connection Sharing), позволяющее использовать одно Интернет-соединение несколькими пользователями локальной сети.

Конфигурирование сайта Active Directory, установка и настройка DHCP-сервера [14, с. 458–476], служб DNS и Wins [14, с. 477–526].

Выпуск семейства ОС Win Server 2003 знаменует очередную ступень в развитии платформы Windows.

В ОС получило дальнейшее развитие модель системы безопасности, использованная в предыдущих версиях Windows, ключевую роль играет локальная служба безопасности LSA (Local Security Authority). Ее основная задача – предоставить доступ в систему только пользователям, имеющим на это право. Локальная служба безопасности тесно связана со службой каталогов Active Directory.

ОС поддерживает механизм создания виртуальной частной сети (Victual Private Network, VPN), позволяющий осуществлять безопасное и надежное взаимодействие со множеством удаленных пользователей.

Процесс работы с Active Directory подробно описан в стр. [14, с. 477–509].

MS Windows Server 2008 [15] – это общее название целого семейства операционных систем, выпускаемых в нескольких редакциях, ориентированных на разные задачи и различные аппаратные платформы.

Windows Server 2008 Web – предназначена для быстрого развертывания специализированных серверов, выполняющих роль веб-сервера.

Windows Server 2008 Standart – базовая система для использования во всех областях. Позволяет устанавливать любые роли, службы и компоненты.

Windows Server 2008 Enterprise – система для развертывания критически важных приложений в корпоративной среде. Обеспечивает максимальную безопасность системы и процессов.

Windows Server 2008 Datacenter – наиболее мощная платформа для развертывания ответственных приложений с высокими возможностями масштабирования нагрузки.

К новым средствам в ОС относится технология виртуализации Hyper-V, позволяющая запускать на компьютере другие операционные системы и прикладные программы, не поддерживаемые в Windows Server 2008. Эта роль сервера может устанавливаться только на процессорах x64, которые, кроме того, имеют аппаратную поддержку визуализации Intel VT или AMD-V.

Материнская плата компьютера должна поддерживать Data Execution Protection (DEP).

Технология защиты доступа к сетям Net-Work Access, Protection (NAP) позволяет предотвратить доступ к внутренней пользовательской сети со стороны небез-

опасного компьютера. Благодаря этому сеть становится менее уязвимой со стороны вирусов и червей.

Администрирование сети описано в разделе «Конфигурирование системы и средства администрирования» [15, с. 156–235].

ЛИТЕРАТУРА

1. Новиков, Ю. В. Аппаратура локальных сетей: функции, выбор, разработка / Ю. В. Новиков, Д. Г. Кариенко. – М. : ЭКОМ, 1998. – 285 с.
2. Компьютерные сети. Принципы, технологии, протоколы : учеб.-метод. пособие для студентов высших учебных заведений / В. Г. Олифер [и др.]; 4-е изд. – СПб. : Питер, 2012. – 943 с.
3. Олифер, В. Г. Сетевые операционные системы : учеб. пособие / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2007. – 538 с.
4. Богуш, В. А. Разработка, проектирование и обеспечение безопасности компьютерных сетей : метод. пособие по курсовому проектированию / В. А. Богуш, И. С. Терех. – Минск : БГУИР, 2007. – 31 с.
5. Поляк-Брагинский, А. В. Локальная сеть. Самое необходимое / А. В. Поляк-Брагинский. – СПб. : Питер, 2009. – 577 с.
6. Колисниченко, Д. Н. Windows 8. Настройка, работа, администрирование / Д. Н. Колисниченко. – СПб. : Питер, 2013. – 189 с.
7. Зозуля, Ю. Н. Windows 7 / Ю. Н. Зозуля. – СПб. : Питер, 2010. – 432 с.
8. Урбанович, П. П. Компьютерные сети: учеб. пособие для студентов вузов / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск : БГТУ, 2011. – 399 с.
9. Новиков, Ю. В. Основы локальных сетей: курс лекций : учеб. пособие для вузов / Ю. В. Новиков. – М. : Интернет-университет информационных технологий, 2005. – 355 с.
10. Закер, К. Компьютерные сети. Модернизация и поиск неисправностей / К. Закер. – СПб. : BHV-Петербург, 2002. – 988 с.
11. Семенов, А. Б. Структурированные кабельные системы / А. Б. Семенов, С. К. Стрижаков, И. Р. Супчелей. – М. : Компания АйТИ, 2004. – 639 с.
12. Аппаратные средства локальных сетей: наиболее полное и подробное руководство / М. Ю. Гук [и др.]. – СПб. : Питер, 2005. – 572 с.
13. Макарова, Н. В. Информатика / Н. В. Макарова, В. Б. Волков. – М. : Питер, 2013. – 574 с.
14. Шарипо, Д. Windows 2000 Server / Д. Шарипо, Д. Бойс. – М. : Вильямс, 2001. – 904 с.
15. Вишневский, А. Windows Server 2003 / А. Вишневский. – СПб. : Питер, 2005. – 767 с.
16. Чекмарев, А. Н. MS Windows Server 2008 / А. Н. Чекмарев. – СПб. : БХВ, 2008. – 872 с.

Св. план 2013, поз. 48

Учебное издание

Лыньков Леонид Михайлович
Ширинский Валерий Павлович

ПРОЕКТИРОВАНИЕ КОМПЬЮТЕРНЫХ СИСТЕМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. И. Герман*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *М. В. Гуртатовская*

Подписано в печать 01.09.2015. Формат 60x84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 3,84. Уч.-изд. л. 3,0. Тираж 100 экз. Заказ 444.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6