А. Н. Сергеев

ОСНОВЫ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

ЛАНЬ

А. Н. СЕРГЕЕВ

ОСНОВЫ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

САНКТ-ПЕТЕРБУРГ
МОСКВА
КРАСНОДАР
2016

ББК 32.973.202я73
С 32

Сергеев А. Н.

С 32 Основы локальных компьютерных сетей: Учебное пособие. — СПб.: Издательство «Лань», 2016. — 184 с.: ил. — (Учебники для вузов. Специальная литература).

ISBN 978-5-8114-2185-5

В учебном пособии рассматриваются теоретические основы и технологии построения локальных компьютерных сетей. Излагаются вопросы базовых понятий, моделей и способов построения компьютерных сетей, организации стека протоколов TCP/IP (IPv4 и IPv6), создания серверов общего доступа и служб для IP-сетей (DNS, электронная почта, веб и др.). Отдельное внимание уделяется вопросам организации локальных сетей на Windows (рабочая группа и домен), физического построения кабельных и беспроводных локальных сетей.

Рекомендовано студентам, изучающим вопросы теории и практики построения компьютерных сетей (дисциплины «Компьютерные сети», «Вычислительные системы, сети и телекоммуникации», «Информационные системы» и др.), а также специалистам сферы информационных технологий, осуществляющим создание и сопровождение компьютерных сетей.

ББК 32.973.202я73

Рецензенты:

И. В. ГЕРМАШЕВ — доктор технических наук, профессор кафедры информатики и информатизации образования Волгоградского государственного социально-педагогического университета;

М. В. ХРАМОВА — кандидат педагогических наук, доцент кафедры информационных систем и технологий в обучении Саратовского национального исследовательского государственного университета им. Н. Г. Чернышевского.

Обложка
Е. А. ВЛАСОВА

Введение

Компьютерные сети прочно вошли в нашу жизнь. Давно миновали времена, когда компьютер понимался исключительно как автономное вычислительное устройство — ЭВМ. Сейчас компьютеры и другие цифровые устройства практически всегда подключаются в сеть, что позволяет обмениваться информацией, получать доступ к цифровым ресурсам, совместно использовать периферийные устройства и др. Компьютерные сети обеспечивают и новый уровень вычислений — за счет распределения нагрузки между многими машинами создаются высокопроизводительные вычислительные сети.

Идея объединения компьютеров в сеть потребовала решения многих задач – разработки принципов совместного использования сетевых ресурсов, сетевых стандартов и протоколов, технологий защиты данных и др. Для практической реализации компьютерных сетей было создано разнообразное аппаратное обеспечение, сетевые операционные системы, а также многочисленные сетевые приложения, используемые как на серверах, так и на рабочих станциях сети.

Данное учебное пособие посвящено основам теории и технологиям построения локальных компьютерных сетей. В отличие от городских и глобальных сетей, которые создаются и администрируются специалистами телекоммуникационных компаний, локальные сети являются базисом информационной инфраструктуры большого числа самых разных организаций, а также часто принадлежат и самим пользователям, пожелавшим объединить свои компьютеры в сеть. В этой связи проблематика локальных компьютерных сетей касается широкого круга специалистов – технического персонала организаций, а также и самих пользователей, от уровня квалификации которых будет зависеть качество построения и эффективность использования локальных сетей. Уверенное владение вопросами построения локальных сетей требует освоения основ и ключевых концепций теории компьютерных сетей, а также наиболее востребованных технологий, применяемых на практике для воплощения различных решений компьютерных сетей.

Основы теории компьютерных сетей, а также вопросы взаимодействия узлов на сетевом уровне рассматриваются *в первых трех разделах* пособия. Здесь излагаются базовые понятия сетевых технологий, раскрывается многообразие видов, моделей и способов построения компьютерных сетей, описывается эталонная модель взаимодействия открытых систем. Отдельное внимание уделяется теоретическим и практическим вопросам организации сетей на основе стека протоколов TCP/IP, так как именно этот стек протоколов является основным для построения локальных, да и глобальных сетей. Рассматриваются принципы организации данного стека протоколов, а также системные службы и технологии, обеспечивающие практическую реализацию сетей на основе IPv4 и IPv6.

Сетевые службы, развертываемые в локальных сетях, рассматриваются *в четвертом и пятом разделах* пособия. Это общесетевые службы, обеспечивающие реализацию системных и прикладных служб в компьютерной сети — DNS, электронная почта, веб, FTP, службы удаленной консоли, а также службы собственно локальных сетей, предназначенные для организации совместной работы компьютеров в рабочей группе или домене Windows.

Физические основы построения локальных сетей раскрываются *в шестом разделе* пособия. Здесь приводится описание технологий и стандартов кабельных сетей Ethernet, беспроводных сетей Wi-Fi, а также виртуальных локальных сетей. Особое внимание в данном разделе уделяется практическим аспектам планирования и физического построения локальных компьютерных сетей.

Надеемся, что данное пособие поможет вам освоить как теорию, так и самые востребованные технологии современных компьютерных сетей. Полученные знания вы сможете с успехом применить при создании локальных сетей и отдельных сетевых сервисов в различных организациях, а также у себя дома, когда вам потребуется объединить несколько компьютеров в сеть. Вы сможете создавать безопасные, удобные и масштабируемые сети, обеспечивающие нужный вам уровень услуг и потенциал для последующего развития. Полученные знания, подкрепленные практикой, позволят вам консультировать пользователей компьютерных сетей, а также обучать информатике по разделам теории и практики сетевых технологий.

Раздел 1. Теоретические основы компьютерных сетей

Для успешного освоения теории компьютерных сетей требуется прежде всего разобраться в базовых понятиях сетевых технологий, многообразии видов и способов построения компьютерных сетей, возможных моделях организации сетевого взаимодействия. Принципиальное значение для правильного понимания всех ключевых вопросов теории компьютерных сетей имеет изучение эталонной модели взаимодействия открытых систем, которая описывает базовые принципы преобразования информации, пересылаемой по сети, а также требования к протоколам взаимодействия сетевых узлов. Изучению данных вопросов посвящен первый раздел учебного пособия.

1.1. Базовые понятия сетевых технологий

Компьютерная сеть — это объединение нескольких компьютеров для совместного решения информационных и вычислительных задач.

Ключевое понятие сетевых технологий — это *сетевой ресурс*, под которым можно понимать аппаратные и программные компоненты, участвующие в процессе совместного использования — в процессе сетевого взаимодействия. Доступ к сетевым ресурсам обеспечивают *сетевые службы* (или, как их еще называют, *сетевые сервисы*).

К базовым понятиям сетевых технологий можно также отнести такие понятия, как сервер, клиент, канал связи, протокол и многие другие. Однако понятия сетевого ресурса и сетевой службы (сервиса) являются основополагающими, так как необходимость организации работы на основе совместного использования компьютерных ресурсов, а значит, создания сетевых ресурсов и соответствующих сетевых служб, является первопричиной создания и самих компьютерных сетей.

Выделяют пять видов сетевых служб: файловая, печати, сообщений, баз данных, приложений.

Файловая служба реализует централизованное хранение и совместное использование файлов. Это одна из важнейших сетевых служб, она предполагает наличие некоторого сетевого хранилища файлов (файловый сервер локальной сети, ftp-сервер или др.), а также использование различных механизмов обеспечения безопасности (разграничение доступа, контроль версий файлов, резервирование информации и др.).

Служба печати обеспечивает возможности централизованного использования принтеров и иных печатающих устройств. Эта служба принимает задания на печать, управляет очередью заданий, организует взаимодействие пользователей с сетевыми принтерами. Технология сетевой печати очень удобна в самых разнообразных компьютерных сетях, так как дает возможность уменьшить количество требуемых принтеров, что в итоге позволяет снизить затраты или использовать более качественное оборудование.

Служба сообщений позволяет организовать информационный обмен между пользователями компьютерной сети. В качестве сообщений в данном случае следует рассматривать как текстовые сообщения (электронная почта, сообщения сетевых мессенджеров, различных средств текстового коллективного общения и др.), так и медиасообщения различных систем голосовой и видеосвязи.

Служба баз данных предназначена для организации централизованного хранения, поиска, обработки и обеспечения защиты данных различных информационных систем. В отличие от простого хранения и совместного использования файлов, служба баз данных обеспечивает и управление, что включает в себя создание, изменение, удаление данных, обеспечение их целостности и защиты.

Служба приложений обеспечивает способ работы, при котором приложение запускается на компьютере пользователя не из локального источника, а из компьютерной сети. Такие приложения могут использовать ресурсы сервера для хранения данных и вычислений. Преимуществом использования сетевых приложений являются возможность их использования из любой точки подключения к компьютерной сети без необходимости установки приложения на локальный компьютер, возможность совместной работы нескольких пользователей, «прозрачное» обновление программного обеспечения, возможность использования коммерческого программного обеспечения на основе подписки.

Службы приложений являются наиболее новым и активно развивающимся видом сетевых служб. Хорошим примером здесь могут служить офисные сетевые приложения онлайн-сервисов Google Drive и Microsoft Office 365.

1.2. Многообразие компьютерных сетей

Компьютерные сети бывают очень разными. В зависимости от тех или иных особенностей построения, сети могут различаться по видам, топологии, физической среде передачи, моделям сетевого взаимодействия и др.

Так, в зависимости от территориального расположения выделяют **виды компьютерных сетей** — глобальные, городские, локальные и персональные сети.

Глобальные сети (*WAN*, *Wide area network*) — это сети, которые охватывают большие географические регионы (города, страны, континенты). Они характеризуются большой протяженностью каналов связи, большим количеством узлов, использованием разнородных сред передачи, сравнительно высокой стоимостью и низкой скоростью передачи данных, наличием достаточно сложных средств для обеспечения работоспособности сети в условиях низкого качества каналов связи. Чаще всего глобальные сети являются объединением компьютерных сетей меньшего масштаба, принадлежащих разным потребителям и поставщикам услуг. Самым ярким представителем глобальных компьютерных сетей является Интернет. Физическую основу соединения узлов глобальной сети составляют, как правило, оптоволоконные и спутниковые каналы связи.

Городские сети (*MAN*, *Metropolitan area network*) объединяют различные узлы в рамках города или региона. В качестве примеров городских сетей можно назвать сети крупных провайдеров, предоставляющие услуги доступа к Интернету, цифровому телевидению и телефонии для самых разнообразных потребителей какого-то города или региона. Если сравнивать с глобальными, то городские сети имеют меньший размер, более высокую скорость и низкую стоимость передачи данных. Как правило, телекоммуникационная инфраструктура городских сетей (кабельная система, соединительное оборудование) принадлежат одному владельцу — поставщику услуг. Такие сети обеспечивают качественный доступ к Интернету и городским цифровым ресурсам, а также соединение территориально разделенных локальных сетей различных организаций. На физическом уровне городские сети основываются, как правило, на оптоволоконных линиях связи и системах беспроводной пакетной передачи данных, таких как 3G, LTE, WiMAX.

Локальные сети (*LAN*, *Local area network*) — обычно понимается, что это сети, которые объединяют компьютеры и различные сетевые устройства в рамках одного здания или группы рядом стоящих зданий. Отличительной особенностью данных сетей является низкая удельная стоимость и высокая

скорость передачи информации. В силу указанных причин в локальных сетях имеется большой запас пропускной способности, что позволяет использовать простые решения планирования сетевого трафика и загрузки узлов. Локальные сети обычно также имеют единую систему управления, а все ее компоненты, такие как компьютеры, сетевое оборудование, кабельные системы, принадлежат одному владельцу (человеку или организации), для обслуживания потребностей которого локальные сети и создаются. Общепризнанным стандартом построения локальных сетей являются технологии Ethernet (локальные сети на основе витой пары и оптоволокна) и Wi-Fi (беспроводная передача).

В некоторых случаях перечень видов локальных сетей дополняют еще одним видом — *кампусные сети* (*CAN*, *Campus Area Network*). Кампусные сети — это сети, которые объединяют группы локальных сетей близко расположенных зданий (например, отдельных корпусов студенческого городка). Как правило, кампусные сети основываются на технологиях локальных сетей и так же, как и локальные сети, принадлежат одному владельцу. В этой связи кампусные сети могут в отдельный вид и не выделяться, а просто рассматриваться частным случаем локальных сетей.

Персональные сети (*PAN*,*Personal area network*) — это сети, которые объединяют персональные электронные устройства пользователя, такие как ноутбуки, смартфоны, телефоны, звуковые гарнитуры и др. Отличительной особенностью таких сетей является небольшой радиус действия, низкая скорость передачи, малое количество узлов, простота подключения и настройки устройств. Персональные сети, как правило, создаются на основе беспроводных технологий. Самым популярным стандартом персональных сетей стал стандарт Bluetooth.

В различных источниках можно также встретить еще один термин — *корпоративная сеть*. Однако корпоративные сети не стоит рассматривать на одном уровне с глобальными, городскими, локальными и персональными, так как эта характеристика относится не к территориальному расположению компьютерной сети, а к особенностям ее организации.

Корпоративная сеть — это сеть некоторой организации, которая создается для обеспечения работы корпоративных информационных систем. Корпоративные сети обычно имеют строгую систему администрирования, правила доступа к сети, использования

корпоративных информационных ресурсов. При этом технологически корпоративная сеть может включать в себя множество территориально обособленных локальных сетей, объединенных между собой при помощи городской или глобальной сети.

Сетевая топология — это способ соединения компьютеров в сеть. Выделяют три базовых сетевых топологии: шина, кольцо, звезда.

Шина — это топология, согласно которой все компьютеры подсоединяются к некоторому общему кабелю (шине, магистрали) (рис. 1.2.1). Шина является одной из старейших топологий, достоинства которой заключаются в простоте и невысокой стоимости сети, а недостатки — в наличии проблем совместного доступа к единой разделяемой среде и низкой надежности.

Рис. 1.2.1. Топология «шина»

Кольцо — это топология, при которой каждый компьютер соединен с двумя другими: от одного он только получает информацию, а другому только передает (рис. 1.2.2). Достоинствами кольцевой топологии являются простота и невысокая стоимость, отсутствие проблем доступа к разделяемой среде, а основным недостатком — невысокая надежность (поломка любого компьютера приводит к выходу из строя всей сети).

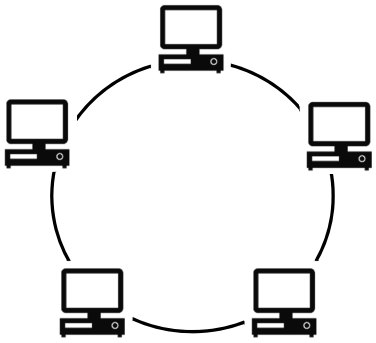


Рис. 1.2.2. Топология «кольцо»

Модификацией топологии «кольцо» является топология «двойное кольцо» (рис. 1.2.3), которая предполагает наличие двух линий связи — основной и резервной. В случае выхода из строя любого узла компьютерной сети или любого кабельного сегмента основная линия связи объединяется с резервной, в результате чего сеть продолжает функционировать.

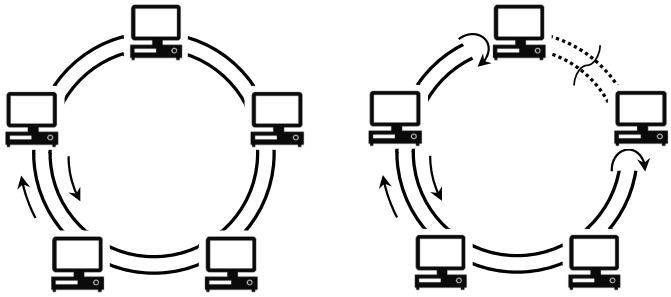


Рис. 1.2.3. Топология «двойное кольцо» в нормальном режиме работы, а также при повреждении кабельного сегмента между парой компьютеров

Заметим, что сети на основе двойного кольца оказываются более надежными, чем сети, построенные в соответствии с топологией «звезда». Сети с топологией «звезда» также отличаются высокой надежностью, но поломка центрального узла (концентратора, коммутатора или др.) все же может привести к выходу из строя всей сети.

Топология «звезда», в отличие от предыдущих, предполагает наличие дополнительного связывающего устройства (концентратора, коммутатора или др.), к которому присоединены все компьютеры (рис. 1.2.4).

Сети на основе «звездной» топологии отличаются высокой отказоустойчивостью и производительностью. Благодаря возможности централизованного управления можно обеспечить разграничение доступа и высокий уровень безопасности. Эти сети легко расширяются за счет независимости подключения пользовательских устройств и возможности соединения нескольких связывающих устройств.

В качестве недостатков можно указать более высокую стоимость (приобретение дополнительного оборудования, высокий расход кабеля), а также уязвимость сети в части выхода из строя связывающего устройства.

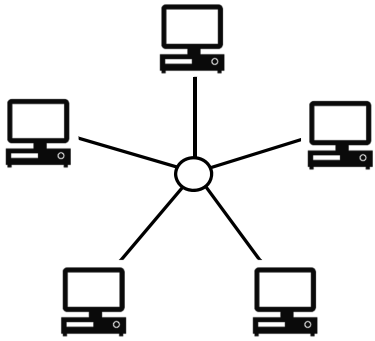


Рис. 1.2.4. Топология «звезда»

Как сказано выше, существует возможность соединения нескольких связывающих устройств, а значит, и компьютерных сетей, имеющих «звездную» топологию. Если при таком соединении не образуется кольцо, то получается топология, которая называется *«дерево»*.

Как правило, современные локальные сети, построенные более чем на одном коммутаторе, имеют древовидную топологию. В редких случаях такие сети могут включать в себя старые сегменты сетей, имеющих топологию «шина», либо фрагменты, где используются специальные решения для резервирования линий связи. В этом случае получается сеть *гибридной* (*смешанной*) *топологии* (рис. 1.2.5).

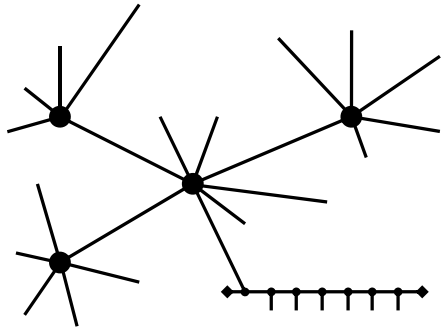


Рис. 1.2.5. Пример структуры сети гибридной (смешанной) топологии

Существует также *полносвязная топология*, которая предполагает, что каждый узел компьютерной сети подключен ко всем остальным. Достоинствами такой сети являются высокая надежность, скорость и безопасность передачи данных между узлами, а недостатком — высокая сложность реализации, которая экспоненциально увеличивается с ростом количества узлов.

По **физической среде передачи** компьютерные сети можно разделить на кабельные и беспроводные.

Кабельные сети, как следует из названия, используют в качестве среды передачи кабель, соединяющий в соответствии с выбранной топологией компьютеры и другие узлы компьютерной сети. Как правило, используется кабель с медными жилами для передачи электрических сигналов или кабель на основе оптоволокна.

В зависимости от вида и поколения сети, протяженности линий связи, места прокладки и др. могут выбираться кабели достаточно разнообразных характеристик. Как правило, в локальных сетях используется кабель «витая пара». Если этим кабелем надо соединить сети соседних зданий, то его следует использовать в экранированном варианте. При построении протяженных локальных сетей, в городских, а также в глобальных сетях будет использоваться оптоволоконный кабель, который обеспечивает высокое качество и скорость передачи данных на большие расстояния, а также слабо подвержен влиянию извне.

Следует также отметить, что компьютерные сети могут создаваться и на основе телефонной инфраструктуры, использовать ту же кабельную систему, что и стационарная телефонная связь. В настоящее время такое решение не обеспечивает существующих потребностей скорости и качества передачи информации, однако во времена становления глобальных сетей именно телефонная инфраструктура позволила быстро создать сети, объединяющие города, страны и континенты, а также обеспечить подключение к этим сетям конечных пользователей.

Беспроводные сети используют в качестве среды передачи радиоэфир либо другие решения, не требующие использования кабельной проводки. Беспроводные технологии используются для всех видов компьютерных сетей. Так, в глобальных сетях используется спутниковая передача, на городском уровне — беспроводные сети сотовых операторов (3G, LTE, WiMAX и др.), в локальных сетях широко применяется технология Wi-Fi, а в персональных — Bluetooth.

Надо учитывать, что радиоэфир — это не единственная возможность построения беспроводных сетей. Свое применение нашли сети и на основе инфракрасного излучения. Это различные решения, позволяющие соединить фрагменты локальных сетей рядом стоящих зданий (там, где в силу тех или иных причин невозможно использовать кабель или радиоэфир), а также технология соединения мобильных устройств пользователя через инфракрасный порт.

По **моделям сетевого взаимодействия** можно выделить сети, которые построены в соответствии с моделью: централизованной обработки информации, «клиент — сервер», распределенной обработки информации, совместной обработки информации, «клиент — сеть».

В сетях, построенных в соответствии с моделью *централизованной обработки информации*, предполагается наличие некоторого центрального компьютера, все ресурсы которого (устройства, приложения, данные) предлагаются для совместного использования пользователями компьютерной сети (рис. 1.2.6). Такой центральный компьютер часто называется *мейнфреймом* (mainframe) или *хостом* (host), а пользователи сети подключаются к этому компьютеру при помощи локальных устройств — *терминалов*. Терминал обычно включает в себя коммуникационное оборудование, устройства ввода и вывода информации.

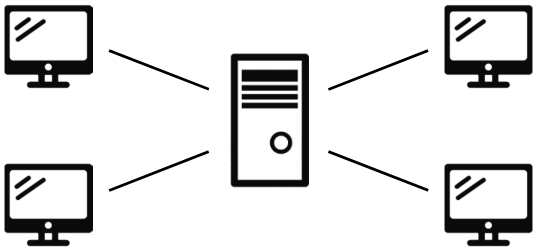


Рис. 1.2.6. Модель централизованной обработки информации

Учитывая простоту исполнения терминала, данные устройства также часто называются *тонкими клиентами* (thin client). Терминал (тонкий клиент) не обязан иметь процессор, запоминающее устройство и другие компоненты, присущие полноценному компьютеру. Отсутствие или максимальное упрощение таких компонент приводит к снижению стоимости и упрощению обслуживания пользовательского оборудования, что в настоящее время часто служит причиной создания сетей на основе модели централизованной обработки информации.

Строго говоря, компьютерные сети на основе централизованной обработки информации нельзя считать полноценными сетями, так как терминалы не позволяют обрабатывать информацию, их использование лишь обеспечивает доступ пользователя к ресурсам центрального компьютера. Такую сеть фактически можно понимать как многопользовательский

компьютер, который позволяет осуществлять одновременную работу нескольких пользователей с разных рабочих мест. Вместе с тем подобная организация работы позволяет решать многие задачи совместного использования информационных ресурсов, которые возлагаются на технологии компьютерных сетей.

Терминальный доступ (модель «терминал — хост») исторически являлся первым способом организации сетевой работы. В настоящее время эта технология используется, как правило, для удаленного администрирования компьютеров (удаленный доступ к консоли, доступ к удаленному рабочему столу), для работы с удаленными приложениями, а также для создания информационных систем, где критичным параметром является низкая стоимость, простота обслуживания и высокая надежность клиентских устройств (системы массового обслуживания и др.).

Модель «клиент — сервер», в отличие от предыдущей модели сетевого взаимодействия, уже предполагает обработку информации на клиентском устройстве (рис. 1.2.7). Общую структуру модели сетевого взаимодействия «клиент — сервер» можно представить так:

1) в сети есть клиентские компьютеры (рабочие станции пользователей) и как минимум один компьютер, который выполняет роль сервера (сервер — это компьютер, который часть своих ресурсов предоставляет в общий доступ);

2) при выполнении своих задач клиенты обращаются к серверу для получения информации (обращаются к файлам, базам данных, различным приложениям для выполнения вычислений и др.);

3) сервер предоставляет необходимую информацию клиенту, где после получения этой информации проводится дальнейшая ее обработка в соответствии с решаемой задачей.

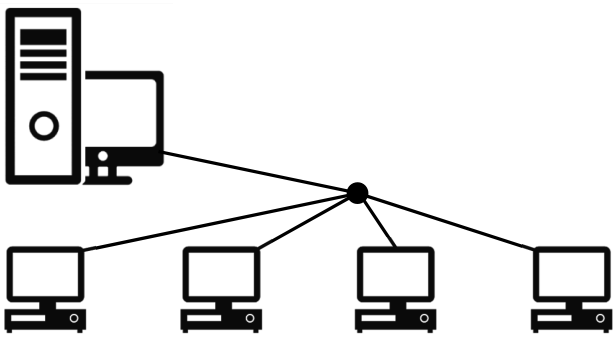


Рис. 1.2.7. Модель «клиент — сервер»

Говоря о *модели сетевого взаимодействия «клиент — сервер»*, следует понимать, что существует также такое понятие, как *архитектура сетевых приложений «клиент — сервер»*, что вносит определенную путаницу в терминологию.

Понятие архитектуры «клиент — сервер» связано с разделением сетевого приложения на две части — серверную и клиентскую. Клиентская часть приложения обращается с запросом к серверной части, на сервере производятся вычисления (поиск необходимой информации в базе данных или др.), полученные результаты отправляются клиентской части, где осуществляется дальнейшая обработка.

Клиент-серверная архитектура противопоставляется файл-серверной архитектуре сетевых приложений, предполагающей, что на сервере осуществляется лишь хранение данных сетевого приложения, но не их обработка. Однако если говорить о клиент-сервере как модели сетевого взаимодействия, то файл-серверная архитектура сетевых приложений тоже относится к модели «клиент — сервер».

Заметим также, что в качестве сервера может выступать как отдельный компьютер (выделенный сервер), так и рабочая станция пользователя, часть ресурсов которой предоставляется в общий доступ. Во втором случае говорят о взаимодействии «равный с равным» (peer-to-peer), а компьютерные сети, где реализована лишь эта модель, называют одноранговыми.

Кроме этого, в ряде случаев сервер тоже может выступать в роли клиента, запрашивая некоторые ресурсы у другого сервера. Такой способ взаимодействия позволяет реализовать многоуровневую архитектуру сетевых приложений.

Весьма часто в компьютерных сетях одновременно реализуются все указанные выше модели – имеется выделенный сервер (сетевое хранилище данных), рабочие станции, которые часть своих ресурсов предоставляют в общий доступ, а также рабочие станции, которые могут выступать лишь в роли клиента компьютерной сети.

Модель распределенной обработки информации (distributed computing) является развитием модели «клиент — сервер» и предполагает, что в компьютерной сети имеется несколько серверов, каждый из которых оптимизирован для решения «своей» задачи — хранение информации, управление базой данных, осуществление вычислений, организация доступа в Интернет и др. (рис. 1.2.8). Подобная модель позволяет решать задачи,

требующие большого объема вычислительных ресурсов, а также обеспечивает более гибкий подход к планированию, разработке и администрированию компьютерной сети за счет возможной «специализации» отдельных серверов, что в итоге позволяет создавать надежные и высокопроизводительные сети. Модель распределенной обработки информации широко используется в компьютерных сетях, обеспечивающих функционирование различных корпоративных информационных систем.

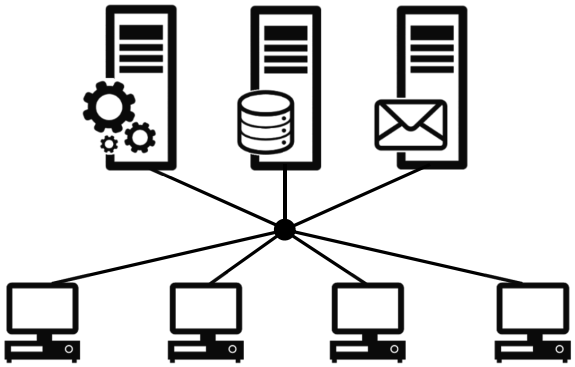


Рис. 1.2.8. Модель распределенной обработки информации

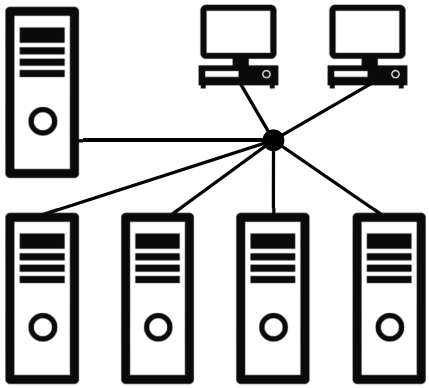


Рис. 1.2.9. Модель совместной обработки информации

Еще одна модель, предполагающая использование многих серверов, называется *моделью совместной обработки информации* (collaborative computing, cooperative processing) (рис. 1.2.9). В этой модели, однако, в отличие от предыдущей, предполагается, что отдельные серверы используются для решения одинаковых задач — общая задача компьютерной

сети «распределяется» по отдельным серверам, что улучшает производительность и повышает отказоустойчивость (т.к. выход из строя любого из серверов не приводит к отказу всей компьютерной сети, а лишь незначительно снижает производительность), а также позволяет гибко управлять имеющимися мощностями, добавляя или убирая необходимое количество серверов.

Классическим примером вычислительных систем, построенных на основе модели совместной обработки информации, является *кластер* и *грид*. Кластер — это группа компьютеров, объединённых высокоскоростными каналами связи, представляющая с точки зрения пользователя единый унифицированный компьютерный ресурс. Как правило, кластеры создаются организациями для получения вычислительных систем высокой производительности (сравнимой с производительность суперкомпьютеров).

Грид-система, в отличие от кластера, снимает требование скоростной связи серверов. Как и кластер, грид-система состоит из множества серверов, однако они не обязаны объединяться между собой высокоскоростными каналами связи. Это, в свою очередь, означает, что отдельные узлы грид-системы могут располагаться на значительном удалении друг от друга, принадлежать различным владельцам. Узлы грид-системы получают задание на вычисления от центрального узла, затем этому же узлу отправляют и полученные результаты (предполагается, что вычисления проводятся без обмена информацией с другими узлами).

Такая особенность грид-систем позволяет организовать вычисления на основе добровольного участия простых пользователей Интернета, пожелавших принять участие в некотором проекте грид-вычислений (добровольный грид).

Пользователи (участники добровольного грида) устанавливают на свой компьютер специальное программное обеспечение, позволяющее выполнять вычисления в тот момент, когда компьютер простаивает.

Как правило, проекты добровольных грид-вычислений нацелены на решение ресурсоемких научных задач: выполнение трудоемких математических вычислений, анализ физических экспериментов, разработка и изучение свойств новых лекарственных препаратов, прогнозирование стихийных бедствий и даже поиск внеземных цивилизаций.

Еще одна модель сетевых взаимодействий, получившая широкое распространение в современных компьютерных сетях, называется *моделью «клиент — сеть»* (client — network) (рис. 1.2.10). Эта модель лежит в основе

идеи *облачных вычислений*, на основе которой реализованы очень многие сервисы Интернета, позволяющие пользователям вести разработку и публикацию собственной информации.

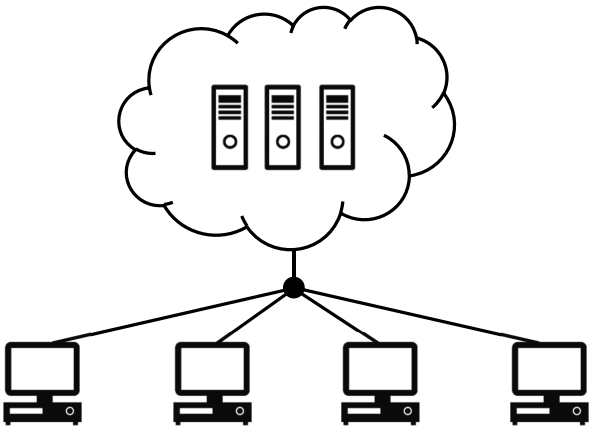


Рис. 1.2.10. Модель «клиент — сеть»

Модель «клиент-сеть» предполагает, что пользователи получают доступ к определенным сервисам, а не к конкретным серверам. Специальные службы сети определяют, на каком именно сервере будет выполняться запрос пользователя. При этом пользователю безразлично, где именно хранятся данные и осуществляются вычисления — важно, что пользователь может обратиться к нужному сервису и получить услугу.

Модель «клиент — сеть» значительно упрощает работу как пользователя, так и владельца сетевого сервиса. Пользователям не требуется знать излишних технических подробностей для доступа к сетевым ресурсам (например, точных имен серверов, новых адресов, которые могли измениться вследствие расширения сети и др.). Владельцы могут произвольно изменять структуру своих сетевых сервисов, наращивать производительность, менять оборудование и др., не останавливая предоставление услуги и не опасаясь потерять своих пользователей вследствие изменения каких-либо технических характеристик.

Важной особенностью облачных вычислений являются возможности предоставления сетевого ресурса пользователю в том объеме, который ему необходим, а также расширения (или уменьшения) объема ресурсов по запросу. Это позволяет пользователям снижать затраты на инфраструктуру, а также расширять объем доступных ресурсов без больших изменений сетевой инфраструктуры и затрат.

1.3. Эталонная модель взаимодействия открытых систем

Как показано выше, существует большое разнообразие в подходах к построению компьютерных сетей. Компьютерные сети бывают разного размера, используют разные среды передачи данных, основываются на различных моделях сетевого взаимодействия и др. Кроме этого, разными являются и узлы компьютерных сетей — от обычных компьютеров и мобильных пользовательских устройств до сложных кластерных и облачных систем. В этой связи возникает проблема согласования принципов и способов передачи данных, проблема стандартизации обмена информацией между разнообразными устройствами в разнообразных сетях.

В основе всех стандартов компьютерных сетей лежит *эталонная модель взаимодействия открытых систем*, называемая также *моделью OSI* (Open systems interconnection basic reference model). Модель разработана международной организацией по стандартизации (ISO, International Organization for Standardization), в результате чего полное название модели записывается как *модель ISO/OSI*.

Модель OSI является уровневой моделью. Она описывает:

- уровни архитектуры компьютерной сети;
- вертикальные связи разных уровней одной системы;
- горизонтальные связи одинаковых уровней разных систем.

Всего выделяются 7 уровней модели OSI: прикладной, представления, сеансовый, транспортный, сетевой, канальный и физический (рис. 1.3.1). Вертикальные связи модели OSI описывают услуги, которые оказывают соседние уровни на одной машине. Горизонтальные связи определяют *протоколы* взаимодействия — правила и процедуры, регулирующие порядок взаимодействия компьютеров в сети.

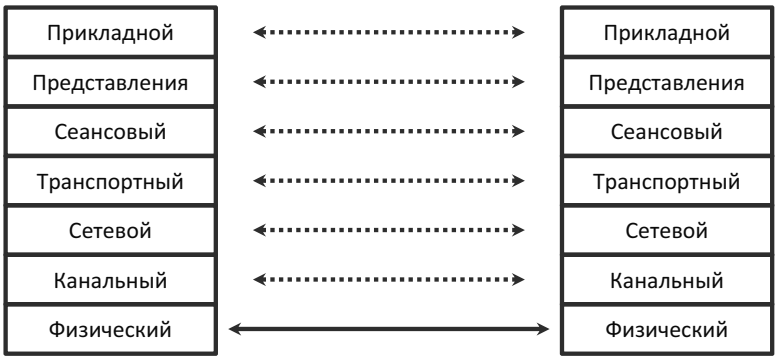


Рис. 1.3.1. Уровни и связи модели OSI

Кратко рассмотрим назначение и особенности реализации каждого из уровней.

Физический уровень (physical layer). На этом уровне определяются методы передачи *битов* данных по физическим каналам, такие характеристики сетевых компонентов, как вид среды передачи (кабель, радиоэфир), типы физических сетевых интерфейсов (соединительные разъемы), топологии сети, способы частотного или временного разделения каналов связи и др.

Физический уровень реализован аппаратно в сетевых устройствах. К техническим средствам исключительно физического уровня можно отнести кабели, разъемы, коммутационные панели, повторители сигналов (репитер, repeater), концентраторы (хаб, hub), медиаконверторы.

Канальный уровень (data link layer). На этом уровне реализуется доставка *кадров* (фреймов) данных в сетях базовой топологии, для чего осуществляется проверка доступности среды передачи, подготовка кадра, контроль (возможно – и исправление) ошибок передачи.

Для правильного понимания особенностей канального уровня следует учитывать, что на этом уровне:

1) передача данных осуществляется кадрами (фреймами) — фрагментами данных, включающими в себя информационные биты и адресную информацию, а также, в зависимости от протокола, информацию для проверки целостности кадра, метку сетевого протокола и др.;

2) доставка кадров данных осуществляется только в сетях базовой топологии (в пределах одного сегмента сети), т.е. в случаях, когда такая доставка может быть осуществлена напрямую, без использования промежуточных узлов;

3) возникает понятие *физического* (*аппаратного*) *адреса — MAC-адреса*, используемого для целевой доставки передаваемых кадров.

Канальный уровень реализован в программном обеспечении сетевых устройств (сетевые адаптеры, коммутаторы, модемы и др.), в том числе при помощи драйвера сетевого адаптера для операционных систем.

Сетевой уровень (network layer). Главной задачей этого уровня является доставка *пакетов* данных в сетях произвольной топологии — в тех сетях, где для доставки необходимо использовать промежуточные узлы. Для решения этой задачи на сетевом уровне вводится своя система адресации (*сетевой адрес*), а также реализуется механизм *маршрутизации* — определения пути передачи данных в компьютерной сети.

Необходимость ввода новой системы адресов определяется тем, что сетевые адреса, обеспечивающие маршрутизацию, должны быть составными.

Они включают в себя логический адрес сети, а также адрес сетевого устройства. В этом случае, если первые части адресов отправителя и получателя совпадают (т.е. совпадают логические адреса их сетей), то считается, что отправитель и получатель находятся в одном сегменте сети, передача пакета данных осуществляется напрямую. В случае когда отправитель и получатель оказываются в разных сетях, то пакет данных передается на промежуточный узел – *шлюз*, откуда он следует получателю или следующему промежуточному узлу.

Правила пересылки пакетов данных определяются на основе таблиц маршрутизации, которые хранятся на всех узлах сети либо формируются автоматически на основе некоторого *протокола динамической маршрутизации*.

Сетевой уровень реализуется через установку и настройку в компьютерной сети соответствующих протоколов (IP, IPv6 или др.). К аппаратным устройствам, работающим на сетевом уровне, следует отнести *маршрутизатор* (роутер, router).

Транспортный уровень (transport layer). Этот уровень обеспечивает подготовку и обратную сборку пакетов данных, а также выполнение процедур для обеспечения необходимого уровня надежности передачи информации. Транспортный уровень позволяет скрыть физическую и логическую структуры сети для верхних уровней, предоставляя стандартный механизм передачи *потоков* данных.

Говоря о надежности передачи информации, следует понимать, что в разных случаях требования к этой надежности могут различаться и это учитывается в различных протоколах транспортного уровня. Так, в широко применяющемся протоколе TCP надежность передачи данных обеспечивается посредством механизма проверки целостности пакетов с уведомлением отправителя о результатах передачи. Протокол UDP, который также часто используется в компьютерных сетях, использует более простую модель передачи без обеспечения надежности. Такая особенность протокола UDP позволяет организовать передачу данных с минимальными затратами, что может оказаться более предпочтительным для некоторых сервисов, осуществляющих регулярные рассылки небольших запросов.

Сеансовый уровень (session layer). Согласно модели OSI, на этом уровне организуются сеансы связи между оконечными машинами, позволяя взаимодействовать длительное время. Уровень управляет созданием и завершением сеанса, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений.

Следует отметить, что в практической реализации многих современных сетей (сетей на основе TCP/IP) протоколы сеансового уровня в явном виде не выделяются, задачи сеансового уровня отнесены к транспортному и прикладному уровням.

Уровень представления (presentation layer). Основная задача этого уровня, согласно модели OSI, заключается в преобразовании передаваемых данных во взаимно согласованные форматы, шифровании, компрессии и декомпрессии данных. Однако заметим, что, как и в предыдущем случае, задачи уровня представления во многих практических реализациях компьютерных сетей отнесены на другие уровни (прежде всего прикладной).

Хорошим примером востребованности уровня представления является задача построения сети, которая связывает компьютеры, использующие разные способы кодирования данных. Чтобы один компьютер «понимал» другой, необходима перекодировка данных в процессе пересылки. Универсальным решением здесь может стать преобразование данных на уровне представления к какому-то общему формату, принятому для пересылки через компьютерную сеть.

Прикладной уровень (application layer). Этот уровень обеспечивает связь прикладных программ, а также доступ к разделяемым ресурсам. Фактически это уровень связи прикладных приложений, его работа обеспечивается сетевыми протоколами, специфичными для конкретных сетевых служб.

К протоколам прикладного уровня можно отнести HTTP, FTP, SMTP, POP, IMAP, Telnet, SSH и многие другие, обеспечивающие сетевое взаимодействие различных сетевых сервисов и пользовательских программ.

Учитывая, что на одном и том же физическом компьютере может функционировать несколько сетевых служб, возникает необходимость их внутренней адресации. В сетях на основе TCP/IP таким внутренним адресом сетевой службы является *порт TCP* (*UDP*). Порт — это некоторое число в диапазоне от 1 до 65535, которое сопоставляется с конкретным протоколом прикладного уровня (а значит, с соответствующей службой) либо с программой клиента, при помощи которой осуществляется доступ к сети.

Например, за протоколом HTTP закреплен порт номер 80, а за SMTP – 25. В этом случае, если пользователь обращается к серверу через браузер с указанием протокола http (http://...), то обращение по указанному адресу поступает на 80-й порт. Почтовая программа,

обратившаяся к этому же серверу, отправит свой запрос на порт 25. При этом самой программе (вкладке браузера), через которую был отправлен запрос, будет присвоено случайное и еще не занятое значение порта (в диапазоне от 1024 до 65535), а почтовая программа, в свою очередь, будет использовать другой незанятый порт. Ответ, который генерирует сервер, будет отправлен на адрес клиента с указанием номера порта, с которого отправлялся запрос. В результате пользователь получит ответ веб-сервера в ту вкладку браузера, с которой он в данный момент работает, или увидит ответ почтового сервера в своей почтовой программе.

В таблице 1.3.1 приведены примеры сетевых протоколов в соответствии с уровнями модели OSI

Таблица 1.3.1

<table>
<tr><th>Уровни OSI</th><th colspan="2">Протоколы</th></tr>
<tr><td>Прикладной</td><td colspan="2" rowspan="3">HTTP, SMTP, POP3, IMAP4, Telnet, FTP, SMB, NTP, SSL</td></tr>
<tr><td>Представления</td></tr>
<tr><td>Сеансовый</td></tr>
<tr><td>Транспортный</td><td colspan="2">TCP, UDP, SPX, GRE</td></tr>
<tr><td>Сетевой</td><td colspan="2">IP, ICMP, IPX</td></tr>
<tr><td>Канальный</td><td>PPP, PPPoE</td><td rowspan="2">Ethernet, Wi-Fi, Bluetooth , Wi-Max</td></tr>
<tr><td>Физический</td><td>100BASE-T, DSL, V.90</td></tr>
</table>

Вопросы и задания

Назовите понятия, относящиеся к сетевым технологиям. Какое из этих понятий является ключевым?

Опишите пять видов сетевых служб.

Приведите характеристики глобальных, локальных и иных сетей, выделяемых в зависимости от территориального расположения сетевых узлов.

Какие сетевые топологии вам известны? В чем их преимущества и недостатки?

Опишите возможные варианты создания кабельных и беспроводных компьютерных сетей.

Назовите модели сетевого взаимодействия. Опишите характеристики моделей, принципиально отличающие каждую из них от других моделей.

Опишите общую структуру модели взаимодействия открытых систем (OSI). Для чего предназначена эта модель?

Какие уровни взаимодействия описываются в модели OSI? Каково предназначение каждого из уровней? Опишите их основные характеристики.

Что такое сетевой протокол? Приведите примеры протоколов, относящихся к разным уровням модели OSI.

Раздел 2. Стек протоколов TCP/IP

Стек протоколов TCP/IP — набор протоколов передачи данных, используемых в большинстве современных компьютерных сетей. Название TCP/IP происходит из двух протоколов семейства — Transmission Control Protocol (TCP) и Internet Protocol (IP), которые были разработаны и описаны первыми в данном стандарте. В целом же стек протоколов TCP/IP включает в себя четыре уровня: прикладной, транспортный, сетевой и канальный. Протоколы этих уровней полностью реализуют функциональные возможности модели OSI вне зависимости от среды физической передачи.

2.1. Протокол IP

Протокол IP является одним из самых важных в стеке протоколов TCP/IP. Этот протокол относится к сетевому уровню и объединяет сегменты сети в единую сеть, обеспечивая доставку пакетов данных между любыми узлами сети, связанными непосредственно или через какое-то количество промежуточных узлов.

Название протокола IP расшифровывается как Internet Protocol, что не случайно. В этом названии заложен смысл протокола — обеспечение межсетевого взаимодействия. Этот протокол послужил основой создания Всемирной компьютерной сети, которая также стала называться Интернет.

Получается, что история протокола IP тесно связна с историей Интернета и именно глобальная сеть получила свое название благодаря основному ее протоколу, а не наоборот.

Наиболее популярная 4-я версия протокола IP была разработана в 1981 году и принята в качестве основного стандарта с 1 января 1983 года. Эта версия до сих пор используется на подавляющем большинстве компьютеров, поэтому преимущественно в данном пособии мы будем рассматривать именно ее. Вместе с тем 4-я версия уже не обеспечивает должного развития Интернета, в связи с чем разработана и внедряется 6-я версия протокола — IPv6. Особенности новой версии мы рассмотрим отдельно.

Одним из ключевых вопросов построения протокола IP является вопрос сетевой адресации. IP-адрес — это 32-битное число, которое принято записывать при помощи четырех октетов, разделенных точками. Например:

192.168.0.1

Каждое число (октет) в структуре IP-адреса занимает 1 байт и может лежать в диапазоне от 0 до 255 (с оговоркой, что в последней позиции 0 означает адрес сети, а 255 — широковещательный адрес).

Такой адрес состоит из двух частей — адреса сети и адреса компьютера в данной сети. Такое разделение, как было описано выше, необходимо для маршрутизации пересылаемых пакетов.

Как происходит разделение адреса на части? Существуют два способа, первый из которых основан на понятии класса сети (классовая адресация), а второй — на понятии сетевой маски.

Классовая адресация — это исторически первый способ разделения адреса на составные части. Основная идея данного способа заключается в анализе первых нескольких бит адреса для того, чтобы определить «линию разграничения» — первую часть адреса, относящуюся к сети, и вторую часть адреса, относящуюся непосредственно к узлу (табл. 2.1.1).

Таблица 2.1.1

Класс	**Диапазон значений первого октета**	**Характеристики адреса**
A	0–127	Разделение по первой точке Пример: 10.0.15.1 • адрес сети — 10 • адрес компьютера — 0.15.1
B	128–191	Разделение по второй точке Пример: 172.16.31.2 • адрес сети — 172.16 • адрес компьютера — 31.2
C	192–223	Разделение по третьей точке Пример: 191.168.0.1 • адрес сети — 192.168.0 • адрес компьютера — 1

Как видно из таблицы, сети класса A – это очень большие сети, они могут включать в свой состав до 16 777 216 компьютеров (это число соответствует 2^{24} — именно 24 разряда отдается на адресацию узлов), но таких сетей в мире может быть лишь 128.

Сети класса B имеют меньший размер — до 65 536 компьютеров, при этом таких сетей может быть значительно больше. Еще больше — сетей класса C, эти сети имеют самый малый размер — до 255 компьютеров.

Выделяют также сети классов D и E. Первый октет адреса в сетях класса D лежит в диапазоне от 244 до 239. Это адреса многоадресной рассылки (групповые адреса). Сети класса E (от 240 до 255) относятся к зарезервированному диапазону.

В настоящее время способ классовой адресации не используется, так как не позволяет экономно использовать имеющиеся диапазоны IP-адресов. Например, для сети из 500 компьютеров приходится выбирать сети класса B и мириться с тем, что лишь 500 адресов в такой сети будет задействовано, а более 65 тысяч — использоваться впустую. Указанного недостатка лишен второй способ разделения IP-адреса — на основе сетевой маски.

Адресация на основе сетевой маски (бесклассовая адресация). Основная идея этого способа заключается в том, что дополнительно к IP-адресу компьютеру сообщается и его сетевая маска (32-битное число), на основе которой можно гибко разделить исходный адрес на составные части.

При этом полностью понять смысл разделения адреса на основе маски можно, лишь оперируя адресами в двоичном виде (то есть так, как это делает компьютер). Поясним процедуру разделения на примерах.

Пример 1:
IP-адрес — 192.168.0.1
Сетевая маска — 255.255.255.0
Запишем адрес и маску в двоичном виде (табл. 2.1.2).

Таблица 2.1.2

Октеты адреса	192								168								0								1							
Биты адреса	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
Октеты маски	255								255								255								0							

Из таблицы видно, что в строке «Биты маски» сначала идут 24 единицы, а потом — 8 нулей. Это означает, что адрес делится в позиции третьей точки: 192.168.0 — это адрес сети, а 1 — это адрес компьютера в данной сети (что, собственно, соответствует и классовой адресации — адрес 192.168.0.1 относится к сетям класса С).

Пример 2:
IP-адрес — 192.168.0.1
Сетевая маска — 255.255.0.0
Двоичное представление адреса и маски представлено в таблице 2.1.3.

Таблица 2.1.3

Октеты адреса	192								168								0								1							
Биты адреса	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Октеты маски	255								255								0								0							

Как видим, битовая маска показывает, что разделение адреса необходимо провести по второй точке. В этом случае адрес сети будет иметь вид 192.168, а адрес компьютера — 0.1.

Заметим, что, несмотря на принадлежность исходного адреса к сетям класса С, мы смогли создать сеть, которая включает в свой состав 65 536 компьютеров. Классовая адресация при использовании сетевой маски не учитывается.

Возможно ли указывать в маске другие числа, отличные от 0 и 255? Да, но надо учитывать правило — в двоичной последовательности сетевой маски сначала должно идти какое-то количество единиц, а затем — все остальные нули. Чередовать 1 и 0 не допускается.

Указанное выше правило, в свою очередь, означает, что в сетевой маске помимо 0 и 255 могут встречаться числа 128, 192, 224, 240, 248, 252 и 254.

Пример 3:
IP-адрес — 192.168.0.1
Сетевая маска — 255.255.255.240
Запишем адрес и маску в двоичном виде (табл. 2.1.4).

Таблица 2.1.4

Октеты адреса	192								168								0								1							
Биты адреса	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Биты маски	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0
Октеты маски	255								255								255								240							

В данном случае уже нельзя говорить, что разделение адреса проходит по какой-то точке. Принадлежность двух адресов одной сети надо определять по двоичной последовательности, сопоставляя сходство и различие бит адресов в тех позициях, где бит маски равен 1.

Например, адреса 192.168.0.1 и 192.168.0.5 будут находиться в одной сети, т.к. они различаются лишь в последнем октете и в двоичном выражении это различие проявляется в тех позициях, где бит маски равен 0 (табл. 2.1.5).

Таблица 2.1.5

Адрес 1	1	0	0	0	0	0	0	0	1
Адрес 2	5	0	0	0	0	0	1	0	1
Маска	240	1	1	1	1	0	0	0	0

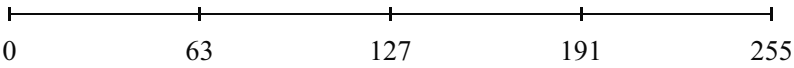
Адреса 192.168.0.1 и 192.168.0.50 будут в разных сетях, т.к. различие уже проявляется и в тех позициях, где бит маски равен 1 (табл. 2.1.6).

Таблица 2.1.6

Адрес 1	1	0	0	0	0	0	0	0	1
Адрес 2	50	0	0	1	1	0	0	1	0
Маска	240	1	1	1	1	0	0	0	0

Чтобы получить более наглядное представление о том, какие значения будут относиться к одной сети, а какие к разным, можно использовать простой прием, не требующий перевода адресов и масок в двоичный вид.

Рассмотрим, например, маску 255.255.255.192. Число 192 разбивает все пространство адресов на сети, состоящие из 64 узлов (192_{10} = = $1100\ 0000_2$, т.е. на адресацию узлов отводится 6 бит). Схематично это можно представить так:



Получается, что к одной сети будут относиться компьютеры, адреса которых попадают в один диапазон. Например, адреса со значением последнего октета 50 и 62 будут относиться к одной сети, а 50 и 75 — к разным.

Заметим также, что маску можно записывать и в более компактном виде. В связи с тем, что двоичная запись маски сначала содержит какое-то количество единиц, а потом нулей, для указания маски достаточно записать лишь количество единиц. Например, маску 255.255.255.240 в сокращенном варианте можно записать как 28. Полностью адрес с маской записывается при этом так: 192.168.0.1/28.

Сокращенный способ записи маски часто используется в Linux, полный — в Windows.

2.2. Маршрутизация

Итак, разделение адреса требуется для маршрутизации. Маршрутизация – это процесс определения маршрута следования пакетов данных в компьютерной сети.

Маршрутизация предполагает, что каждый компьютер, получивший пакет данных, должен принять решение — передавать этот пакет напрямую либо через промежуточный узел (шлюз). Напрямую пакеты передаются в том случае, когда отправитель и получатель находятся в одной сети. Через шлюз — когда сети разные.

Рассмотрим пример. Пусть наш компьютер-отправитель имеет адрес 192.168.0.1 и стандартную маску 255.255.255.0. Пусть имеются два пакета данных для двух получателей:

- получатель 1 — 192.168.0.18;
- получатель 2 — 192.168.1.15.

Сопоставим по сетевой маске адрес компьютера-отправителя с адресами получателей (табл. 2.2.1).

Таблица 2.2.1

Компьютер-отправитель	192	168	0	1
Маска (отправителя)	255	255	255	0
Получатель 1	192	168	0	18
Получатель 2	192	168	1	15

Как видно из таблицы, адреса компьютера-отправителя и получателя 1 отличаются лишь в позиции, где значение маски равно 0. Это означает, что компьютеры находятся в одной сети и пакет данных можно доставить напрямую.

Адреса отправителя и получателя 2 отличаются уже в двух позициях. При этом важно, что есть отличие в той позиции, где значение маски равно 255. Это однозначно указывает на то, что компьютеры находятся в разных сетях и доставка возможна только через промежуточный узел.

Если маска в своем описании содержит не только 0 и 255, но и другие значения, такие как 128, 192 и др., то сопоставление адресов надо проводить в двоичном виде либо пользоваться линейкой с диапазонами, как это рассматривалось в примере выше.

Например, если отправитель имеет адрес 192.168.50.0 и маску 255.255.192.0, а получатели: 1) 192.168.50.31; 2) 192.169.0.25; 3) 192.168.62.201; 4) 192.168.75.8, то мы имеем два очевидных случая и два неочевидных.

Очевидно, что первому получателю пакет данных можно отправить напрямую (адреса различаются только в той позиции, где маска равна 0), а второму получателю можно отправить лишь через промежуточный узел (адреса различаются в той позиции, где маска равна 255).

Неочевидные случаи — 3 и 4. Здесь различие наблюдается там, где маска равна 192. Однако по приведенной выше линейке видно, что числа 50 и 62 попадают в один диапазон, а 50 и 75 — в разный. Это

означает, что третьему получателю можно отправить пакет данных напрямую, а четвертому — лишь через промежуточный узел.

Как происходит выбор промежуточных узлов, принимающих пакеты данных, для дальнейшей пересылки в случае, когда отправитель не может отправить эти пакеты напрямую?

В простейшем (и самом распространенном случае) таким промежуточным узлом является *шлюз по умолчанию* (основной шлюз). Адрес такого шлюза указывается в сетевых настройках компьютера — обычно это адрес маршрутизатора, обеспечивающего общий доступ локальной сети к Интернету.

В более сложных случаях, когда на компьютере имеется несколько сетевых подключений либо структура сети такова, что ее отдельные фрагменты находятся в зонах, недоступных ни Интернету, ни вашему сегменту локальной сети, выбор «правильного» шлюза осуществляется на основе таблицы маршрутизации, где указываются адреса шлюзов для конкретных сетей.

Ниже приводится фрагмент такой таблицы, из которого видно, что компьютеры с адресами 192.168.0.x доступны напрямую, пакеты данных для компьютеров 10.x.y.z следует отправлять на компьютер 10.2.0.1, а пакеты данных для всех остальных адресов – на шлюз по умолчанию 192.168.0.1.

```
IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.100     10
         10.0.0.0        255.0.0.0         10.2.0.1      10.2.101.97     11
      192.168.0.0    255.255.255.0         On-link     192.168.0.100    266
===========================================================================
```

Таблицы маршрутизации могут быть статическим и динамическими. В первом случае они настраиваются на компьютере вручную. Во втором — таблица формируется автоматически на основе некоторого протокола маршрутизации (RIP, IGRP или др.).

Динамическая маршрутизация применяется, как правило, на крупных узлах, обслуживающих большое количество сетей. Такой способ настройки маршрутизации позволяет избавить администратора от трудоемкой настройки оборудования, а также учитывать изменения сети в процессе ее эксплуатации.

Заметим, что новые записи в таблице маршрутизации могут появляться и в результате создания различных соединений «точка — точка» (PPP, PPPoE, PPTP и др.). Эти записи обеспечивают доступ к ресурсам по создаваемым каналам.

2.3. Частные и публичные IP-адреса

Несложно понять, что IP-адреса должны быть уникальными в пределах всей сети. Это, в свою очередь, означает, что адреса должны распределяться централизованно, необходим учет адресов, задействованных в компьютерной сети.

В Интернете распределением адресов занимаются IANA (Internet Assigned Numbers Authority — Администрация адресного пространства Интернета), а также региональные интернет-регистраторы. Выделяемые ими адреса уникальны в пределах всего Интернета. Такие адреса называются *публичными*.

Примеры публичных адресов:

- 88.87.74.20 — mif.vspu.ru;
- 77.88.21.11 — yandex.ru;
- 173.194.122.201 — google.com.

Проблема практического использования публичных IP-адресов заключается в том, что выделение таких адресов может осуществляться лишь специальными компаниями, а данная услуга является, как правило, платной. Кроме этого, пул свободных IP-адресов к 2015 году уже практически исчерпан, что является серьезным ограничением развития публичных сервисов на основе рассматриваемой версии протокола IP.

Наряду с публичными существуют диапазоны *частных IP-адресов*, которые можно самостоятельно назначать в локальных сетях. Поскольку в разных локальных сетях такие адреса могут повторяться, их использование должно ограничиваться только создаваемыми вами сетями. Применение частных адресов для создания публичных интернет-узлов, а также для связи разных локальных сетей с повторяющимися адресами технически невозможно.

Диапазоны частных IP-адресов:

- 10.x.y.z;
- 172.16.x.y — 172.31.x.y;
- 192.168.x.y.

Учитывая дефицит и достаточно высокую стоимость публичных IP-адресов, в локальных сетях, как правило, используют частные адреса одного из представленных выше диапазонов. Однако для того, чтобы организовать доступ такой сети к Интернету, все же приходится использовать и публичные IP-адреса — как минимум один такой адрес должен быть назначен маршрутизатору локальной сети. Доступ в Интернет в этом случае организуется на основе NAT или Proxy.

К особому диапазону адресов можно отнести и адреса вида 127.x.y.z. Это адреса сетевой петли. На каждом компьютере обычно используется один такой адрес — 127.0.0.1 (localhost). Для любого компьютера этот адрес означает — «я сам». То есть обращение к компьютеру с таким адресом — это обращение к самому себе.

2.4. Использование доменных имен

Несмотря на то что в сетях TCP/IP передача информации осуществляется обязательно по IP-адресам, на практике возникла необходимость создания и другой системы имен — *доменной*. Проблема заключается в том, что числовые IP-адреса, которыми оперируют компьютеры, оказались неудобны для человека — их сложно запоминать, записывать, такие адреса могут часто меняться, их может быть несколько у одного узла. Более удобными оказались доменные имена, которые являются символьными и в своей записи используют обозначения, «поясняющие» характер сетевого ресурса.

Примеры доменных имен:

- yandex.ru;
- mif.vspu.ru;
- server.fizmat.vspu.ru.

Технический смысл использования доменных имен заключается в том, что за каждым именем может «скрываться» один или несколько IP-адресов, а с каждым IP-адресом может быть связано одно или несколько имен.

Примеры таких связей приводятся в таблице 2.4.1 (значения указаны для примера и могут отличаться в связи с изменениями в сети).

Таблица 2.4.1

Одно имя и несколько адресов	
yandex.ru	• 77.88.21.11 • 93.158.134.8 • 87.250.251.11 • 87.250.250.8
Один адрес и несколько имен	
88.87.74.20	• edu.vspu.ru • mif.vspu.ru • lms.vspu.ru • chess.vspu.ru

Как это работает на практике? Когда пользователь вводит некоторое доменное имя и обращается к сетевому ресурсу, то сначала происходит преобразование доменного имени в IP-адрес (если адресов несколько, то случайным образом выбирается один из них), после чего уже отправляется запрос к соответствующему серверу. Пользователь, таким образом, не должен указывать IP-адрес. Более того, процедура преобразования имени в адрес производится для пользователя практически незаметно — большинству пользователей даже и не требуется знать, что такие адреса существуют.

О том, как технически реализована служба, обеспечивающая такое преобразование, будет сказано ниже. Здесь лишь отметим, что эта служба называется DNS и для ее настройки на компьютере необходимо указать адрес как минимум одного DNS-сервера, доступного в вашей сети.

Отдельный вопрос присвоения доменных имен связан с выбором домена верхнего уровня, к которому относится сетевой ресурс. Созданием, поддержанием и управлением доменов верхнего уровня занимается международная организация ICANN (Internet Corporation for Assigned Names and Number — интернет-корпорация по присвоению имён и номеров).

Среди доменов верхнего уровня выделяют *общие домены* (com, edu, net, org, mil и более современные — info, mobi, name, travel, museum и др.), а также географические (ru, ua, by, de, uk, fr, ch, jp, cn и др.).

Знаковым нововведением в 2010 году стало использование географических доменов на национальных языках (рф, укр, бг, қаз, امارات, مصر и др.). Еще одно новшество, которое также окажет свое влияние на облик Интернета, — создание доменов верхнего уровня для крупных городов (например, moscow или paris).

2.5. Протокол IPv6

Протокол IPv6 (Internet Protocol, version 6) — это новая версия протокола IP, призванная решить существующие проблемы традиционной, 4-й версии протокола (иногда называемой IPv4).

Основная из этих проблем — исчерпание пула свободных IP-адресов. В связи с тем, что адрес IPv4 записывается 32-битным числом, общее количество сетевых устройств, имеющих уникальные адреса, не может быть более 2^{32}, что составляет примерно 4,3 млрд. Это заметно меньше, чем число потенциальных пользователей Интернета, что является существенным ограничением для развития глобальных коммуникационных систем. К 2015 году пул свободных IP-адресов уже практически исчерпан, дальнейшее уверенное развитие Интернета может быть связано только с внедрением протокола IPv6.

За счет увеличения длины сетевого адреса с 32 до 128 бит адресное пространство IPv6 становится по сути неисчерпаемым. Новый протокол имеет и другие особенности, обеспечивающие преимущества для построения высокопроизводительных компьютерных сетей. Ниже рассмотрим особенности IPv6 в сравнении с традиционной 4-й версией протокола.

Огромный запас адресов протокола IPv6 весьма часто подчеркивают яркими сравнениями с какими-то большими значениями. Например, приводят факт, что существующего запаса IPv6-адресов хватает для назначения 100 таких адресов каждому атому на поверхности Земли, или сравнивают количество выделенных адресов провайдерам Российской Федерации с весом нашей планеты в граммах (адресов больше, чем вес планеты в граммах). Подобные сравнения позволяют понять, что адресное пространство IPv6 на самом деле неисчерпаемо, количества доступных адресов с большим запасом хватает на любую обозримую перспективу.

Адресация протокола IPv6

Самое заметное отличие новой версии протокола проявляется в структуре адресов. Адрес IPv6 представляет собой 128-битное число, записываемое как восемь четырехзначных шестнадцатеричных чисел, разделенных двоеточием. Пример адреса:

2001:0db8:1f34:09d7:8a2e:07a0:11a3:765d

Адреса IPv6 могут записываться в кратком формате. Так, если несколько числовых групп, следующих друг за другом, равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::), а числа 0 в начале каждой группы могут сокращаться в соответствии с правилами математики. Примеры полной и сокращенной записи IPv6-адресов приведены ниже:

2001:0db8:0000:0000:0000:0000:11a3:765d
2001:db8::11a3:765d

2001:0db8:0000:0000:0000:0000:0000:0000
2001:db8::

0000:0000:0000:0000:0000:0000:0000:0001
::1

Сокращению может быть подвергнут только один набор нулевых групп, так как в противном случае восстановление исходного адреса будет неоднозначным. Другими словами, в сокращенном адресе двойное двоеточие может встретиться только один раз, при восстановлении исходного адреса между двоеточиями требуется лишь записать необходимое количество нулей.

Адрес ::1 является IPv6-адресом сетевой петли (аналог 127.0.0.1). Попробуйте на своем компьютере выполнить команду ping ::1, если вы получаете ответ, то на вашем компьютере установлен и успешно работает протокол IPv6.

Как и в случае четвертой версии протокола, адреса IPv6 разделяются на две части — идентификатор сети и идентификатор узла (интерфейса) в этой сети. Для такого разделения, однако, используется только префиксная нотация (через указание количества двоичных знаков, используемых для

обозначения сети). Привычный для IPv4 способ указания маски десятеричными числами (255.255.255.0 и др.) не используется. Пример разделения адреса в соответствии с префиксом /48 приводится в таблице 2.5.1.

Таблица 2.5.1

2001:0db8:1f34:09d7:8a2e:07a0:11a3:765d/48							
48 бит			80 бит				
2001	0db8	1f34	09d7	8a2e	07a0	11a3	765d
Идентификатор сети			Идентификатор узла				

Разделение адреса на две части является простейшим способом построения иерархии IPv6-адресов. В более сложных случаях можно задавать и другие иерархические границы, выделяя в адресе три и более частей. Например, IPv6-адрес может включать в себя:

- *глобальный префикс* — определяет блок адресов, полученных провайдером для дальнейшего распределения конечным пользователям (глобальный префикс указывает, в сети какого провайдера находится узел);
- *идентификатор области* — определяет блоки адресов, назначаемых провайдером своим клиентам;
- *идентификатор подсети* — позволяет логически разделить локальную сеть на отдельные подсети;
- *идентификатор интерфейса* — служит указателем на конкретный узел (интерфейс) в компьютерной сети.

Пример подобного разделения IPv6-адреса приводится в таблице 2.5.2.

Таблица 2.5.2

2001:0db8:1f34:09d7:8a2e:07a0:11a3:765d							
48 бит			16 бит	16 бит	48 бит		
2001	0db8	1f34	09d7	8a2e	07a0	11a3	765d
Глобальный префикс			Область	Подсеть	Интерфейс		

Узлы компьютерной сети на разных этапах маршрутизации пакетов оперируют каким-либо одним префиксом в соответствии со своим местом в иерархии маршрутизаторов. Например, на глобальном уровне маршрутизация будет осуществляться в соответствии с префиксом глобальной маршрутизации /48, провайдер будет оперировать префиксом /64, а в локальной сети будет использоваться префикс /80. Такое решение позволяет описать иерархию сети и выстроить в соответствии с этой иерархией правила маршрутизации.

Подобное решение также используется и на основе прежней версии протокола IP. Однако, учитывая особенности IPv6, с новым протоколом появляется возможность простого и четкого планирования схемы распределения таких адресов. Например, в IPv6 используются префиксы, определяющие границы разделения адреса в пределах не менее полубайта, что позволяет в адресе явно выделять фрагменты, «отвечающие» за свою часть иерархии.

Еще одной особенностью адресации сетевых узлов на основе протокола IPv6 является широкое применение идеи типизации IPv6-адресов. Выделяют три типа адресов IPv6.

1. *Unicast* (индивидуальный). Это «обычный» IPv6-адрес, который позволяет идентифицировать интерфейс в компьютерной сети. Пакеты данных, отправленные на такой адрес, будут доставлены на какой-либо конкретный узел (если узел с таким адресом присутствует в сети).
2. *Multicast* (групповой). Используется для отправки пакетов по нескольким адресам назначения – тем узлам, которые присоединены к соответствующей группе мультивещания. Групповые IPv6-адреса имеют префикс ff00::/8. Среди них выделяют некоторые специальные, значение которых всегда предопределено. Например, это FF02::1 — все узлы сети, а FF02::2 — все маршрутизаторы.
3. *Anycast* (произвольный). Это любой индивидуальный адрес, который назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к какому-то одному устройству с этим адресом (в соответствии с выбранной метрикой). Отличие произвольных адресов от групповых, таким образом, заключается в том, что multicast-рассылка предполагает отправку пакета данных сразу многим узлам, а anycast-рассылка — отправку пакета данных некоторому одному узлу из выбранного множества.

В IPv4 также используются описанные группы адресов, но в дополнение к ним — еще и *broadcast* (широковещательные) адреса. Пакет данных, отправленный на широковещательный адрес, направляется абсолютно всем узлам компьютерной сети (используется в сетях IPv4 для работы протоколов DHCP, ARP и др.). В протоколе IPv6 наличие широковещательных адресов не предусмотрено. Вместо широковещательной рассылки используется групповая рассылка на адрес FF02::1 (или на адреса особых служб).

Как и ранее, в IPv6 выделяются группы особых адресов. Мы уже упомянули про адреса сетевой петли и групповой рассылки. В дополнение к этим группам в IPv6 выделяются и особые индивидуальные адреса. Перечень основных групп IPv6-адресов по сравнению с аналогичными IPv4-адресами приводится в таблице 2.5.3. Адреса, не входящие в особые диапазоны, являются глобальными и могут назначаться компьютерам в сети Интернет.

Таблица 2.5.3

Группа адресов	**Описание**	**Аналог в IPv4**
::1/128	Loopback. Адрес сетевой петли	127.0.0.0/8
fc00::/7	Unique Local. Уникальные локальные адреса	Частные адреса (192.168.0.0/16 и др.)
fe80::/10	Link Local. Генерируется автоматически, обеспечивая работоспособность локальной сети в пределах одного сегмента	169.254.0.0/16
ff00::/8	Multicast. Адреса групповой рассылки	224.0.0.0/4
::ffff:0:0/96	IPv4-совместимые адреса. В младших 32 битах вписывается IPv4-адрес, что позволяет организовывать соединение узлов, использующих разные версии протокола	
2001:db8::/32	Адреса для примеров в документации	

В IPv6 широко используется возможность присвоения одному интерфейсу нескольких адресов. Так, при включении компьютера интерфейсу будет назначен Link Local адрес, сгенерированный на основе MAC-адреса интерфейса. Если после этого будет получен дополнительный адрес (через DHCP или др.), то этот адрес будет назначен вторым для интерфейса. Выбор нужного адреса естественным образом определяется на основе адреса назначения — выбирается наиболее подходящий адрес интерфейса, обеспечивающий прямую доставку либо маршрутизацию пакета данных через шлюз.

Один и тот же IPv6-адрес на некотором узле также может быть назначен и нескольким интерфейсам (например, если создаются интерфейсы виртуальных частных сетей, то они могут получать адреса, совпадающие с адресом родительского интерфейса). Чтобы явно обозначить привязку адреса к определенному интерфейсу, используется специальный суффикс при записи адреса. Например, в ОС Windows это может быть записано так: 2001:db8::11a3:765d%10, в Linux — 2001:db8::11a3:765d%eth0.

Возможности применения аппаратного адреса как части адреса IPv6 позволили реализовать и новые способы автоматического назначения IPv6-адресов в пределах сегментов компьютерной сети. Уникальные локальные и глобальные IPv6-адреса могут автоматически назначаться не только на основе DHCP, но и специальных рассылок маршрутизаторов, что позволяет упростить настройку сервисов сети. Подробнее про возможные способы назначения адресов будет сказано ниже (в разделе «Динамическая настройка узлов при помощи DHCP»).

Улучшение производительности сетей на основе IPv6

Протокол IPv6 создавался не только для решения проблемы нехватки IP-адресов, но и как протокол, который способен обеспечить высокую производительность компьютерных сетей. Для улучшения производительности был существенно переработан (упрощен) заголовок IPv6-пакетов, из которого удалена информация, не используемая маршрутизаторами для определения правил следования пакета, а также внедрены некоторые новые технологии обработки пакетов маршрутизаторами.

Так, в IPv6 отказались от расчета контрольной суммы – контроль целостности пересылаемых данных осуществляется на других уровнях OSI,

экономя ресурсы маршрутизаторов, которым теперь не приходится каждый раз проводить новые вычисления из-за изменения TTL (Hop Limit).

Резервом снижения нагрузки на маршрутизаторах стал также отказ от фрагментирования пакетов маршрутизатором при превышении MTU — используется технология Path MTU discovery, которая предполагает уменьшение размера пакета на отправляющей стороне по сигналу маршрутизатора.

Еще одна возможность экономии ресурсов маршрутизаторов проявляется в том, что маршрутизация пакетов теперь может осуществляться на основе меток потоков. Данная технология предполагает, что отправляющая сторона добавляет метку потока ко всем пакетам, отправляемым на один и тот же адрес. Маршрутизатор, один раз вычислив маршрут, использует эту информацию для того, чтобы не повторять свои вычисления для каждого нового пакета, следующего между теми же узлами. Пакеты пересылаются на основе меток потока, а также информации о маршруте, сохраненной в памяти маршрутизатора.

Снижение нагрузки на маршрутизаторы достигается и увеличением размеров пакетов (а значит, снижением их количества, снижением доли пересылаемой служебной информации). Пакеты IPv6 могут достигать весьма значительных размеров (до 4 гигабайт – IPv6 Jumbograms), что используется для построения сверхскоростных сетей.

Наряду с упрощением заголовка в пакетах IPv6 допускается использование расширенных заголовков (Extension Headers), которые помещаются между основным заголовком и пересылаемыми данными. В расширенных заголовках могут определяться различные дополнительные поля. Например, это может использоваться для уточнения маршрутов следования пакетов (source routing и др.), аутентификации, шифрования и др.

Увеличение скорости передачи информации в IPv6-сетях также достигается за счет наличия широких возможностей многоадресного вещания (групповая рассылка), что позволяет существенно снизить нагрузку на сеть в случае многоадресной пересылки мультимедийной информации (передача потокового видео сразу нескольким клиентам и др.).

Совместное использование IPv4 и IPv6

Протокол IPv6 позволяет получить многие преимущества по сравнению с протоколом IPv4. Однако повсеместное внедрение нового протокола ограничивается весьма серьезным обстоятельством — необходимостью обеспечения доступа к ресурсам существующих сетей, функционирующих на основе прежней, четвертой, версии протокола. Так как протоколы IPv4 и IPv6 несовместимы между собой, возникают сложности переходного периода, когда оба протокола приходится использовать вместе.

Очевидным решением совместного использования протоколов IPv4 и IPv6 является применение технологии двойного стека, когда в сети используются сразу два протокола — новый и старый. В этом случае интернет-ресурсы, поддерживающие новую версию протокола, будут доступны по IPv6, а старые ресурсы, поддерживающие только старую версию, доступны по протоколу IPv4 (рис. 2.5.1). Отметим, что в этом случае двойной стек должен поддерживаться не только в локальной сети, но и на стороне провайдера Интернета.

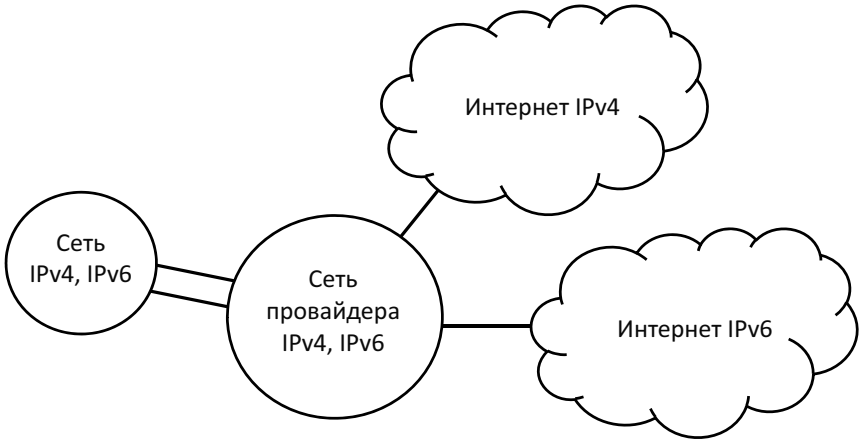


Рис. 2.5.1. Использование IPv4 и IPv6 в режиме двойного стека

Более сложная ситуация возникает тогда, когда провайдер Интернета не поддерживает сразу два стека протоколов, а поддерживает только один из них – IPv4 или IPv6. В этом случае возникают следующие вопросы.

1. Как получить доступ из своей IPv6-сети к другим таким сетям и IPv6-ресурсам Интернета, если провайдер не поддерживает IPv6?
2. Как получить доступ с старым IPv4-ресусам Интернета, если ваша сеть, а также сеть провайдера Интернета поддерживает только IPv6?

Первая ситуация, наиболее часто встречающаяся в настоящие дни, решается при помощи туннелирования – способа транспортировки пакетов одного протокола через сеть, использующую другой протокол. В нашем случае туннелирование обеспечивается тем, что исходные пакеты IPv6 вкладываются в виде блока данных в пакеты протокола IPv4 и пересылаются через сеть. В этом случае в каждой IPv6-сети должен быть маршрутизатор, обеспечивающий туннелирование, подключенный к некоторой общей IPv4-сети. Пример возможной схемы такой сети представлен на рисунке 2.5.2.

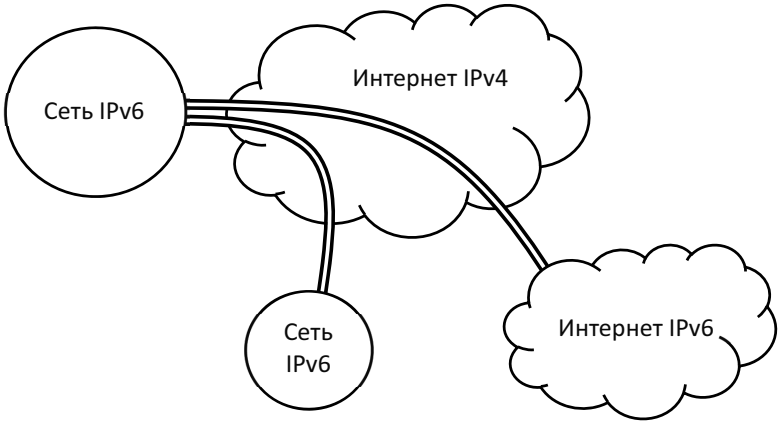


Рис. 2.5.2. Туннелирование пакетов IPv6 через сеть IPv4

Благодаря особой системе IPv6-адресов, применяемых в туннелированных сетях, каждый маршрутизатор имеет информацию об адресе другого маршрутизатора, которому надо передать пакет с инкапсулированными данными. Получается, что сеть IPv6 функционирует как единое целое, основываясь на старой сети IPv4.

Получить IPv6-адрес и использовать его по описанной технологии сейчас можно через услуги *туннельного брокера* (сервиса туннелей). Такие услуги на бесплатной основе предлагают многие крупные телекоммуникационные компании разных стран. Подключившись к туннельному брокеру, вы сможете работать с Интернетом IPv6, даже если ваш провайдер не поддерживает новый протокол.

Вторая ситуация, которая будет становиться все более актуальной по мере внедрения протокола IPv6, решается путем технологии преобразования протоколов и сетевых адресов (NAT64). Согласно этой технологии, IPv6-пакеты, направляемые на IPv4-адреса, на границе сетей преобразуются

маршрутизатором к IPv4-пакетам, адрес назначения которых вычисляется через адрес IPv6 (IPv4-адрес записывается как часть адреса IPv6). Схематично такая сеть представлена на рисунке 2.5.3. Как видно из рисунка, узлы IPv6-сети могут напрямую взаимодействовать с Интернетом IPv6, а с Интернетом IPv4 – через NAT64-маршрутизатор, установленный в сети провайдера.

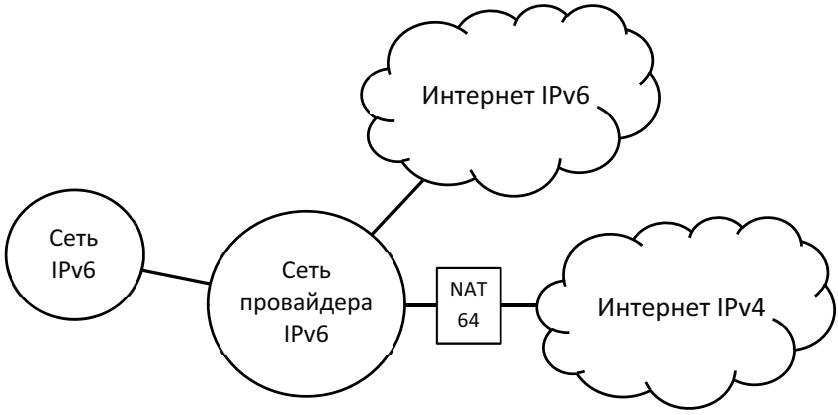


Рис. 2.5.3. Организация доступа к узлам IPv4 из сети IPv6

Применение NAT64 требует изменений в работе службы DNS. В частности, IPv4-адреса, возвращаемые DNS-серверами из IPv4-сети, должны преобразовываться к виду, «понятному» узлам, использующим лишь протокол IPv6. Такое преобразование делается при помощи службы DNS64, которая может функционировать на маршрутизаторе, осуществляющем преобразования NAT64.

Технология NAT64 используется только для доступа из сети IPv6 в сеть IPv4, но не наоборот. Обратное преобразование невозможно из-за имеющейся разницы в количестве адресов. Вместе с тем существует возможность и двусторонней связи сетей IPv4 и IPv6 через маршрутизатор, осуществляющий прямое преобразование. В таких сетях, однако, должны использоваться особые IPv6-адреса, которые в качестве своей части включают IPv4-адрес (адреса с префиксом ::ffff:0:0/96).

Возможны ситуации, когда ваша сеть поддерживает два стека протоколов, а сеть провайдера только новый протокол IPv6. В этом случае возможно сочетание технологий туннелирования (IPv4 через сеть IPv6) и двойного стека. Преобразования адресов и протоколов для доступа с узлов IPv6 к узлам IPv4 здесь не потребуется.

Вопросы и задания

Опишите назначение протоколов IP и TCP в соответствии с уровнями модели OSI.

Приведите примеры IP-адресов. Как эти адреса разделяются на части, указывающие на сеть и на узел в сети?

Для чего предназначена маска сети? Назовите два способа описания сетевой маски.

Что такое маршрутизация? Как определяется маршрут на основе адресов и маски?

Чем отличаются частные и публичные адреса? Как можно получить частный или публичный адрес для использования в своей сети?

Что такое доменная система имен? Как связаны доменные имена и IP-адреса компьютеров в сети?

Что послужило причиной разработки 6-й версии протокола IP? Какими преимуществами обладает протокол IPv6 по сравнению с прежней, четвертой, версией протокола?

Приведите пример адреса IPv6. Какие варианты сокращенной записи такого адреса существуют?

Что такое индивидуальные и групповые IPv6-адреса? Какие еще типы IPv6-адресов существуют?

Назовите особые диапазоны адресов IPv6.

Какие способы совместного использования протоколов IPv4 и IPv6 вы можете назвать?

Раздел 3. Управление сетями TCP/IP

Каждый узел в сетях TCP/IP имеет особые настройки, назначаемые в соответствии с требованиями сети. Эти настройки в самом простом случае включают в себя указание адреса, маски, шлюза по умолчанию и сервера DNS, а в более сложных — еще и правил маршрутизации, ограничения трафика, преобразования адресов и др. В данном разделе описываются технологии динамической настройки узлов, организации доступа и защиты в компьютерной сети. Понимание этого материала требуется для планирования сети, а также настройки различных сетевых сервисов, позволяющих реализовать на практике указанные технологии.

3.1. Динамическая настройка узлов при помощи DHCP

Как было показано в предыдущем разделе, для полноценной работы в сети TCP/IP на каждой рабочей станции требуется указать IP-адрес, маску, шлюз по умолчанию и адрес как минимум одного сервера DNS. Все перечисленные параметры могут задаваться вручную, однако более удобным оказывается вариант автоматической настройки параметров сети. Для автоматизации этого процесса, как правило, используется служба *DHCP* (Dynamic Host Configuration Protocol – протокол динамической настройки узла).

Техническая реализация службы DHCP предполагает, что в сети есть как минимум один DHCP-сервер, который управляет процессом назначения сетевых параметров рабочим станциям в компьютерной сети. Взаимодействие рабочих станций и сервера осуществляется согласно логике 4 этапов.

1. *Обнаружение сервера.* На этом этапе рабочая станция, желая получить параметры сети, отправляет широковещательный запрос с целью обнаружить доступные DHCP-серверы. Как правило, такой запрос отправляется в процессе включения рабочей станции — загрузки операционной системы.
2. *Предложение.* Сервер, получив запрос, подбирает конфигурацию для рабочей станции и отправляет свое предложение, используя аппаратный адрес компьютера, с которого пришел запрос. Заметим, что на этом этапе свои предложения подготовят несколько DHCP-серверов, если они существуют в компьютерной сети.

3. *Запрос.* Рабочая станция, получив разные предложения от DHCP-серверов, выбирает наиболее подходящее из них и отправляет запрос на выбранную конфигурацию соответствующему серверу.
4. *Подтверждение.* DHCP-сервер, получив запрос на использование конфигурации, отправляет подтверждение рабочей станции, фиксируя в своей базе данных, что конфигурация закреплена. Рабочая станция, получив подтверждение, настраивает свой сетевой интерфейс согласно выбранной конфигурации.

Несмотря на то что каждый раз при включении рабочей станции процедура выбора сетевой конфигурации выполняется снова, служба DHCP все же стремится обеспечить стабильность назначения адресов. Так, на шаге 2 DHCP-сервер по возможности будет выбирать ту конфигурацию, которая ранее уже использовалась данной рабочей станцией, а на шаге 3 — из всех предложенных конфигураций компьютер для себя выберет ту, которая прежде ему уже назначалась.

Еще один аспект работы службы DHCP – сетевые параметры, как правило, назначаются рабочим станциям не на постоянное время, а выдаются в аренду. В таком случае, если компьютер завершает свою работу в аварийном порядке и не успевает отправить серверу сообщение с отказом от конфигурации, эта конфигурация возвращается серверу автоматически по истечении срока аренды.

В качестве сервера DHCP в компьютерных сетях могут использоваться машины, работающие под управлением Windows Server, Linux, FreeBSD или других серверных операционных систем, а также аппаратные устройства, такие как маршрутизаторы и точки доступа. Минимальная настройка сервера DHCP заключается в определении диапазона свободных IP-адресов (эти адреса будут назначаться рабочим станциям), а также других обязательных параметров протокола TCP/IP (маска, шлюз по умолчанию, адреса серверов DNS).

Отметим, что DHCP — это не единственный способ автоматической настройки сетевых параметров узлов компьютерной сети. В частности, настройка интерфейса может осуществляться в процессе установки соединения «точка — точка» (PPP, PPPoE, PPTP и др.). На компьютерах Windows адрес может быть назначен автоматически в процессе выполнения процедуры назначения адреса в отсутствие DHCP (выдаются адреса вида 169.254.x.y с маской сети 255.255.255.0).

Назначение сетевых параметров в сетях IPv6

В сетях IPv6 реализованы особые механизмы назначения сетевых параметров, которые могут использоваться вместо или вместе со службой DHCP. Так, IPv6-адрес и другие сетевые параметры в автоматическом режиме могут быть назначены одним из следующих способов.

1. Адреса могут быть *сгенерированы автоматически* на основе аппаратного адреса интерфейса. Это Link Local адреса с префиксом fe80::/10 (аналог адресов 169.254.x.y), которые способны обеспечить работоспособность компьютеров в пределах одного сегмента локальной сети. Отличие протокола IPv6 здесь проявляется в том, что частью Link Local адреса является MAC-адрес интерфейса. Link Local адреса, как правило, назначаются интерфейсу даже в том случае, когда каким-либо другим способом интерфейс получает также иной адрес, в том числе обеспечивающий выход в Интернет.
2. Адрес компьютера и другие сетевые настройки могут быть получены путем *процедуры автоматической настройки SLAAC* (Stateless Address Autoconfiguration), которая предполагает участие в этом процессе маршрутизатора сети. Процедура реализуется так: маршрутизатор делает рассылку объявления с указанием специфических настроек сети — префикса сети, шлюза по умолчанию и сервера DNS. Получив такое объявление, станция генерирует вторую часть адреса (на основе MAC-адреса или случайным образом) и назначает сетевые параметры на свой интерфейс. Процедура SLAAC, таким образом, позволяет в автоматическом режиме назначить необходимый минимум сетевых параметров без использования DHCP.

Маршрутизаторы делают рассылку объявлений с некоторой периодичностью (например, 200 секунд) по групповому адресу FF02::1 (то есть всем узлам компьютерной сети). Такое объявление может быть отправлено и по запросу рабочей станции (станция отправляет запрос на групповой адрес маршрутизаторов — FF02::2).

Вторая часть адреса, дополняющая полученный префикс, в наиболее простом варианте генерируется автоматически на основе MAC-адреса интерфейса. Такой подход, отличаясь простотой, позволяет создать уникальный IPv6-адрес, так как уникальны сами MAC-адреса. Однако высказываются опасения о наличии возможностей идентификации физического компьютера из сети Интернет. Узлы, к которым

обращается компьютер, могут однозначно идентифицировать ваш компьютер по MAC-адресу, так как этот адрес является частью адреса IPv6. Такая возможность нарушает правила конфиденциальности, дает возможность построения алгоритмов навязчивой рекламы и др. В этой связи операционные системы могут применять и другой алгоритм назначения второй части адреса, предполагающий генерацию случайной последовательности чисел с последующей проверкой отсутствия полученного адреса на других компьютерах сети.

3. В случае когда узлам сети требуется установка параметров, не рассылаемых маршрутизатором сети (DNS-префикс по умолчанию, адрес сервера DNS, который не всегда удобно рассылать маршрутизатором и др.), возможно совместное применение процедур SLAAC и назначение сетевых параметров при помощи DHCP (иногда в соответствии с версией протокола называемом как DHCPv6). В этом случае адрес и другие минимально необходимые настройки назначаются способом, описанным в п. 2, но в дополнение к этому маршрутизатор сообщает, что расширенные параметры необходимо получить у сервера DHCP. Запрос к такому серверу рабочая станция отправляет на групповой адрес FF02::1:2 – адрес всех серверов DHCP. В ответе DHCP-сервер сообщает расширенные параметры компьютерной сети. Эти параметры, в дополнение к уже имеющемуся адресу, назначаются интерфейсу рабочей станции.

Так как сервер DHCP не формирует адрес, назначаемый рабочей станции, а лишь предлагает общие параметры сети, то такой сервер работает в режиме без отслеживания состояния. Серверу не приходится запоминать назначенные адреса, контролировать их уникальность, отслеживать состояние рабочих станций. Настройка сервера DHCP без отслеживания состояния является более простой, чем «обычного» сервера DHCP.

4. Назначение адреса IPv6 может полностью осуществляться при помощи DHCP. Процедура такого назначения по своей сути не отличается от описанной применительно к четвертой версии протокола IP. Единственным заметным нововведением является лишь отсутствие широковещательного запроса на обнаружение DHCP. Такой запрос отправляется с Link Local адреса на групповой адрес DHCP-серверов – FF02::1:2.

3.2. Настройка сервера общего доступа к Интернету

Большинство локальных сетей в настоящее время создаются не только для работы с внутренними сетевым ресурсами, но и для организации доступа рабочих станций к сети Интернет (часто именно это является основной задачей). Для того чтобы обеспечить доступ всех компьютеров локальной сети к Интернету, достаточно иметь подключение лишь на одном из компьютеров этой сети. Настроив сервер общего доступа, вы сможете обеспечить подключение к Интернету и всех остальных компьютеров локальной сети.

Обратите внимание, что с технической точки зрения способ внешнего подключения к Интернету не играет существенной роли. Ваша локальная сеть может иметь доступ в Интернет через оптоволоконный кабель, ADSL-модем, радиоканал и др. Важно лишь то, что сервер общего доступа имеет подключение как к Интернету, так и к локальной сети. Если такое условие выполняется, то доступ к Интернету можно предоставить и всем остальным компьютерам локальной сети.

Итак, рассмотрим ситуацию, когда у нас есть локальная сеть и в этой сети *один* компьютер каким-либо способом подключен к Интернету (рис. 3.2.1). Как обеспечить доступ к Интернету со всех остальных компьютеров локальной сети? Рассмотрим три способа организации такого подключения.

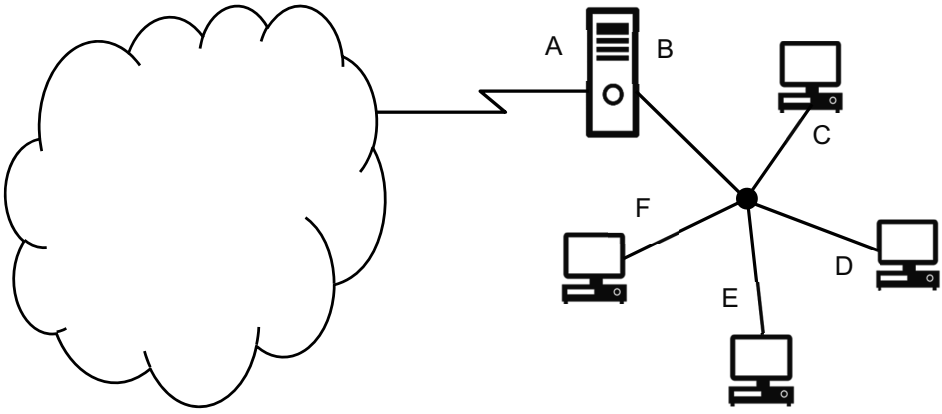


Рис. 3.2.1. Общая схема подключения
локальной сети к Интернету

Способ 1. Настройка прямой маршрутизации

Данный способ предполагает, что сервер общего доступа имеет два сетевых интерфейса. Первый интерфейс (A) — внешний (подключение к Интернету), второй (B) — внутренний (подключение к локальной сети). Оба интерфейса этого сервера, а также все рабочие станции в локальной сети (интерфейсы C–F) *должны иметь публичные IP-адреса*. В качестве шлюза на рабочих станциях указывается внутренний интерфейс сервера общего доступа (интерфейс B), а на сервере общего доступа настраивается маршрутизация — пересылка IP-пакетов с внутреннего интерфейса (B) на внешний (A) и наоборот.

Подобная организация сети обеспечивает прямую маршрутизацию между вашими компьютерами и узлами сети Интернет. Пакеты данных из локальной сети, следуя через шлюз, будут достигать требуемых узлов в Интернете. Аналогичным образом будут пересылаться и ответы — компьютеры вашей локальной сети доступны по своему адресу любым узлам Интернета через созданный вами шлюз.

Настройка прямой маршрутизации обеспечивает полноценное подключение к Интернету. Фактически, локальная сеть становится *частью* Интернета – предоставляется доступ не только из локальной сети в Интернет, но и наоборот – из Интернета в созданную вами сеть. Вы сможете без ограничений использовать все возможности сетевого доступа к самым разнообразным службам Интернета.

Такой способ подключения обладает и недостатками. Первый недостаток связан с необходимость получения вами большого количества публичных IP-адресов. Напомним, что для четвертой версии протокола IP эта услуга является платной и существенной проблемой является исчерпание пула свободных IPv4-адресов. Второй недостаток — наличие потенциальной угрозы безопасности рабочих станций вашей сети, к которым существует принципиальная возможность доступа из сети Интернет. Так как в большинстве случаев доступ из Интернета к рабочим станциям локальной сети полезной нагрузки не несет, то в целях обеспечения безопасности требуется специальная настройка межсетевого экрана.

Для настройки общего доступа на основе прямой маршрутизации можно использовать компьютер под управлением Windows, Linux или FreeBSD, а также аппаратное устройство — маршрутизатор, DSL-модем или др.

Заметим, что при использовании Windows не требуется применять исключительно серверную версию этой операционной системы. Все современные версии Windows могут выполнять роль маршрутизатора. Вместе с тем в разных версиях Windows реализованы разные способы организации общего доступа к сети Интернет. Однако среди Windows наибольшими возможностями для создания сервера общего доступа обладают все же серверные версии операционной системы, где реализована специальная служба — RRAS (Routing and Remote Access Service — служба маршрутизации и удаленного доступа).

Некоторым промежуточным решением между использованием компьютера или аппаратного устройства может стать маршрутизатор, настроенный на компьютере с pfSense.

pfSense — это операционная система, которая создана на основе FreeBSD и предназначена для создания межсетевых экранов и маршрутизаторов. Несмотря на то что операционная система работает на полноценном компьютере, способы ее настройки и управления реализованы так, как обычно это делается в аппаратных маршрутизаторах. То есть управление данной операционной системой производится удаленно через веб-интерфейс, а настройка осуществляется на основе выбора предлагаемых опций.

Способ 2. Настройка общего доступа через преобразование сетевых адресов (NAT)

NAT (Network Address Translation) — преобразование сетевых адресов. Данный способ призван преодолеть недостатки прямой маршрутизации. В этом случае вам потребуется только один публичный адрес — на внешнем интерфейсе (A) сервера общего доступа. Все остальные адреса («внутри» локальной сети) вполне могут быть частными (интерфейс B сервера, а также интерфейсы C–F рабочих станций).

Особенностью данного подключения является то, что сервер общего доступа не только пересылает IP-пакеты с внутреннего интерфейса на внешний и наоборот, но и производит замену адресов:

1) при следовании пакета из локальной сети в Интернет заменяется адрес отправителя — вместо адреса рабочей станции (адреса какого-либо из интерфейсов C–F) записывается адрес внешнего интерфейса сервера общего доступа (адрес интерфейса A);

2) при следовании пакета из Интернета в локальную сеть (точнее – при поступлении пакета из Интернета на внешний интерфейс сервера общего доступа) проверяется, является ли этот пакет ответом на ранее отправленный пакет для какого-то компьютера из локальной сети (такая проверка производится на основе фиксации портов); если это так, то в пакете меняется адрес получателя — вместо адреса внешнего интерфейса (A) сервера общего доступа записывается адрес соответствующего компьютера локальной сети (какого-либо из интерфейсов C–F) и пакет далее отправляется в локальную сеть.

Как видим, в данном случае достаточно лишь одного публичного IP-адреса, а доступ, инициированный из Интернета к рабочей станции вашей локальной сети, просто невозможен. Таким образом, NAT позволяет снять сразу две проблемы, присущие прямой маршрутизации. Кроме этого, вам не придется перестраивать всю сеть, если вы меняете провайдера Интернета (изменится только публичный адрес и связанные с ним настройки на внешнем интерфейсе маршрутизатора, все адреса и настройки локальной сети останутся прежними).

Вместе с тем у данного способа существуют свои достаточно существенные недостатки. Во-первых, обращения всех компьютеров локальной сети к Интернету отправляются с одного адреса — адреса внешнего интерфейса (A) сервера общего доступа к сети Интернет. Это приводит к проблемам, если сервисам Интернета требуется различение пользователей по IP-адресам (различные блокировки пользователей, защита от спам-атак, накруток голосования и др.). В данном случае действия, совершенные каким-либо пользователем в локальной сети, могут привести к блокировке этого действия для всех остальных пользователей.

Во-вторых, NAT-подключение не позволяет обеспечивать доступ к Интернету для больших сетей. Так как в процессе преобразования серверу общего доступа приходится запоминать порты (строить таблицу сопоставления: адрес и порт рабочей станции — порт сервера общего доступа), то число одновременно поддерживаемых подключений не может быть больше 65535. Учитывая, что одна рабочая станция может задействовать несколько (как правило, десятки) подключений, реальное число компьютеров, подключенных к Интернету через NAT, может быть значительно меньше указанного значения.

В-третьих, как было сказано, NAT не обеспечивает прямого доступа из Интернета к компьютерам локальной сети, а такой доступ иногда все же необходим. Это требуется при использовании некоторых протоколов

(BitTorrent, протоколы VPN-доступа, видеосвязи и др.), а также при создании общедоступных сервисов Интернета. Данная проблема частично решается при помощи механизма *пробрасывания портов* (*port mapping*), однако полноценное решение будет связано только с прямой маршрутизацией.

Применение протокола IPv6 снимает проблему нехватки IP-адресов, а существующие механизмы позволяют легко назначать адреса и другие сетевые параметры компьютерам в сети. В этих условиях технология NAT применительно к IPv6-сетям теряет свою актуальность. Основным способом подключения локальных IPv6-сетей к Интернету является прямая маршрутизация.

Другой аспект организации доступа к Интернету IPv6-сетей связан с совместным использованием протоколов IPv6 и IPv4. Возможные способы сочетания сетей IPv4 и IPv6 описаны нами ранее в разделе «Протокол IPv6».

Для создания NAT-подключения, как правило, можно использовать те же программно-аппаратные решения, что и для прямой маршрутизации. Сервер общего доступа на основе NAT можно сделать на основе компьютера под управлением Windows, Linux или FreeBSD, а также аппаратного устройства — маршрутизатора, DSL-модема или др.

Способ 3. Использование прокси-подключения

Термином прокси (proxy — представитель, уполномоченный) обычно обозначают службы, которые позволяют выполнять косвенные запросы к другим сетевым службам. В данном случае речь идет о прокси-сервере, который будет служить своеобразным посредником при обращении рабочих станций к веб-ресурсам Интернета.

Назначение IP-адресов при прокси-подключении может быть точно таким же, как и в случае использования NAT (достаточно лишь одного публичного адреса на внешнем интерфейсе прокси-сервера, все остальные адреса могут быть частными). Однако требуется и специальная настройка браузеров на компьютерах клиентов — в параметрах подключения необходимо указать адрес прокси-сервера и используемый порт (обычно это 8080 или 3128).

При обращении к сетевому ресурсу браузер отправляет запрос не напрямую в Интернет, а прокси-серверу. Сервер, анализируя запрос клиента, запрашивает от своего имени необходимую информацию в Интернете и

далее пересылает ее клиенту. Прокси-сервер, таким образом, является посредником, «перевалочной базой» для документов, запрашиваемых пользователем во внешней сети. Технология прокси-подключения функционирует на прикладном (седьмом) уровне модели ISO/OSI, а не на сетевом (третьем), как в случае с прямой маршрутизацией или NAT.

В чем достоинства прокси-подключения? Как и в случае с NAT, прокси-подключение снимает проблемы востребованности большого количества публичных IP-адресов, а также доступа к локальным ресурсам из Интернета. Но в дополнение к этому есть и другие преимущества, присущие исключительно прокси.

1. Прокси-сервер запоминает пересылаемую информацию в своей кеш-памяти. Это позволяет не запрашивать повторно информацию, которая ранее уже доставлялась клиентам локальной сети. Прокси-сервер, таким образом, может существенно ускорить доступ к ресурсам Интернета, снизить нагрузку на внешние каналы связи, снизить стоимость подключения в случае использования тарифов с оплатой за трафик.
2. Прокси-сервер способен детально анализировать пересылаемую информацию (включая анализ указателей ресурсов, содержания пересылаемых файлов и страниц) и принимать на основе анализа советующие решения. Например, это может быть блокировка ресурсов, работа с которыми не допускается из вашей сети, удаление рекламы, ограничение скорости загрузки, перенаправление запросов к другим серверам и др.
3. Прокси-сервер может вести детальную статистику и учет доступа пользователей к Интернету, что может использоваться как для ограничения доступа к сетевым ресурсам тем или иным пользователям, создания различных биллинговых систем, так и для контроля использования Интернета сотрудниками организаций.

В качестве недостатков прокси-подключения можно указать возможность работы лишь с определенными типами сервисов Интернета (как правило, это доступ лишь по протоколам HTTP и FTP), более сложную настройку сети, высокие требования к аппаратной части сервера общего доступа. Кроме того, учитывая современный и достаточно высокий уровень развития глобальных коммуникаций, а также тот факт, что наиболее часто используемые ресурсы Интернета являются динамическими и кешированию не подлежат, привлекательность прокси-подключения в настоящее время

становится не такой высокой. Данный способ подключения сейчас уже не следует рассматривать как основной.

Для упрощения настройки локальных сетей, использующих прокси-подключение, разработаны различные технологии, обеспечивающие автоматическую настройку компьютеров пользователей. В частности, существует протокол автоматической настройки прокси-подключения через скрипты автонастройки (WPAD, Web Proxy Auto-Discovery Protocol), а также технология прозрачного прокси.

В первом случае предполагается, что браузер автоматически «находит» скрипт автонастройки (для этого может использоваться DHCP или DNS) и использует указанные параметры для подключения к Интернету. Во втором случае настраивается лишь сервер общего доступа — все обращения к Интернету автоматически направляются к прокси-серверу. Специальная настройка рабочих станций в этом случае не требуется. Запросы, отправляемые в Интернет, автоматически и «прозрачно» для пользователя пересылаются прокси-серверу, который обеспечивает получение ответа.

Для создания прокси-сервера требуется установка и настройка специального компьютера, аппаратные решения в данном случае неприменимы. Как правило, это компьютер на основе Linux или FreeBSD, а в качестве прокси-сервера используется Squid.

3.3. Межсетевой экран

Межсетевой экран — это аппаратное устройство или программное средство, которое осуществляет контроль и фильтрацию проходящих сетевых пакетов в соответствии с заданными правилами. Межсетевой экран также часть называют *файрволом* (от *англ*. firewall) или *брандмауэром* (от *нем*. brandmauer). Все эти термины равнозначны.

В локальный сетях, как правило, межсетевой экран настраивается на маршрутизаторе, обеспечивающем общий доступ локальной сети к Интернету. В этом случае межсетевым экраном контролируется процесс пересылки пакетов данных между внешним и внутренним интерфейсами маршрутизатора (интерфейсами A и B согласно рис. 3.2.1), что обеспечивает необходимый уровень доступа и защиту от внешних атак для всей локальной сети.

Межсетевым экраном обычно анализируются следующие параметры пересылаемых пакетов:

1) адрес отправителя или получателя;
2) порт отправителя или получателя;
3) используемый протокол.

На основе анализа указанных параметров межсетевым экраном принимается решение о пересылке или блокировке пакетов. Это позволяет открыть или заблокировать доступ к каким-либо серверам Интернета (или рабочим станциям локальной сети), блокировать возможность использования тех или иных протоколов.

Например, межсетевой экран может пропускать пакеты данных на порт 80 и блокировать пакеты на порт 25. В этом случае пользователи могут работать с сайтами Интернета, но не могут при помощи своих почтовых программ отправлять электронные письма другим пользователям Интернета, минуя корпоративный почтовый сервер. Такая настройка межсетевого экрана позволяет бороться с вирусными и спам-рассылками из локальной сети, иногда случающимися из-за заражения компьютеров.

Другой пример — это блокировка пактов протокола ICMP при разрешенном протоколе IP. В этом случае доступ к различным службам Интернета будет производиться в штатном режиме, но утилиты ping и tracert покажут недоступность узлов.

Настройка межсетевого экрана может производиться по белым или черным спискам. В первом случае по умолчанию блокируются все ресурсы, а потом составляется список тех, к которым все же надо предоставить доступ. Во втором случае наоборот, доступ по умолчанию открыт ко всем ресурсам и ведется отдельный список тех из них, к которым доступ надо блокировать. Если используемый вами межсетевой экран позволяет использовать обе стратегии настройки, то выбирайте ту из них, которая позволит лучше контролировать необходимый уровень доступа в соответствии с задачами и кругом пользователей вашей сети.

Отметим, что, помимо простых проверок (адреса, порты, протоколы), доступных во всех реализациях межсетевых экранов, в более «продвинутых» случаях может производиться и дополнительный анализ трафика, связанный с логикой работы сетевых протоколов, количеством запросов, анализом пересылаемых данных и др. Такой анализ позволяет бороться с различными атаками из Интернета, которым могут подвергаться ваши серверы и локальная сеть.

Еще одна задача, которая часто возлагается на межсетевой экран, — это *перенаправление портов* (пробрасывание портов, port mapping). Перенаправление портов — это технология, которая позволяет получить доступ к ресурсам какого-то компьютера, обращаясь к ним по адресу другого компьютера (маршрутизатора), где настроено перенаправление портов.

В частности, пакеты данных, отправляемые из Интернета на адрес и определенный порт маршрутизатора, могут без изменений пересылаться во внутреннюю сеть – на определенный адрес и порт компьютера, даже если этот компьютер получает доступ к Интернету через NAT. Подобная пересылка пакетов позволяет создавать общедоступные сервисы Интернета на компьютерах, расположенных «внутри» локальной сети. Адресом такого сервиса для пользователей Интернета будет адрес маршрутизатора.

Перенаправление портов часто используется из-за необходимости — как частичное решение проблемы доступа из Интернета к локальной сети, подключенной с использованием NAT (настройка BitTorrent, организация внешнего доступа к тем или иным ресурсам). Однако такая технология может быть полезной и с точки зрения создания гибкой и безопасной серверной инфраструктуры вашей сети. В частности, она позволяет обеспечить доступ ко всем ресурсам сети через единый адрес маршрутизатора, используя при этом разные машины для физической реализации отдельных служб.

Организацию доступа к общедоступным сервисам, защищенным межсетевым экраном, можно реализовать и на основе технологии DMZ (Demilitarized Zone — демилитаризованная зона). Не останавливаясь подробно на профессиональных решениях организации DMZ, скажем, что в простых маршрутизаторах «домашнего» уровня часто имеется возможность указать DMZ-хост (компьютер «внутри» локальной сети). В этом случае все порты компьютера становятся доступными через соответствующие порты маршрутизатора. Он может выполнять роль общедоступного сервера, несмотря на свое размещение «внутри» локальной сети.

Настройка межсетевого экрана, как правило, осуществляется согласованно с настройкой маршрутизации или NAT. Обычно это реализовано в одном комплекте программного обеспечения — специальных программных комплексах, на уровне ядер операционных систем, в микропрограммах аппаратных устройств. Поэтому если вы каким-либо способом настроили маршрутизацию или NAT, то скорее всего в рамках того

же инструментария вам предложат настроить и какие-то параметры межсетевого экрана.

Вместе с тем существуют и специальные решения межсетевых экранов — специализированное программное обеспечение, а также аппаратные устройства, для которых функция защиты является основной. Как правило, эти решения отличаются высокой надежностью, присутствием дополнительных функций, связанных с анализом трафика и защитой сетей, а также наличием различных сертификатов, подтверждающих возможность их использования в случаях построения сетей, к безопасности которых предъявляются законодательные требования (обработка персональных данных и др.).

К программному обеспечению для защиты локальных сетей можно также отнести и специализированные программы, предназначенные для фильтрации интернет-трафика в школьных сетях. Это такие программы, как «Интернет Цензор», KinderGate, «Интернет Контроль Сервер» и др. Основная задача таких программ — обеспечение доступа из школьной сети только к тем ресурсам Интернета, которые соответствуют ограничениям по возрасту и кругу учебных задач. Как правило, такие программы открывают доступ к Интернету на основе списков рекомендованных сайтов, что позволяет в максимальной степени обеспечить безопасный доступ к Интернету для детей.

3.4. Удаленные подключения VPN

VPN (Virtual Private Network, виртуальная частная сеть) — обобщенное название технологий, позволяющих создавать сетевые соединения поверх другой сети. В зависимости от решаемых задач и применяемых протоколов, VPN позволяет создавать соединения вида «точка — точка», «точка — сеть», «сеть — сеть».

Не останавливаясь подробно на теоретических основах и особенностях технической реализации VPN, скажем, что данная технология позволяет решить, например, следующие задачи.

1. *Предоставить доступ к Интернету клиентам некоторого поставщика услуг*. Как правило, подключение к Интернету предусматривает парольный доступ к предоставляемым услугам, учет использованного трафика, защиту передаваемых данных через общедоступные сети. Технологии VPN дают возможность

обеспечить выполнение этих условий, предоставить удобный и безопасный доступ к Интернету большому числу пользователей через единый физический канал.

2. *Настроить подключение компьютера к удаленной локальной сети.* Например, если у вас есть локальная сеть на работе (с выходом в Интернет), то, используя VPN, вы сможете настроить доступ к этой сети с вашего домашнего компьютера (также подключенного к Интернету). Этот доступ будет организован через виртуальный канал, работающий «поверх» Интернета. Виртуальный интерфейс, создаваемый при подключении к удаленной сети, логически не будет отличаться от физических интересов на компьютерах той сети, к которой вы подключаетесь. Ваш домашний компьютер будет иметь полноценный доступ ко всем ресурсам локальной сети, как и компьютеры, имеющие к ней физическое подключение.
3. *Соединить территориально удаленные локальные сети в одну локальную сеть*. Например, если у некоторой организации есть территориально удаленные офисы, в каждом из которых есть локальная сеть с выходом в городскую сеть или Интернет, то, используя VPN, можно логически объединить эти сети — сделать так, чтобы доступ к компьютерам одного офиса с компьютеров другого офиса логически ничем не отличался от «обычного» доступа в рамках одного физического сегмента локальной сети. Независимо от того, в каком месте расположены ресурсы такой сети, работа с ними будет производиться единообразно независимо от того, из какого офиса соответствующие ресурсы запрашиваются.

Пример объединения удаленных компьютеров в единую сеть VPN приводится на рисунке 3.4.1. В данном случае предполагается, что две локальные сети, а также отдельный компьютер территориально разделены и имеют независимое подключение к Интернету. При помощи VPN данные компьютеры объединены в единую виртуальную частную сеть. Логическое взаимодействие между всеми компьютерами осуществляется так же, как и в случае их физического соединения в единую сеть.

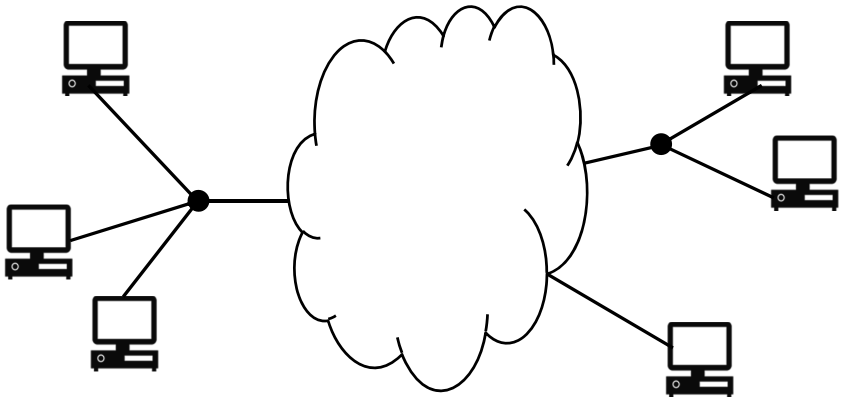


Рис. 3.4.1. Пример объединения удаленных компьютеров в единую виртуальную сеть

Технологии VPN предполагают, что при настройке соединения одна сторона должна выполнять роль сервера, а вторая — клиента. В качестве сервера можно использовать Windows Server, Linux, FreeBSD или аппаратный маршрутизатор с поддержкой VPN. Роль клиента может быть возложена на более широкий класс операционных систем и устройств: это вполне может быть какая-то клиентская версия Windows или недорогой аппаратный маршрутизатор.

Существует большое количество протоколов, реализующих технологии VPN. Наиболее популярными являются протоколы PPPoE и PPTP, реализованные в Windows. Первый протокол обеспечивает соединение «точка — точка» через сеть Ethernet (PPPoE — Point-to-Point Protocol over Ethernet). Второй — соединение «точка — точка» через IP-сеть (PPTP — Point-to-Point Tunneling Protocol).

Самое заметное отличие данных протоколов заключается в том, что PPPoE не требует указания адреса и каких-либо настроек VPN-сервера (этот сервер должен располагаться в одном сегменте Ethernet вместе с клиентом, в результате чего не возникает проблем с автоматическим поиском данного сервера). Протокол PPTP требует указания IP-адреса VPN-сервера и может подключаться к такому серверу через какие-либо промежуточные узлы (требуется прямое подключение на основе маршрутизации).

Большую популярность имеет независимая свободная реализация – OpenVPN. Эта версия протокола обеспечивает как подключение в режиме маршрутизации («точка — точка»), так и подключение в

режиме моста. При этом, в отличие от протокола PPTP, подключение может работать даже тогда, когда клиент имеет доступ к VPN-серверу через NAT.

Для использования OpenVPN требуется устанавливать специальное программное обеспечение, которое доступно для большинства операционных систем.

3.5. Утилиты стека протоколов TCP/IP

В данном разделе приводится краткое описание некоторых утилит командной строки, предназначенных для получения информации, проверки работоспособности и настройки компьютерных сетей.

ipconfig

Утилита Windows для просмотра и обновления информации о сетевых подключениях. В кратком формате (ipconfig) выводит информацию об адресе, маске и основном шлюзе компьютера. В полном формате (ipconfig /all) отображаются подробные сведения обо всех сетевых подключениях.

ifconfig

Команда UNIX и UNIX-подобных операционных систем (Linux, FreeBSD и др.) для просмотра конфигурации и настройки сетевых интерфейсов. Можно сказать, что это аналог утилиты ipconfig, за тем существенным исключением, что утилита ifconfig позволяет не только просматривать, но и настраивать параметры сетевых подключений.

ping

Утилита для проверки соединений в сетях TCP/IP. Принцип работы заключается в том, что утилита отправляет на указанный узел несколько небольших тестовых пакетов и выводит информацию о том, в какой срок были получены ответы.

Пример работы утилиты ping приводится ниже:

```
C:\>ping yandex.ru

Обмен пакетами с yandex.ru [87.250.250.8] с 32 байтами данных:
Ответ от 87.250.250.8: число байт=32 время=24мс TTL=54
Ответ от 87.250.250.8: число байт=32 время=24мс TTL=54
Ответ от 87.250.250.8: число байт=32 время=24мс TTL=54
Ответ от 87.250.250.8: число байт=32 время=24мс TTL=54

Статистика Ping для 87.250.250.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 24 мсек, Максимальное = 24 мсек, Среднее = 24 мсек
```

Утилита ping позволяет провести первичную диагностику компьютера и компьютерной сети в случае, когда с передачей данных наблюдаются какие-либо проблемы. При анализе ответа утилиты ping можно выявить следующее:

1) удалось ли вашему компьютеру получить IP-адрес того ресурса, который был запрошен? Если адрес получен не был, то у вас имеются проблемы с настройкой (или работоспособностью) службы DNS;
2) удалось ли утилите отправить пакеты данных на указанный адрес? Если не удалось (no route to host), то на вашем компьютере имеются проблемы с настройкой шлюза по умолчанию или таблицы маршрутизации;
3) получены ли ответы на отправленные пакеты? Если утилита сообщает о 100% потерь, то компьютер, к которому вы обращаетесь, защищен межсетевым экраном или недоступен (проблема с самим компьютером или с каким-либо оборудованием, через которое должны передаваться данные, — более точную диагностику можно провести при помощи утилиты tracert);
4) есть ли потери в полученных ответах? Если утилита сообщает о потери части пакетов (или время получения ответов нестабильно), то это свидетельствует о каких-либо перебоях сетевого оборудования, внешних помехах или об очень сильной загрузке компьютерной сети.

tracert (traceroute)

Утилита tracert (traceroute — для UNIX-систем) предназначена для определения маршрутов следования данных в сетях TCP/IP. В отличие от

утилиты ping, в данном случае отображается не только факт доступности запрашиваемого узла, но и информация по всем узлам маршрута следования пакета.

Пример работы утилиты tracert представлен ниже:

```
C:\>tracert yandex.ru

Трассировка маршрута к yandex.ru [87.250.250.8]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  192.168.0.1
  2     8 ms    25 ms    <1 мс  10.93.255.126
  3    <1 мс    <1 мс    <1 мс  lag-7-435.voronezh.ertelecom.ru [88.87.67.34]
  4    23 ms    23 ms    23 ms  net131.ertelecom.ru [188.234.131.104]
  5    23 ms    23 ms    24 ms  net131.ertelecom.ru [188.234.131.105]
  6     *        *        *     Превышен интервал ожидания для запроса.
  7    25 ms    25 ms    26 ms  87.250.239.62
  8    25 ms    25 ms    25 ms  myt-p2-be2.yndx.net [87.250.239.73]
  9    25 ms    24 ms    25 ms  myt6-c1-ae1.yndx.net [87.250.239.143]
 10    24 ms    24 ms    24 ms  rusearch.yandex.com [87.250.250.8]

Трассировка завершена.
```

Для каждого промежуточного узла указывается его доменное имя (если это удается определить), а также время следования пакета к данному узлу.

Если в сети существуют проблемы, то утилита tracert поможет узнать, на каком именно шаге обрывается передача информации, либо она позволит вам понять, что какой-то из узлов вашей сети отправляет данные не на тот шлюз.

Обратите также внимание, что некоторые узлы не сообщают о себе информации (в приведенном примере узел 6). В случае когда трассировка завершается успехом, такое поведение компьютеров говорит не о наличии проблем, а о том, что данный конкретный узел защищен таким образом межсетевым экраном.

Утилиты ping и tracert можно использовать не только в локальном режиме (запуская на компьютерах, к которым у вас есть прямой доступ). Иногда возникает необходимость запуска этих утилит на каких-либо внешних узлах для проверки доступности вашего сервера из сети Интернет. В этом случае можно воспользоваться некоторым интернет-сервисом сетевых утилит. Найти такие сервисы достаточно легко по запросу *«сетевые утилиты онлайн»* в любой поисковой системе.

route

Утилита route позволяет просматривать, удалять и добавлять статические маршруты в таблицу маршрутизации. В Windows просмотр маршрутов осуществляется при помощи вызова этой утилиты с ключом print, добавление и удаление – с ключами add и delete.

Пример полной таблицы маршрутизации, сформированной утилитой route, приводится ниже:

```
C:\>route print
===========================================================================
Список интерфейсов
 10...00 25 22 86 e1 38 ......Сетевая карта Realtek RTL8168D/8111D
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 таблица маршрута
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.100     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.0.0    255.255.255.0         On-link     192.168.0.100    266
    192.168.0.100  255.255.255.255         On-link     192.168.0.100    266
    192.168.0.255  255.255.255.255         On-link     192.168.0.100    266
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     192.168.0.100    266
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     192.168.0.100    266
===========================================================================
Постоянные маршруты:
  Отсутствует
```

Обратите внимание, что утилита сообщает об отсутствии постоянных маршрутов. Все маршруты, добавляемые вами при помощи route add, добавляются в таблицу лишь до первой перезагрузки компьютера. Если требуется добавить постоянный маршрут (он сохранится и после перезагрузки), то используйте ключ -p. Например:

```
route -p add 10.2.0.0 mask 255.255.0.0 10.2.0.1
```

nslookup

Утилита, позволяющая в режиме командной строки отправлять обращения к серверам DNS и получать от них самую разнообразную информацию. Эта информация может быть получена как с серверов DNS, указанных по умолчанию, так и с тех серверов, которые указывает сам пользователь.

Пример простого запроса к DNS при помощи утилиты nslookup приводится ниже:

```
C:\>nslookup
Сервер по умолчанию:  UnKnown
Address:  192.168.0.1

> yandex.ru
Сервер:  UnKnown
Address:  192.168.0.1

Не заслуживающий доверия ответ:
Имя:     yandex.ru
Addresses:  2a02:6b8::11
          87.250.250.8
          77.88.21.11
          87.250.251.11
          93.158.134.8

> quit
```

Обратите внимание, что утилита отображает все адреса, закрепленные за доменным именем (а не один адрес, как утилита ping). Ответ классифицируется как не заслуживающий доверия (это не ошибка, а просто указание на то, что ответ получен с сервера, который не является хранителем зоны yandex.ru). Для завершения работы с утилитой необходимо указать команду quit.

В данном разделе приведено лишь краткое описание сетевых утилит. Чтобы получить дополнительную информацию и посмотреть примеры, любую из указанных утилит можно вызвать с параметром /? (например, route /?).

Вопросы и задания

Для чего используется служба DHCP? Опишите 4 этапа назначения адреса при помощи DHCP.

Какие существуют варианты автоматического назначения адреса в сетях IPv6? Требуется ли в таких сетях применение DHCP?

Назовите три способа подключения локальной сети к Интернету. В чем их достоинства и недостатки?

Что такое межсетевой экран? Каким образом межсетевой экран позволяет осуществлять контроль и блокирование трафика?

Что такое виртуальные частные сети? Какие задачи позволяет решить данная технология?

Назовите основные утилиты стека протоколов TCP/IP, опишите их предназначение. Приведите примеры использования утилит для настройки и диагностики сети.

Раздел 4. Сетевые службы Интернета

Поскольку современные локальные сети строятся на основе стека протоколов TCP/IP, то в локальных сетях существует возможность создания сетевых служб, ранее реализованных для Интернета. К таким службам, востребованным в локальных сетях, следует отнести DNS, электронную почту, веб и др. В данном разделе рассматриваются указанные и некоторые другие службы. Освоение предлагаемого материала позволит вам создавать локальные сети, в которых будут представлены собственные сервисы и ресурсы сети Интернет.

4.1. Служба DNS

Как уже было сказано выше, в сетях TCP/IP наряду с числовой адресацией используется и символьный способ именования узлов. С каждым символьным (доменным) именем связывается IP-адрес (или несколько адресов), а с каждым IP-адресом, в свою очередь, может быть связано доменное имя (или несколько доменных имен).

Как хранится информация о соответствии имен и адресов? Каким образом узлы компьютерной сети могут получать эту информацию?

Первый способ реализации системы доменных имен был основан на использовании файлов *hosts* — текстовых файлов, где хранятся пары соответствий адресов и имен. Предполагалось, что такие файлы должны храниться и регулярно обновляться на всех узлах компьютерной сети.

Очевидно, что этот способ сейчас является устаревшим, так как в современных условиях уже невозможно на каждом компьютере хранить и регулярно обновлять всю информацию обо всех других компьютерах Интернета. Вместе с тем файлы hosts до сих пор используются в большинстве операционных систем — для уточнения информации, хранящейся на серверах DNS. Например, в таких файлах определяется имя сетевой петли — localhost. Типичный пример файла hosts для операционной системы Windows приводится ниже:

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# Это образец файла HOSTS, используемый Microsoft TCP/IP для Windows.
#
# Этот файл содержит сопоставления IP-адресов именам узлов.
# Каждый элемент должен располагаться в отдельной строке. IP-адрес должен
```

```
# находиться в первом столбце, за ним должно следовать соответствующее имя.
# IP-адрес и имя узла должны разделяться хотя бы одним пробелом.
#
# Кроме того, в некоторых строках могут быть вставлены комментарии
# (такие, как эта строка), они должны следовать за именем узла и отделяться
# от него символом '#'.
#
# Например:
#
#      102.54.94.97     rhino.acme.com          # исходный сервер
#       38.25.63.10     x.acme.com              # узел клиента x

127.0.0.1       localhost
```

Информация в файле hosts имеет приоритет над информацией из DNS, что, в свою очередь, создает возможности злонамеренного сопоставления IP-адресов и доменных имен. Различные вредоносные программы могут менять файл hosts, записывая туда строки с новыми адресами для различных интернет-сайтов (почтовых служб, социальных сетей и др.).

Пользователь, обратившийся к такому сайту, получает доступ не к настоящему ресурсу, а к его подставной копии, которая внешне может быть очень похожей на настоящий сайт. Введя свой пароль к настоящему ресурсу, пользователь этот пароль теряет, так как он становится известен злоумышленникам.

Такой вид атаки, к сожалению, достаточно распространен. Если есть подозрение, что ваш компьютер был подобным образом атакован, проверьте файл hosts, удалите лишние строки. Контроль изменений файла hosts осуществляют и многие антивирусные программы, этот контроль позволяет предотвратить похищение паролей.

Второй способ реализации системы доменных имен основан на использовании *службы DNS*, представляющей собой распределенную систему, в которой информация о доменах хранится на большом количестве связанных между собой DNS-серверов.

Если про особенности технической реализации службы DNS говорить кратко, то надо сказать, что данная служба базируется на множестве серверов, каждый из которых хранит информацию только о своей зоне, все серверы связаны между собой и позволяют получать необходимую информацию всей системы DNS-серверов. Служба DNS устроена так, что точка подключения к ней не имеет значения, — вы должны получать одинаковые ответы вне зависимости от того, к какому серверу обратились.

Если разбираться в технической реализации DNS более подробно, то надо ответить на следующие вопросы.

1. Что такое зона DNS, как соотносятся зоны, домены и серверы DNS?
2. Как связаны между собой отдельные серверы DNS?
3. Каким образом происходит поиск ответа при обращении клиента к службе DNS?
4. Какая информация о зонах DNS хранится на серверах?
5. В чем особенности прямого и обратного преобразования имен и адресов?

Домены, зоны и серверы DNS

DNS – это служба *доменных* имен, она предполагает, что все компьютеры в сети разделяются на логические группы — *домены*. При этом доменные имена образуют иерархическую структуру, так как одни домены могут являться частью других. В этой связи выделяют домены первого уровня, второго и т. д.

Подобно тому, как файлы на жестком диске объединяются в папки, отдельные компьютеры в сети объединяются в домены. Одни папки могут содержать другие — такое же правило справедливо и для доменов. Полное имя компьютера (равно как и полное имя файла) будет содержать перечисление всех доменов (для файла — папок), в которые компьютер входит.

Например, адрес **server.fizmat.vspu.ru** следует понимать так: «это компьютер **server**, который находится в домене **fizmat**, который находится в домене **vspu**, который находится в домене **ru**».

Можно также говорить, что компьютер **server** расположен в домене **fizmat.vspu.ru**. Сам такой домен называется доменом третьего уровня и он, в свою очередь, является частью домена второго уровня **vspu.ru**.

Зона DNS — это часть пространства имен DNS, размещаемая как единое целое на определенном сервере. Каждая зона представляет собой дерево, которое является дочерним по отношению к той зоне, частью которой она является (рис. 4.1.1).

Выделение зон является основным механизмом для передачи ответственности (делегирования полномочий) за соответствующую часть домена другому лицу или организации. Именно этот механизм позволяет

разделить все пространство доменных имен на части, обслуживаемые разными DNS-серверами.

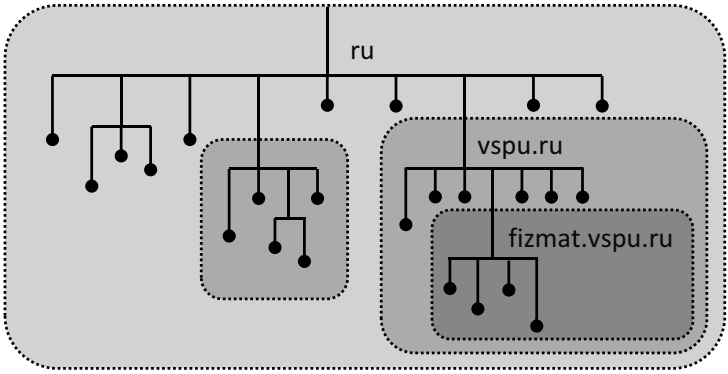


Рис. 4.1.1. Пример выделения зон в пространстве имен DNS

Таким образом, каждый DNS-сервер хранит только часть информации DNS – информацию о своих зонах. Перечень поддерживаемых зон на каждом конкретном DNS-сервере определяется соответствующими записями на DNS-серверах родительских зон (подробнее об этом будет сказано ниже). Администратор настраивает сервер в соответствии с его ролью в общей системе DNS (включает поддержку соответствующих зон, добавляет в файлы зон необходимую информацию).

Заметим также, что для каждой зоны в целях обеспечения качества обслуживания рекомендуется создавать как минимум два DNS-сервера. Один из таких серверов должен быть основным (master), а все остальные — вспомогательными (slave) серверами DNS. Основной сервер от вспомогательных отличается тем, что только через этот сервер производится обновление записей DNS. Вспомогательные серверы лишь копируют весь файл зоны для того, чтобы они, как и основной сервер, могли давать ответы на поступающие запросы. Обновление информации DNS через вспомогательные серверы не предусмотрено.

Связь серверов DNS

Серверы DNS, образуя иерархическую структуру, имеют связи двух типов.

Первый тип связей — это прямые связи на уровне информации, хранящейся в DNS. В записях каждой зоны хранится информация о серверах дочерних зон, лежащих на ступеньку ниже по отношению к текущей.

Например, если в структуре доменных имен есть зоны vspu.ru и fizmat.vspu.ru, обслуживаемые разными DNS-серверами, то это означает, что на сервере зоны vspu.ru хранится запись о сервере зоны fizmat.vspu.ru. В свою очередь, для сервера зоны vspu.ru есть запись на сервере зоны ru.

Именно такие записи обеспечивают целостность информационной базы службы DNS, ее иерархическую структуру. Когда некоторый клиент обращается к DNS с запросом на получение IP-адреса компьютера server.fizmat.vspu.ru, то сначала выясняется адрес сервера для зоны ru, затем — для зоны vspu.ru, через него — для fizmat.vspu.ru, и только после этого (после получения адреса DNS-сервера, на котором хранится информация зоны fizmat.vspu.ru) выясняется и адрес компьютера server.fizmat.vspu.ru.

Из приведенного выше описания становится понятным, что для полноценной настройки зоны fizmat.vspu.ru требуется настройка нужных записей и в зоне vspu.ru. Это означает, что произвольно (по своему желанию) в Интернете просто технически невозможно создавать новые зоны — новые уровни доменных имен. Всегда требуется согласие владельца (администратора) вышестоящей зоны.

Созданием и поддержанием новых имен в доменах верхнего уровня (ru, com, org и многих других) занимаются специальные компании — регистраторы доменных имен. В нашей стране крупнейшим регистратором имен является компания RU-CENTER.

Сами домены верхнего уровня создаются и поддерживаются на уровне корневого домена — этим занимается международная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers — интернет-корпорация по управлению именами и IP-адресами).

Второй тип связей — это обратные связи на уровне настроек серверов DNS. Каждый сервер для получения информации из DNS, которой он не обладает, должен «уметь» обратиться к некоторому вышестоящему серверу, который предоставит необходимый ответ. При этом совсем необязательно это должен быть сервер вышестоящей зоны — чаще всего прямые и обратные связи не совпадают, т.к. для обратных связей обычно выбирается сервер, который находится на наиболее «близком» расстоянии (например, сервер провайдера – поставщика услуг).

Если специальный сервер для пересылки не указывается совсем, то распознавание имен начинается с обращения к некоторому корневому

серверу. Адреса корневых серверов указаны в настройках всех DNS-серверов.

Существуют 13 корневых серверов DNS, которые именуются буквами от A до M и относятся к домену root-servers.org. Данные серверы находятся в разных странах, управляются различными организациями, действующими по согласованию с ICANN.

Указанное количество серверов определяется ограничениями, которые накладывались на размеры DNS-пакета. Однако у многих корневых серверов DNS существуют зеркала, в результате чего за 13 именами скрывается более 200 физических серверов.

Процесс распознавания имени в DNS

Итак, служба DNS основана на множестве серверов, каждый из которых содержит информацию о своей зоне и имеет связи с другими серверами DNS. Пользователь может обратиться к любому серверу DNS, чтобы получить информацию. Как происходит поиск ответа по запросу пользователя на распознавание доменных имен?

Принцип поиска ответа сервером DNS можно описать следующим образом: «либо я сам знаю ответ, либо не знаю, но знаю, к кому обратиться дальше».

Если на сервере DNS хранится та информация, которую запрашивает пользователь, то эта информация и сообщается в качестве ответа. Такие ответы называются авторитетными (authoritative response). Заметим, что авторитетными будут ответы как основного (master), так и всех вспомогательных (slave) DNS-серверов, на которых хранится информация о зоне.

Если сервер DNS не содержит информацию о зоне, в которой хранится запись ресурса, для которого надо получить ответ, то в этом случае надо обратиться к внешнему серверу, который «приблизит» процесс распознавания имени к нужному результату. Выбор такого внешнего сервера будет осуществляться одним из двух вариантов:

1) если запрашиваемый ресурс входит в дочернюю зону по отношению к тем зонам, которые обслуживает сервер DNS, то выбор следующего сервера будет осуществляться на основе связей первого типа – прямых связей на основе информации о серверах дочерних зон. Например, если обратиться к серверу зоны vspu.ru с запросом об адресе компьютера server.fizmat.vspu.ru, то в качестве

следующего DNS-сервера будет предложен адрес машины с информацией о зоне fizmat.vspu.ru. Очевидно, что на этом сервере будет храниться запрашиваемая информация. Если изначально обратиться к серверу зоны ru, то сначала будет определен адрес сервера зоны vspu.ru, а затем — и fizmat.vspu.ru;

2) если запрашиваемый ресурс не входит в дочерние зоны DNS, то следующий сервер будет определен на основе связей второго типа – обратных связей на основе информации о вышестоящих серверах. Например, если обратиться к серверу, содержащему информацию о зоне vspu.ru с запросом об адресе сервера yandex.ru, то в качестве следующего DNS-сервера будет выбран сервер интернет-провайдера либо некоторый корневой сервер DNS. В итоге, получив доступ к корневому серверу (напрямую либо через провайдера), вы получите информацию по своему запросу, что будет сделано на основе процедуры, описанной в п. 1.

Заметим, что мы пока рассмотрели только процесс выбора внешнего сервера, но не обращения к нему. Такое обращение тоже реализуется двумя способами — на основе нерекурсивной или рекурсивной процедуры.

Нерекурсивная (non-recursive) процедура — это способ получения информации из DNS, при котором сервер, к которому вы обращаетесь, сообщает вам не искомый ответ, а адрес следующего сервера, к которому надо обратиться.

Рекурсивная (recursive) процедура, в свою очередь, предполагает, что все последующие запросы делает сам сервер DNS и клиенту в итоге сообщается сам искомый ответ.

Как правило, на практике используется рекурсивная процедура, являющаяся более простой для сетевых пользователей, так как серверы DNS сами запрашивают недостающую информацию и сообщают пользователю конечный ответ. Однако такие ответы, полученные через другие серверы, отмечаются как неавторитетные (non authoritative response, не заслуживающие доверия). Нерекурсивная процедура, реализованная в полном объеме, всегда позволяет получить авторитетный ответ. При правильной настройке службы DNS авторитетные и неавторитетные ответы совпадают, поэтому упрощение процедуры распознавания имен для пользователей компьютерной сети не приводит к недопустимо высоким рискам получения недостоверной информации.

Еще одно существенное замечание, касающееся процедуры получения информации из DNS, касается того факта, что, как правило, DNS-серверы являются *кеширующими*, т.е. они способны запоминать информацию, пересылаемую пользователям. Кеширование информации на серверах DNS позволяет значительно снизить нагрузку на всю службу в целом, так как полученная информация повторно не запрашивается. Если некоторый сервер искомую информацию содержит в своем кеше, то он сразу даст ответ, не обращаясь к другим серверам.

Обратной стороной кеширования являются задержки распространения информации в случае ее обновления. В частности, когда у некоторого ресурса меняется IP-адрес, то служба DNS в течение какого-то времени может сообщать пользователям старую информацию, актуальную до обновлений.

Время хранения информации о зоне в кеш-памяти сервера DNS определяется администратором зоны (это один из параметров описания зоны). Как правило, такое время исчисляется часами либо каким-то небольшим количеством дней.

Ресурсные записи DNS

В этом разделе более подробно рассмотрим вопрос о видах информации, которую может содержать служба DNS о ресурсах компьютерной сети. Единицей хранения информации о ресурсе является *ресурсная запись*, которая содержит информацию соответствия какого-либо имени и служебной информации DNS.

Ресурсная запись состоит из следующих полей:

- *имя* (NAME) — имя, которое может запрашиваться у сервера DNS;
- *время жизни* (TTL) — время хранения записи в кеше DNS;
- *класс* (CLASS) — чаще всего указывается IN (от слова «Internet»), однако может принимать и другие значения, если служба DNS используется в сетях, основанных не на TCP/IP;
- *тип* (TYPE) — формат и назначение записи;
- *данные* (DATA) — информация о ресурсе.

В ресурсной записи могут определяться не все поля. Например, если отсутствует поле NAME, то оно наследуется от предыдущей записи. Если отсутствует поле TTL, то соответствующее значение берется из описания всей зоны.

Различия в описании записей будут также проявляться в поле DATA. Формат и синтаксис оформления этого поля определяются типом записи (значением поля TYPE).

Стандартом DNS определено множество самых разнообразных типов записей. Ниже мы рассмотрим основные из них, наиболее часто используемые на практике.

Запись SOA (Start of Authority — начальная запись зоны) — обязательная запись, которая описывает настройки зоны, определяет зону ответственности сервера DNS. Для каждой зоны должна существовать только одна запись SOA и она должна быть первая.

В поле данных записи SOA указывается имя главного сервера DNS, адрес администратора зоны, серийный номер файла зоны, а также информация о времени обновления зоны. Пример описания записи SOA приводится ниже:

```
fizmat.vspu.ru.     IN SOA  server.fizmat.vspu.ru. admin.fizmat.vspu.ru. (
                            201504181  ; serial
                            3600       ; refresh (1 hour)
                            900        ; retry (15 minutes)
                            604800     ; expire (7 days)
                            3600       ; minimum (1 hour)
                            )
```

Запись NS (Name Server — сервер имен) — указывает на DNS-сервер для некоторой дочерней зоны. Количество записей типа NS должно соответствовать количеству DNS-серверов, обслуживающих зону (включать все такие DNS-серверы). Пример описания записей NS приводится ниже:

```
fizmat.vspu.ru.     NS      ns.vspu.ru.
fizmat.vspu.ru.     NS      ns.fizmat.vspu.ru.
```

Запись NS указывается как для текущей зоны, которую обслуживает сервер DNS, так и для дочерних зон, обслуживаемых внешними серверами. Именно эти записи создают связи первого типа между серверами DNS, которые рассматривались нами ранее.

Запись A (Address Record — запись адреса) — связывает доменное имя с адресом протокола IPv4. Например:

```
server              A       88.87.74.18
```

```
ns                  A       88.87.74.19
www                 A       88.87.74.20
```

Запись AAAA (IPv6 address record) — аналог записи типа A, но для протокола IPv6. Например:

```
server              AAAA    2001:0db8::2a5e:04a0:321d
```

Обратите внимание, что в приведенных примерах в одних случаях в конце указываемых имен стоит точка (например, при указании имени fizmat.vspu.ru), а в других случаях (server, ns, www) точка отсутствует. Это не случайно и не ошибка — точка в конце адреса указывает, что адрес записан полностью. Если точка не стоит, то используется сокращенное имя ресурса. Полное имя будет определяться областью, для которой указаны эти краткие имена (в данном примере полные имена ресурсов — server.fizmat.vspu.ru, ns.fizmat.vspu.ru и www.fizmat.vspu.ru).

Запись CNAME (Canonical Name Record — каноническая запись имени) — используется для указания псевдонима (алиаса) ресурса (для перенаправления на реальное имя). В приведенном ниже примере описывается ресурс mail.fizmat.vspu.ru, который получает тот же адрес, что и server.fizmat.vspu.ru

```
mail                CNAME       server.fizmat.vspu.ru.
```

Запись MX (Mail Exchange — почтовый обменник) — указывает серверы доставки почты для домена. Таких серверов может быть несколько и при их описании указывается приоритет доставки (почта отправляется на сервер с наименьшим числом приоритета, и лишь в случае неудачи выбирается сервер с более высоким значением этого числа).

В приведенном ниже примере определяются два сервера для доставки почты на адреса вида имя@fizmat.vspu.ru. Почта всегда сначала будет отправляться на сервер mail.fizmat.vspu.ru, и лишь в случае возникновения проблем – на вспомогательный сервер mail.vspu.ru.

```
fizmat.vspu.ru.     MX      10 mail.fizmat.vspu.ru.
fizmat.vspu.ru.     MX      20 mail.vspu.ru.
```

Запись SRV (Server Selection — выбор сервера) — указывает на серверы, обеспечивающие работу тех или иных служб (например, Active

Directory, Jabber или др.). В описании записи, помимо указания имени сервера, определяется приоритет и вес для выбора сервера (в том случае, когда их указано несколько), а также порт, на котором работает необходимая служба. В приведенном ниже примере описывается сервер, на котором хранится глобальный каталог службы Active Directory:

```
gc                  SRV     0 100 3268 server.fizmat.vspu.ru.
```

Запись PTR (Pointer — указатель) — связывает IP-адрес хоста с его символьным именем. Этот тип записей используется в обратных зонах DNS для преобразования IP-адресов в доменные имена. Подробнее о таких преобразованиях будет сказано ниже.

Отдельный вопрос организации хранения информации в DNS связан с использованием имен сетевых ресурсов в национальных кодировках, например в доменной зоне рф. Так как стандартом DNS разрешено использование символов только латинского алфавита, для хранения национальных символов используется специальная кодировка — *Punycode* (произносится как пьюникод).

Данная кодировка преобразует национальные символы в последовательности знаков, разрешенных в DNS. Например, адрес **яндекс.рф** записывается в punicode как **xn--d1acpjx3f.xn--p1ai**. Именно эта последовательность символов отправляется в DNS для того, чтобы получить IP-адрес ресурса. Такое преобразование делает браузер и оно не заметно для пользователя.

Прямое и обратное преобразование DNS

Как правило, DNS используется для преобразования доменных имен в IP-адреса, что называется *прямым* преобразованием. Вместе с тем иногда требуется выполнить и обратный процесс — по известному IP-адресу получить доменное имя ресурса. Такое преобразование называется обратным. Чтобы обеспечить возможность выполнения такой процедуры, в DNS используются обратные зоны, которые создаются и настраиваются независимо от прямых.

Для обратных зон используется специальный домен — in-addr.arpa, который делится на поддомены в соответствии с используемыми адресами. Например, если надо описать имена компьютеров для сети, имеющей адреса

вида 88.87.74.x, то эти имена описываются как PTR записи зоны 74.87.88.in-addr.arpa. Пример таких записей приводится ниже:

```
18                  A       server.fizmat.vspu.ru.
19                  A       ns.fizmat.vspu.ru.
20                  A       www.fizmat.vspu.ru.
```

Таким образом, если службе DNS приходит запрос на определение символьного имени компьютера с адресом 88.87.74.20, то этот запрос выполняется как поиск описания ресурса 20 в домене 74.87.88.in-addr.arpa.

Обратное преобразование требуется производить гораздо реже, чем прямое. Обратные зоны могут быть описаны не всегда, а имеющаяся в них информация может не соответствовать той информации, которая хранится в прямых зонах. В большинстве случаев, если вы лишь пользуетесь сервисами Интернета, такая ситуация проблем создавать не будет.

Однако все же существуют случаи, когда настройка обратного преобразования является исключительно важной. Например, это необходимо делать при создании своего почтового сервера. Если обратное преобразование адреса вашего почтового сервера не будет соответствовать прямому, то отправляемые вам письма другими почтовыми серверами с очень большой вероятностью будут отмечаться как спам. Чтобы этого не происходило, обратитесь к вашему провайдеру с просьбой описать правильные имена для адреса почтового сервера в обратной зоне.

Завершая раздел о технической реализации службы DNS, скажем, что эта служба представляет собой достаточно сложную и развитую систему, обеспечивающую взаимное преобразование доменных имен и IP-адресов, а также получение самой разнообразной информации о сетевых ресурсах. Служба DNS создавалась для Интернета, но в настоящее время используется и в локальных сетях, основанных на TCP/IP. В частности, DNS является одной из основных служб доменов Windows (Active Directory), без ее установки и настройки локальная сеть на основе домена Windows работать не будет, даже если выход в Интернет не предусмотрен.

Для того чтобы службу DNS можно было использовать в доменах Windows, в первоначальный стандарт этой службы были внесены некоторые изменения: добавлен тип записей SRV, введена технология динамического обновления записей (динамический DNS —

автоматическая регистрация рабочих станций в DNS), разрешено использовать символ «_» в именах ресурсов.

Для создания сервера DNS можно использовать компьютер под управлением Windows Server, Linux или FreeBSD. В Windows используется специальная служба DNS-сервера, в Linux и FreeBSD, как правило, для создания DNS-сервера используется программный пакет BIND.

Создание и настройка DNS-сервера заключаются в установке необходимого программного обеспечения, настройке общих параметров сервера (перечень поддерживаемых зон, адрес сервера для пересылки и др.), а также в описании собственно файлов зон, для которых создаваемый сервер является основным. Напомним также, если ваша зона должна стать частью систем имен Интернета, то NS-запись о вашем сервере должен сделать и администратор сервера вышестоящей зоны.

4.2. Электронная почта

Служба электронной почты относится к одной из старейших служб Интернета. Данная служба позволяет обмениваться текстовыми сообщениями между компьютерами, подключенными к единой сети. Важно, что такой обмен производится в асинхронном режиме — отправитель и получатель сообщения не обязаны находиться за своими компьютерами одновременно.

Традиционный подход к работе с электронной почтой предполагает использование специальных почтовых клиентов — таких программ, как Outlook Express, The Bat!, Mozilla Thunderbird и др. *Почтовый клиент* (*почтовая программа*, *клиент электронной почты*) — это программное обеспечение, устанавливаемое на компьютере пользователя и предназначенное для получения, хранения, подготовки и отправки сообщений электронной почты одного или нескольких пользователей. Почтовые программы позволяют успешно пользоваться электронной почтой в условиях низкоскоростных и нестабильных каналов связи, в отсутствие постоянного подключения к Интернету.

В современных условиях, когда наличие скоростного и постоянного доступа к Интернету не является большой проблемой, более высокой популярностью пользуется подход работы с электронной почтой при помощи специализированных веб-служб (Gmail, Яндекс.Почта и др.). В этом случае все операции с электронными письмами осуществляются на сайте веб-

службы электронной почты, для чего используется браузер. Почтовый клиент, таким образом, выполнен в виде веб-приложения, что снимает проблемы установки и настройки дополнительного программного обеспечения, позволяет работать со своей почтой на любом электронном устройстве (компьютере, планшете, смартфоне), подключенном к сети Интернет.

Следует отметить, что традиционная и веб-почта являются частью одной системы электронной почты Интернета. Пользователи могут обмениваться электронными сообщениями независимо от того, какой подход к работе с электронной почтой использует каждый из них.

Для работы с электронной почтой требуется регистрация на одном из почтовых серверов. В процессе регистрации пользователю назначается электронный адрес, который записывается как name@domain.com. В такой записи name — это имя пользователя электронной почты, а domain.com — домен, в котором пользователь зарегистрирован.

В настоящее время чаще всего используются личные адреса, полученные при регистрации в какой-либо веб-службе Интернета, а также служебные адреса, назначенные пользователю для деловой переписки в различных организациях.

Общее описание системы электронной почты

Техническую основу электронной почты в Интернете составляет система связанных между собой почтовых серверов, каждый из которых может обслуживать множество пользователей, принимая для них сообщения, а также пересылая сообщения во внешнюю сеть. Работа электронной почты основывается на протоколах SMTP, POP3, IMAP, а также тесно связана со службой DNS. Одна из наиболее простых схем пересылки электронных писем представлена на рисунке 4.2.1.

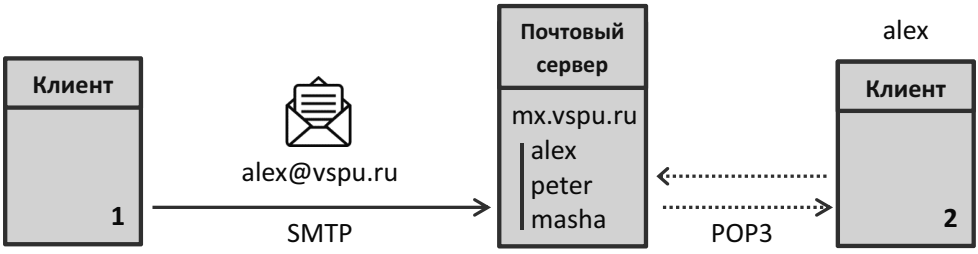


Рис. 4.2.1. Схема работы электронной почты

Как видно из рисунка, центральным звеном системы передачи электронных писем является почтовый сервер. *Почтовый сервер* (*агент пересылки сообщений*, *mail transfer agent*, *MTA*) — это компьютер, который принимает электронную почту от пользователей и других серверов, осуществляет ее обработку в соответствии с заданными правилами (производит дальнейшую пересылку или сохраняет в почтовых ящиках пользователей). Пользователи могут обращаться к почтовому серверу, чтобы получить доступ к адресованной для них корреспонденции.

Процесс отправки и получения электронных писем в соответствии с приведенной схемой выглядит следующим образом.

1. Некоторый пользователь Интернета на компьютере 1 в своей почтовой программе готовит электронное письмо для пользователя с адресом alex@vspu.ru.
2. В момент отправки электронного письма почтовая программа обращается к службе DNS и получает информацию, что почтовым сервером для домена vspu.ru является компьютер mx.vspu.ru.
3. Почтовая программа отправителя устанавливает соединение с почтовым сервером mx.vspu.ru и пересылает электронное письмо, указывая, что оно предназначено для пользователя alex@vspu.ru. Установка соединения и отправка электронного письма осуществляются с использованием протокола SMTP.
4. Почтовый сервер получает электронное письмо и сохраняет его в виде текста в почтовом ящике пользователя alex.
5. Пользователь alex в удобное для себя время обращается к почтовому серверу, чтобы проверить наличие новой корреспонденции. Такая проверка осуществляется при помощи почтовой программы и с использованием протокола приема данных, например POP3. Если обнаруживается новое письмо, то оно копируется на компьютер пользователя для просмотра и дальнейшей работы.

Рассмотренная схема иллюстрирует *базовые* принципы передачи электронной почты. На практике работа почтовой службы реализуется несколько сложнее — передача электронной почты может производиться с использованием многих почтовых серверов, а в процессе установки соединений и пересылки писем могут проводиться различные дополнительные проверки.

Так, чаще всего будет использоваться схема передачи с двумя почтовыми серверами (рис. 4.2.2).

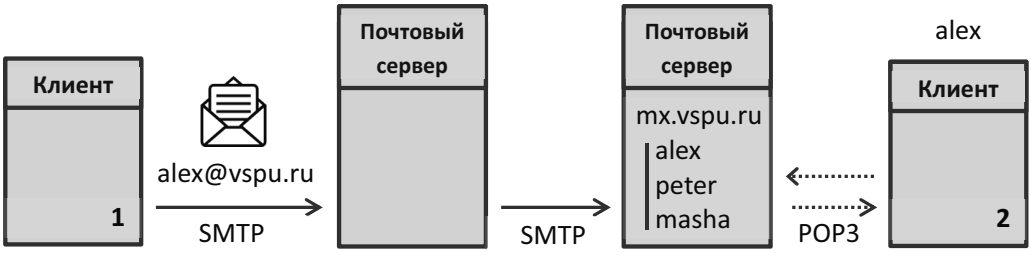


Рис. 4.2.2. Схема передачи электронной почты
с использованием двух почтовых серверов

В этом случае почтовая программа отправителя пересылает электронное письмо не серверу получателя, а «своему» SMTP-серверу, адрес которого указан в настройках почтовой программы. Этот сервер осуществляет поиск сервера получателя и дальнейшую пересылку электронного письма. После второй пересылки письмо оказывается в почтовом ящике получателя, откуда может быть доставлено на компьютер пользователя (с использованием протокола приема, например POP3).

Преимущество доставки электронных писем с использованием двух почтовых серверов заключается в более быстрой и надежной отправке сообщений для пользователя компьютера 1. Проблемы, связанные с поиском почтового сервера получателя, установкой соединения и пересылкой электронного письма, решаются в данном случае почтовым *сервером* отправителя, что экономит время и ресурсы пользователя, повышает доверие к отправляющей стороне.

Более высокая скорость и надежность отправки электронных писем в системе с использованием двух почтовых серверов определяется тем, что, как правило, почтовый сервер отправителя располагается на «близком» расстоянии в локальной сети организации или у поставщика интернет-услуг. Дальнейшая пересылка письма проводится почтовым сервером в автоматическом режиме без участия пользователя. В том числе — почтовый сервер берет на себя заботы сохранения и повторной отправки корреспонденции в случае, если почтовый сервер получателя оказывается временно недоступным.

При пересылке электронной корреспонденции может использоваться и более двух почтовых серверов. Последовательность пересылки определяется настройкой почтового сервера, исходя из структуры компьютерной сети, а также соображений обеспечения качества доставки электронных писем.

Например, организация может поддерживать корпоративный SMTP-сервер для своих сотрудников, осуществляющий отправку корреспонденции на внешние серверы через доверенный почтовый сервер своего провайдера или специального поставщика услуг (рис. 4.2.3). В данном случае для каждого пересылаемого электронного письма будет реализована схема с тремя почтовыми серверами, при которой прием отправляемого письма от пользователя организации будет осуществляться «быстрым» корпоративным сервером, а наиболее сложные вопросы обеспечения качества передачи будут решаться провайдером (поставщиком услуг), способным делать это более эффективно.

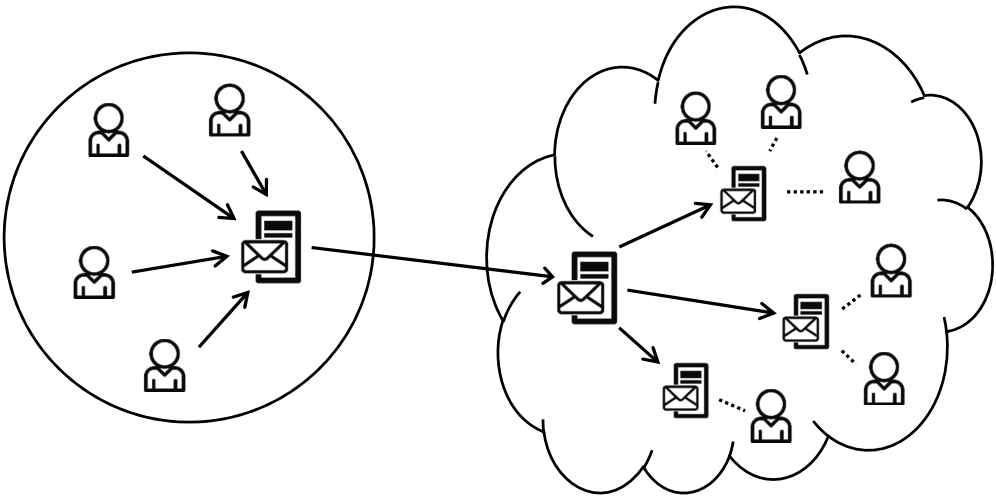


Рис. 4.2.3. Схема передачи электронных писем с использованием корпоративного почтового сервера и сервера провайдера

Несколько почтовых серверов могут назначаться и для получения электронной почты (см. раздел «Техническая реализация службы DNS»). В этом случае, как правило, создается резервный почтовый сервер, который при неполадках основного сервера принимает корреспонденцию пользователей домена для временного хранения и дальнейшей пересылки на основной сервер после восстановления его работоспособности.

Структура сообщения электронной почты

Ранее было упомянуто, что система электронной почты позволяет обмениваться *текстовыми* сообщениями. Это действительно так, несмотря на то что к электронному письму могут быть прикреплены и дополнительные

файлы, такие как текстовые документы, изображения, архивы и др. Сообщение электронной почты представляет собой текстовый файл, который состоит из двух частей — *заголовка* и *тела сообщения*. Ниже приводится пример такого сообщения:

```
To: alligator@mail.ru
Subject: My phone has rung
Return-Path: kornej-chukovskij@gmail.com
From: Kornej Chukovskij <kornej-chukovskij@gmail.com>
Received: by mail-la0-x22e.google.com with SMTP id v1so190124874lag.3
        for <alligator@mail.ru>; Sat, 17 Jan 2015 18:03:28 +0000
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset=UTF-8

Добрый день!

Постой, не тебе ли на прошлой неделе я выслал две пары отличных калош?

16.01.2015, 15:25, "Крокодил" <alligator@mail.ru>:
> Мой милый, хороший, пришли мне калоши, и мне, и жене, и Тотоше.

---
С уважением, Корней Чуковский
```

В заголовке сообщения указывается служебная информация (адреса отправителя и получателя, тема письма, информация о кодировке и др.), а также пометки почтовых серверов, через которые прошло письмо. Каждая строка заголовка начинается со служебного слова (From, To, Subject и др.), двоеточия и соответствующей информации. Заголовок сообщения может содержать только 7-битные символы (кириллица и другие национальные символы, например в теме сообщения, записываются при помощи специальных кодировок).

Тело сообщения отделяется от заголовка пустой строкой и содержит собственно пересылаемый текст. В теле сообщения размещаются и прикрепленные файлы (изображения, архивы и др.), для чего они преобразуются к 7-битному виду при помощи кодировок Base64 или UUE. Двоичные данные, таким образом, записываются текстовыми символами, в результате чего электронные письма могут пересылаться и обрабатываться как простой текст.

Протокол SMTP

SMTP (*Simple Mail Transfer Protocol — простой протокол передачи почты*) — это протокол доставки электронных писем. Как уже было показано выше, на основе этого протокола осуществляется пересылка электронного письма от клиента или промежуточного почтового сервера (сервера пересылки) почтовому серверу получателя. Данный протокол не позволяет «забирать» электронную почту с удаленного сервера — для этого используются протоколы приема данных, такие как POP3 и IMAP.

Согласно протоколу SMTP, процесс передачи электронного письма производится следующим образом.

1. Клиент отправляет почтовому серверу запрос на установку соединения (адрес сервера определяется при помощи службы DNS, запрос отправляется на порт 25).
2. Сервер сообщает о готовности к приему электронной корреспонденции.
3. Клиент передает серверу два адреса — отправителя и получателя электронного письма.
4. Сервер проверяет полученные адреса и в случае успеха дает согласие на пересылку самого электронного письма.
5. Клиент передает электронное письмо и завершает соединение.

Заметим, что на шаге 2 и 4 сервер может отказать в соединении. В первом случае клиент имеет возможность продолжить попытки установки соединения, ожидая готовности сервера. Во втором — причиной отказа чаще всего будет являться ошибка в электронном адресе получателя либо попытка пересылки электронного письма через сервер, который не поддерживает обработку электронных писем для указанных пользователей и адресов. При отказе сервера на шаге 4, таким образом, повторные попытки отправки электронного письма не осуществляются.

Как правило, каждый почтовый сервер обслуживает только «своих» клиентов. Электронное письмо принимается для дальнейшей обработки в случае, если выполняется одно из следующих условий:

1) отправитель сообщения располагается в доверенной сети (ограничение по местоположению) либо подключается к почтовому серверу с указанием данных для аутентификации;
2) электронное письмо адресовано пользователю, который зарегистрирован на почтовом сервере.

Почтовый сервер, который готов принимать электронные письма от любых пользователей и пересылать их дальше для любых других пользователей, называется *открытым релеем* (open relay). Такой почтовый сервер является нежелательным для почтовой службы, так как открывает возможности для массовой рассылки спама (злоумышленник скрывает свое реальное местоположение, а также пользуется «услугой» рассылки многих копий электронного письма для каждого получателя, указанного в оправляемом письме).

Для борьбы со спамом различные службы Интернета ведут черные списки открытых релеев. Если ваш сервер попал в такой список, то с большой вероятностью вся отправляемая с него корреспонденция будет идентифицироваться как спам и блокироваться другими серверами. Для исправления ситуации необходимо правильно настроить почтовый сервер и отправить заявку на удаление вашего адреса из черного списка. Перед удалением из черного списка ваш сервер будет проверен на наличие открытого релея.

Протоколы POP3 и IMAP

Протоколы POP3 и IMAP ориентированы на прием электронной корреспонденции с почтовых серверов.

Протокол *POP3* (*Post Office Protocol — протокол почтового отделения*, *версия 3*) позволяет почтовой программе проверить наличие новых писем на почтовом сервере, скопировать эти письма на личный компьютер пользователя.

IMAP (*Internet Message Access Protocol — протокол доступа к электронной почте Интернета*) – это более сложный протокол, который дает возможность пользователю работать с электронными сообщениями на самом почтовом сервере, не копируя его на какой-то отдельный компьютер пользователя.

Если вы работаете с электронной почтой только на одном компьютере, то вам вполне подойдет протокол POP3. Ваша почтовая программа будет просто копировать новые письма на рабочий компьютер (как правило, удаляя их с сервера), где вы сможете выполнять над ними разнообразные операции (отправлять ответы, распределять по папкам, ставить пометки и др.).

Если вам приходится работать за несколькими компьютерами, например на работе и дома, то письма, полученные (или написанные) на работе, вы не сможете посмотреть дома, и наоборот. В этом случае

лучше подойдет протокол IMAP, который всю корреспонденцию сохраняет на сервере и отображает в вашей почтовой программе независимо от того, с какого компьютера вы подключаетесь к серверу.

Протоколы POP3 и IMAP предполагают обязательную аутентификацию пользователя (в отличие от протокола SMTP, где аутентификация возможна только в современных версиях и обязательной не является). И это не единственные протоколы приема электронных писем, так как в ряде случаев могут использоваться протоколы специализированных почтовых систем (например, Microsoft Exchange, IBM Notes или различных почтовых веб-служб).

Создание и настройка сервера электронной почты

Создание сервера электронной почты возможно на компьютере, имеющем публичный IP-адрес и постоянное подключение к Интернету. Как правило, для этого используется компьютер под управлением Linux или FreeBSD. Настройка почтового сервера возможна и на Windows, однако это чаще всего реализуется в рамках создания более крупных корпоративных систем обмена сообщениями и совместной работы (например, на основе Microsoft Exchange Server).

Для создания полноценного почтового сервера необходимо настроить следующие компоненты.

1. Агент передачи почты (*сервер SMTP*). Этот агент позволит организовать отправку электронной корреспонденции пользователями вашего почтового сервера другим пользователям Интернета, а также прием и хранение электронных писем на адреса ваших пользователей.

В системах Linux и FreeBSD, как правило, такой агент установлен изначально (обычно используется Sendmail), однако он настроен для приема и пересылки электронной корреспонденции лишь в пределах самого компьютера.

Система Sendmail является одним из старейших агентов передачи почты, обеспечивающим чрезвычайно высокие возможности и гибкость настройки почтовых систем. Обратной стороной гибкости и возможностей Sendmail является его довольно сложная настройка, специфический формат конфигурационного файла.

В качестве более современной альтернативы был разработан агент передачи почты Postfix. Считается, что он работает быстрее, требует меньше ресурсов, легче в администрировании и более защищен.

Sendmail и Postfix полностью совместимы друг с другом, распространяются на основе свободной лицензии и позволяют создавать надежные и высокопроизводительные почтовые серверы.

Для того чтобы этот агент мог работать в структуре почтовой системы, необходимо указать области доверенных компьютеров (с которых можно отправлять электронную почту), перечень поддерживаемых доменов, а также, возможно, адреса внешних серверов для пересылки сообщений. На данном шаге важно не допустить ошибку, которая превратит ваш почтовый сервер в открытый релей (т.е. нельзя указывать перечень доверенных компьютеров более широким, чем это фактически требуется).

Отдельным вопросом создания сервера SMTP может стать настройка системы авторизации пользователей. Как выше уже говорилось, протокол SMTP не требует обязательной авторизации, однако это может пригодиться, если пользователям надо предоставить возможность отправки электронных писем не только из локальной сети организации, но и из других точек подключения к Интернету (например, со своего ноутбука при подключении в какой-то внешней сети).

В системах электронной почты используются криптографические протоколы SSL и TLS. Данные протоколы обеспечивают аутентификацию пользователей и шифрование пересылаемой информации. Настройка этих протоколов на почтовом сервере будет заключаться в установке соответствующего программного обеспечения, а также в получении и размещении на сервере необходимых сертификатов.

Если сравнивать протоколы SSL и TLS, то более современным и защищенным является второй протокол — TLS. Помимо почтовых систем, данные протоколы могут использоваться в веб-службах, системах обмена мгновенными сообщениями, IP-телефонии и др.

Сертификаты, которые требуются для настройки этих протоколов, могут быть созданы вами самостоятельно (самоподписанные сертификаты), а также получены от какого-либо центра сертификации.

В первом случае пользователи, подключающиеся к вашему серверу, будут получать вопрос: доверяют ли они самоподписанному сертификату? Этот вопрос не является следствием ошибки в настройке, но он необходим, так как решение о доверии сертификату может принять лишь сам пользователь.

Во втором случае — вопрос доверия к сертификату возникать не будет (доверие подтверждается авторитетной стороной — центром сертификации), но сам такой сертификат, как правило, вы сможете получить для своего сервера лишь на условиях оплаты.

Так как использование защищенного соединения не является обязательным, то для подключения к SMTP-серверу с использованием протокола SSL или TSL требуется также настраивать и почтовый клиент. При настройке указывается желаемый криптографический протокол и соответствующий порт SMTP-сервера, который отличается от стандартного порта (для SSL/TLS используется, как правило, порт 465).

При использовании защищенных соединений следует также внимательно относиться ко времени, которое установлено на вашем компьютере. Если ваше время сильно отличается от времени сервера (например, из-за проблем с батарейкой на системной плате), то установить защищенное соединение не удастся.

2. Сервер POP3 и IMAP. Данный компонент позволит пользователям вашего почтового сервера «забирать» свою электронную корреспонденцию с почтового сервера по одноименным протоколам.

Для создания сервера POP3 и IMAP необходима установка и настройка соответствующего программного обеспечения, для чего могут использоваться такие пакеты, как Courier Mail Server, Cyrus IMAP server, Dovecot или др.

В наиболее простом варианте такой сервер может использовать системы хранения электронной почты и учетных записей пользователей, принятых в операционной системе (в Linux и FreeBSD — в виде простых текстовых файлов). В сложных конфигурациях могут создаваться собственные базы данных, системы виртуальных почтовых аккаунтов и др. Помимо этого, несмотря на обязательную авторизацию пользователей при получении писем как по протоколу POP3, так и IMAP, дополнительно могут использоваться и криптографические протоколы SSL и TLS, что будет обеспечивать безопасную передачу данных авторизации (логина и пароля), а также шифрование пересылаемых писем.

3. Записи почтовой службы в системе DNS. Эти записи необходимы для того, чтобы внешние почтовые агенты могли «находить» почтовый сервер вашего домена. Например, если вы создаете почтовый сервер для домена vspu.ru (т.е. используете адреса вида name@vspu.ru), то в описании

зоны vspu.ru в системе DNS должны быть указаны, например, следующие строки:

```
vspu.ru.     MX     10  mx.vspu.ru.
vspu.ru.     MX     20  mx2.vspu.ru.
```

Указанные записи означают, что вся почта для домена vspu.ru должна направляться на сервер mx.vspu.ru (приоритет 10), а при его недоступности — на сервер mx2.vspu.ru (приоритет 20). Второй сервер в этом случае может временно хранить полученную корреспонденцию для ее последующей отправки на сервер mx.vspu.ru после восстановления работоспособности.

Настройка записей DNS при создании почтового сервера должна производиться и в отношении *обратных записей* для IP-адреса вашего сервера. Обычно такое описание можно сделать лишь на стороне провайдера (поставщика услуг Интернета), но, несмотря на организационные сложности, этой настройкой пренебрегать нельзя.

Правило настройки следующее: запрос в службу DNS на получение доменного имени по IP-адресу вашего почтового сервера должен возвращать осмысленное имя, которое соответствует MX-имени вашего почтового сервера. Например, если запрос адреса для доменного имени mx.vspu.ru возвращает значение 88.87.74.18, то обратный запрос доменного имени для адреса 88.87.74.18 должен (в идеальном варианте) вернуть значение mx.vspu.ru.

Подобную проверку IP-адреса осуществляет большинство почтовых серверов при получении электронного письма. Если обратный запрос не возвращает ответа или в качестве ответа сообщается некоторое техническое значение доменного имени (например, host-88-87-74-18.domain.com), то ваше письмо с очень высокой вероятностью будет расценено как спам и отвергнуто.

Настройка серверов SMTP, POP3 (IMAP) и записей DNS является минимально необходимой для создания своей почтовой системы. Дальнейшая настройка почтового сервера будет заключаться в основном лишь в создании учетных записей новых пользователей (новых почтовых ящиков).

Вместе с тем почтовый сервер может содержать и дополнительные компоненты, призванные повысить удобство и качество работы почтовой службы, а также ее безопасность. В частности, на почтовом сервере можно реализовать следующие дополнительные компоненты.

1. Средства проверки входящей и исходящей почты на вирусы (может использоваться свободно распространяемый пакет Clam AntiVirus либо коммерческие решения известных производителей антивирусного программного обеспечения).
2. Средства проверки и фильтрации нежелательных рассылок (спама). Для этого могут использоваться инструменты комплексного анализа электронных писем (например, SpamAssassin), а также различные настройки почтового сервера для проверки писем по внешним базам.
3. Веб-интерфейс администрирования почтового сервера (например, PostfixAdmin) для более простой последующей настройки почтовой системы (включая создание почтовых ящиков пользователей и выполнение других текущих административных операций).
4. Веб-интерфейс для работы с электронной почтой (например, Roundcube, Horde, SquirrelMail). Такое приложение позволит вам создать свою почтовую службу наподобие почтовых систем Gmail, Яндекс.Почта и др.
5. Средства мониторинга производительности и визуализации статистики почтового сервера (например, pflogsumm, Mailgraph, AWStats и др.).

Как видно из приведенного описания, создание и настройка сервера электронной почты являются достаточно сложной задачей. Проблемы возникают не только в плане установки и настройки программных компонент, но и в плане постоянного контроля за работоспособностью почтовой системы. Необходимо следить за осуществлением доставки ваших электронных писем на внешние адреса (проблемы могут возникать из-за некорректного описания обратной зоны, спам-проверок, вирусных рассылок, попаданием вашего сервера в черные списки и др.), реагировать на вирусные и спам-атаки на пользователей почтового сервера.

Хорошим выходом из такой ситуации для собственных почтовых систем является использование сервиса «Почта для домена» крупных почтовых служб Интернета (Gmail, Яндекс.Почта и др.) или специализированных поставщиков услуг. Такой сервис позволит вам создать почтовую систему с адресами *имя_пользователя@ваш_домен* на площадке выбранной вами компании. Настройка почтовой системы будет заключаться в выборе и подтверждении домена для своей почты, а также в создании почтовых ящиков для своих пользователей. Все остальные проблемы (поддержка работы технической площадки, проверка на вирусы, фильтрация

спама, контроль качества доставки электронных писем и др.) будут решаться на стороне поставщика услуг.

Услуга «Почта для домена» в большинстве случаев предлагается на условиях оплаты. Однако если вы создаете небольшую почтовую систему, то сможете скорее всего воспользоваться и бесплатным предложением какой-либо крупной почтовой службы Интернета. Несмотря на некоторые ограничения (в зависимости от службы — на количество пользователей, число отправляемых писем, размер сообщения, объем списков рассылки или др.), вы сможете без дополнительных финансовых затрат создать надежную почтовую службу для своих нужд.

4.3. Служба веб

Интернет как глобальная компьютерная сеть является основой реализации множества сервисов (сетевых служб), обеспечивающих общение пользователей и доступ к информации. Однако среди всех служб Интернета в настоящее время наиболее значимое место занимает *служба веб* (Web, WWW, Всемирная паутина) — глобальное информационное пространство, основанное на физической инфраструктуре Интернета и протоколе передачи данных HTTP.

Всемирную паутину образуют миллионы веб-серверов Интернета, расположенных по всему миру и обеспечивающих доступ к веб-страницам и другим ресурсам глобальной сети. Информация веб-страниц представлена в виде гипертекста, а для ее просмотра на компьютерах и мобильных устройствах пользователей применяются программы специального назначения — *веб-браузеры*. Основная функция веб-браузеров — отображение гипертекста, а также сетевая навигация на основе механизма перекрестных ссылок.

Существует множество браузеров, предназначенных для компьютеров, а также для мобильных пользовательских устройств. Среди наиболее известных следует назвать Microsoft Explorer, Mozilla Firefox, Google Chrome, Safari. Клиентом службы веб может являться и какая-либо специализированная программа, которая, как и браузер, получает информацию по протоколу HTTP. В качестве примеров таких программ можно назвать Google Earth (Google Планета Земля), а также многочисленные приложения для мобильных устройств (клиенты различных интернет-служб).

В рамках Всемирной паутины возможно как размещение статической информации, так и создание динамических сайтов, реализация различных сетевых сервисов, среди которых широкую известность получили форумы, чаты, веб-системы электронной почты, а в настоящее время – и большое количество социальных сервисов веб 2.0, позволяющих интернет-пользователям размещать собственную информацию и выстраивать сеть личных отношений в виртуальной среде.

Появление Всемирной паутины кардинальным образом изменило облик Интернета как технической системы, позволило реализовать глобальный информационный ресурс, который в настоящее время ставится в один ряд с системами телевидения и радиовещания, а также с печатными средствами массовой информации.

Структура и адресация веб-станиц

Информация Всемирной паутины представлена в виде связанных между собой веб-станиц. Каждая веб-страница — это текстовый документ, оформленный с использованием правил разметки языка HTML, включающий (помимо текста) ссылки на другие страницы, а также различное медиа-содержимое, такое как графические изображения, анимационные объекты, видео и др.

Язык HTML (*HyperText Markup Language — язык разметки гипертекста*) – это стандартный язык разметки веб-страниц. Согласно правилам языка HTML, структура веб-страниц включает в себя обычный текст и управляющие конструкции — *теги*. Каждый тег представляет собой служебное слово языка HTML, заключенное в угловые скобки.

При помощи тегов оформляются разделы веб-страницы (заголовок и тело документа), задается форматирование, устанавливаются гиперссылки, размещаются медиаэлементы, описываются свойства документа и др. Пример простой веб-страницы, описанной при помощи языка HTML, приводится ниже:

```
<html>
  <head>
    <title>Лисичкин хлеб</title>
  </head>
  <body>
    <h1>Лисичкин хлеб</h1>
    <p>Однажды я проходил по лесу целый день и под вечер вернулся
    домой с богатой добычей. Снял я с плеч тяжелую сумку и стал
    свое добро выкладывать на стол.</p>
```

```
    <p>...</p>
    <p><i>Михаил Пришвин</i></p>
  </body>
</html>
```

Подобная веб-страница может быть оформлена при помощи простого текстового редактора и сохранена в виде файла с расширением html. При просмотре данного файла в браузере пользователь увидит страницу, где заголовок оформлен крупным шрифтом, имеется один абзац с текстом, а имя и фамилия автора выделены курсивом. Для разработки веб-страниц (и сайтов Интернета), таким образом, достаточно лишь простого текстового редактора и браузера. Это, однако, не исключает возможности использования и специализированных средств веб-разработки, предоставляющих дополнительные инструменты.

Помимо HTML, современные веб-страницы и сайты Интернета создаются с применением и других языков и технологий, поддерживаемых браузером. В частности, широко используется *CSS* (*Cascading Style Sheets — каскадные таблицы стилей*) — язык описания внешнего вида документов, а также язык программирования *JavaScript*, сценарии которого обрабатываются браузером и позволяют наделять страницы свойством интерактивности.

Три языка вместе (HTML, CSS и JavaScript) обеспечивают возможности использования динамического HTML (Dynamic HTML, DHTML) — технологии создания интерактивных веб-страниц и приложений, исполняемых на стороне браузера. Это могут быть как простые страницы с отдельными элементами интерактивности (например, выпадающими меню), так и сложные веб-приложения, сравнимые по возможностям с крупными настольными программными системами (например, офисные веб-приложения, средства разработки различного медиаконтента).

Веб-страница, таким образом, может храниться и просматриваться на локальном компьютере. Однако для того, чтобы доступ к ней можно было получить через Интернет, эту страницу необходимо опубликовать на некотором веб-сервере. Каждый сетевой документ, опубликованный в Интернете, получает свой уникальный адрес, называемый *URL* (*Uniform Resource Locator*, *универсальный указатель ресурса*). Примеры адресов URL приводятся ниже:

```
http://mif.vspu.ru/books/primer.html
```

```
http://mabi.vspu.ru/portfolio/
http://edu.vspu.ru/login.php?action=register
```

Адрес URL состоит из трех частей.

1. *Протокол доступа*. Чаще всего будут указываться протоколы http и https (версия протокола http, поддерживающая шифрование). В более редких случаях — протоколы ftp, telnet и др., которые относятся не к службе веб, а другим службам Интернета.
2. *Имя сервера.* Полное доменное имя веб-сервера, на котором расположен ресурс.
3. *Путь к объекту.* Информация о нахождении ресурса на сервере. Как правило, это составное имя файла (перечень каталогов и имя самого файла) относительно главного каталога веб-сервера. В отдельных случаях имя файла может не указываться (в этом случае автоматически подставляется имя, принятое на веб-сервере по умолчанию; чаще всего — index.html и index.php). Помимо этого, может указываться и дополнительная информация, которая записывается после знака ? в формате имя_параметра=значение и требуется для динамического создания веб-страниц на стороне сервера. Несколько параметров в адресе URL разделяются знаком &.

Веб-страницы могут не только храниться на сервере, но и создаваться там динамически в момент обращения пользователя. Такая технология позволяет создавать *динамические сайты* и *серверные веб-приложения*, которые каждому пользователю предоставляют уникальный контент в зависимости от его регистрационных данных, параметров запроса, географического месторасположения и др.

Например, в виде таких динамических сайтов и серверных веб-приложений создаются сайты поисковых систем, веб-службы электронной почты, различные интернет-каталоги, многочисленные сервисы Интернета, обеспечивающие серверное хранение пользовательской информации.

Для создания динамических сайтов и серверных веб-приложений используются многие технологии и языки. Среди имеющегося многообразия выделим технологию *CGI* (*Common Gateway Interface*, *общий интерфейс шлюза*), позволяющую использовать практически любые языки программирования, а также специализированный язык *PHP*, наиболее часто применяемый в рассматриваемой ситуации.

Протокол HTTP

HTTP (*HyperText Transfer Protocol — протокол передачи гипертекста*) — протокол передачи данных прикладного уровня, используемый для получения информации с серверов веб. Изначально протокол был предназначен для передачи лишь HTML-документов, а в настоящее время — произвольных данных, включая потоковую передачу видео и звука.

Протокол соответствует клиент-серверной архитектуре, взаимодействие клиента и веб-сервера осуществляется по стандартной схеме «запрос — ответ». При этом каждое HTTP-сообщение (независимо от того, следует оно от клиента к серверу или наоборот) состоит из трех частей: обязательной *стартовой строки*, *заголовка* и *тела сообщения*.

Стартовая строка определяет тип сообщения. Если сообщение следует от клиента к серверу (HTTP-запрос), в стартовой строке указывается метод (название операции, которая должна быть выполнена), адрес запрашиваемого ресурса и версия протокола HTTP. Стартовая строка в сообщении, являющимся ответом сервера (HTTP-ответ), содержит версию протокола, код состояния и текстовое пояснение.

Коды состояния, возвращаемые веб-сервером, обозначаются трехзначными числами и разделяются на группы, определяемые первой цифрой. Каждый код связан со своим кратким текстовым пояснением. Существуют следующие группы кодов состояния.

1xx — информация о состоянии процесса передачи. Например, 100 Continue (продолжай), 102 Processing (идет обработка) и др.

2xx — информация об успешном принятии запроса и его обработке. Например, 200 OK (успешно обработано), 201 Created (создано), 202 Accepted (принято) и др.

3xx — информация о том, что необходимо выполнить запрос по другому адресу, указанному в заголовке location. Например, 301 Moved Permanently (перемещено навсегда), 302 Moved Temporarily (перемещено временно) и др.

4xx — информация об ошибках со стороны клиента. Например, 401 Unauthorized (неавторизован), 403 Forbidden (доступ запрещен), 404 Not Found (не найдено) и др.

5xx — информация об ошибках на стороне сервера. Например, 500 Internal Server Error (внутренняя ошибка сервера), 503 Service Unavailable (сервис недоступен), 504 Gateway Timeout (шлюз не отвечает) и др.

Заголовок характеризует тело сообщения и параметры его передачи. Например, в HTTP-запросах может указываться информация:

- DNS-имя компьютера, на котором расположен веб-сервер;
- адрес ресурса, с которого клиент сделал запрос;
- информация об используемом браузере;
- предпочитаемый язык запрашиваемого ресурса и др.

В HTTP-ответах могут указываться следующие заголовки:

- формат и способ представления информации в теле сообщения;
- время отправления ресурса;
- информация об используемом сервере;
- информация о количестве байт в теле сообщения и др.

Тело сообщения — это непосредственно пересылаемые данные, например информация HTTP-запросов или содержимое веб-страниц, пересылаемых от сервера клиенту. Тело сообщения отделяется от заголовка пустой строкой.

Ниже приводится пример обычного диалога браузера и веб-сервера на получение веб-страницы, хранящейся на сервере:

Запрос клиента:

```
GET /books/ HTTP/1.1
Host: mif.vspu.ru
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:34.0) Gecko/20100101 Firefox/34.0
Accept: text/html
Connection: close
(пустая строка)
```

Ответ сервера:

```
HTTP/1.1 200 OK
Date: Wed, 25 Feb 2015 12:51:18 GMT
Server: Apache
X-Powered-By: PHP/5.3.8
Last-Modified: Wed, 25 Feb 2015 12:51:18 GMT
Content-Language: ru
Content-Type: text/html; charset=utf-8
Content-Length: 4521
Connection: close
(пустая строка)
(запрашиваемая веб-страница)
```

Важной особенностью протокола HTTP является отсутствие механизма сохранения состояния между парами «запрос — ответ». Другими словами, каждое обращение к веб-серверу производится как впервые, без учета того, что ранее сервер уже возвращал какие-либо данные клиенту.

Это, в частности, не позволяет реализовать поддержание долговременных сессий при работе с сайтами Интернета непосредственно на основе протокола HTTP. Веб-приложения, требующие авторизации пользователя, должны сами поддерживать соответствующие механизмы, что чаще всего реализуется при помощи cookie.

Особенности технической реализации сервера веб

Итак, веб-сервер — это компьютер Интернета, принимающий HTTP-запросы от клиентов (веб-браузеров) и выдающий соответствующие ответы в виде веб-страниц и других запрашиваемых объектов. Веб-сервером также называют специальное программное обеспечение, которое позволяет реализовать указанный функционал на некотором физическом сервере Интернета.

Как и любой другой сервер Интернета, веб-сервер находится в постоянном активном состоянии, ожидая запросы пользователей из сети Интернет. Соединение с веб-сервером по протоколу HTTP осуществляется через 80-й порт, а по протоколу HTTPS — через порт 443.

HTTPS (*HyperText Transfer Protocol Secure*) — расширение протокола HTTP, поддерживающее шифрование с использованием криптографических протоколов SSL или TLS.

Как и в других случаях использования SSL и TLS, защита соединения предполагает наличие сертификата на стороне сервера, которому доверяют клиенты. Доверие означает, что должен использоваться сертификат, выданный каким-либо известным центром сертификации, либо самоподписанный сертификат, решение о доверии которому принимает непосредственно пользователь.

Веб-сервер, получив запрос пользователя, устанавливает с ним соединение и отправляет страницу (графическое изображение, медиаобъект или др.), хранящуюся в виде файла. Если запрос адресован какому-либо серверному веб-приложению, то веб-сервер обеспечивает выполнение соответствующих процедур (запускает приложение или сам обрабатывает

серверный сценарий) и возвращает клиенту ресурс, динамически сгенерированный по поступившему запросу.

Существует множество программных реализаций сервера веб. Анализируя многообразие технических решений следует также иметь в виду, что зачастую под сервером веб понимается не только приложение, обрабатывающее HTTP-запросы, но и целый широкий программный комплекс, включающий в свой состав интерпретаторы различных языков программирования (PHP, Perl и др.), системы управления базами данных, модули для интеграции веб-сервера с другими информационными службами (электронная почта, сетевой каталог и др.), а также другие компоненты. Самым популярным решением для создания сервера веб в таком широком понимании является платформа LAMP, предполагающая использование следующих компонентов:

1) операционной системы Linux (FreeBSD);
2) веб-сервера Apache;
3) системы управления базами данных MySQL;
4) языков программирования PHP, Perl и Phyton.

Платформа LAMP получила свое название по первым буквам указанных выше компонент. Центральным элементом этой платформы, обеспечивающим ее работу именно как сервера веб, является Apache — кроссплатформенный и свободно распространяемый веб-сервер, обеспечивающий высокую надежность и гибкость конфигурации. Данный веб-сервер содержит большое число внешних модулей, обеспечивающих поддержку разнообразных технологий. При помощи Apache можно сделать платформу со множеством виртуальных веб-серверов, обеспечивающих работу на одной физической машине большого числа автономных сайтов.

Настройка Apache в своей основной части заключается в описании директорий с веб-содержимым — путей к каталогам с файлами опубликованных сайтов, правил доступа и обработки содержимого этих каталогов. На практике настройка указанного сервера может быть связана также с установкой дополнительных модулей Apache, необходимых для реализации какого-либо особого функционала разрабатываемых веб-приложений и обеспечения работоспособности устанавливаемых CMS (например, модулей для обработки графических изображений, перекодировки текста, создания pdf-документов и др.).

Установка Apache для создания полноценного веб-сервера в соответствии с принципами платформы LAMP возможна на любом компьютере, работающем под управлением Linux или FreeBSD, имеющем

публичный IP-адрес и постоянное подключение к Интернету. Вы можете создать такой сервер самостоятельно либо воспользоваться услугами хостинг-провайдера, который предоставит готовую техническую площадку со всеми настроенными компонентами. Второй подход потребует оплаты услуг хостинг-провайдера, но у вас будут сняты технические проблемы обслуживания собственной аппаратной платформы, а также обеспечен высокоскоростной и бесперебойный доступ к вашему серверу из сети Интернет.

Если вы создаете веб-сервер для собственных нужд (изучение платформы LAMP, разработка сайтов, тестирование CMS и др.), то вполне можете реализовать необходимое программное окружение и на своем локальном компьютере. Для этого можно воспользоваться одним из специальных комплектов быстрого создания веб-сервера на локальной Windows-машине. Это такие комплекты, как Denwer, XAMPP, WAMP, EasyPHP, VertrigoServ и др.

Несмотря на то что установленное программное обеспечение будет работать под управлением Windows (платформа WAMP), вы сможете получить веб-сервер со всеми компонентами, присущими и полноценным веб-серверам. Разработанные на такой платформе ресурсы будет легко перенести на публичный веб-сервер Интернета, функционирующий в соответствии с принципами платформы LAMP.

Помимо Apache и платформы LAMP, для создания веб-серверов могут применяться и другие решения. Например, это может быть веб-сервер от компании Microsoft — *IIS* (*Internet Information Services*), который распространяется совместно с Windows и ориентирован на поддержку технологий данной операционной системы. Веб-сервер IIS благодаря возможностям интеграции с другими информационными сервисами от компании Microsoft получил широкое распространение в корпоративном секторе для создания веб-приложений, опирающихся на инфраструктуру корпоративных сетей (например, систем электронного документооборота организаций).

4.4. Файловая служба на основе протокола FTP

До появления протокола HTTP основным средством доступа к удаленным файловым ресурсам была файловая служба на основе протокола FTP.

FTP (*File Transfer Protocol — протокол передачи файлов*) – это протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов, загружать файлы с сервера или на сервер, удалять, переименовывать и перемещать файлы, а также выполнять другие файловые операции.

Файловая служба на основе протокола FTP является одной из первых, реализованных в Интернете. Несмотря на то что появившийся значительно позже протокол HTTP в плане получения информации из Интернета составил файловой службе большую конкуренцию, протокол FTP актуален и сейчас, так как он обладает более широким спектром возможностей работы с удаленной файловой системой (загрузка файлов на сервер и др.). В частности, эти возможности протокола FTP оказываются востребованными при управлении содержимым собственных веб-серверов — административный доступ к файловым ресурсам веб-сервера обычно осуществляется с использованием протокола FTP.

Протокол FTP построен на основе клиент-серверной технологии. В качестве *клиента* выступает программа, установленная на компьютере пользователя и используемая для доступа к файловым ресурсам FTP-сервера (браузер, программа для закачки файлов, консольный или графический FTP-менеджер, текстовый редактор с возможностью сохранения по FTP или др.). *FTP-сервер* — это компьютер, на котором имеются общедоступные файлы, работа с которыми осуществляется по протоколу FTP.

Подключение к серверу возможно в двух режимах доступа — *анонимном* и *на основе авторизации*.

Анонимный доступ — это режим работы, при котором в качестве имени пользователя указывается «anonymous», а сам доступ предоставляется лишь к публичным ресурсам сервера. Если FTP-сервер поддерживает анонимный доступ, то он называется *анонимным FTP*.

Доступ на основе авторизации предполагает указание реального имени пользователя (и пароля), зарегистрированного на FTP-сервере. В этом случае пользователь получает доступ не только к публичным ресурсам, но к своим собственным, не доступным (или ограниченным только для чтения) для других пользователей FTP-сервера.

Заметим, что в зависимости от настроек FTP-сервера пользователь может получить доступ как ко всей удаленной файловой системе (с ограничениями на просмотр и редактирование файлов), так и лишь к своей домашней папке. Во втором случае разные пользователи FTP-сервера будут получать разное окружение при подключении к серверу со своими учетными данными.

Протокол FTP реализует самый простой способ авторизации, предполагающий пересылку пароля в открытом текстовом виде. Чтобы повысить уровень безопасности, можно использовать различные методы защищенной авторизации, шифрования команд FTP и пересылаемых данных. Такие методы могут быть основаны на использовании криптографических протоколов SSL (TLS) или туннелированных FTP-сессий через SSH-соединение.

Достаточно заметной особенностью технической реализации протокола FTP является то, что для своей работы он использует *множественное соединение* с сервером (как минимум двойное). Первое соединение является управляющим, через которое отправляются команды серверу и возвращаются его ответы. Такое соединение устанавливается на 21-й порт FTP-сервера. Остальные соединения используются для передачи данных. Номера портов дополнительных соединений определяются клиентом или сервером (в зависимости от режима FTP-подключения) и могут принимать различные значения.

Протокол FTP поддерживает два режима работы — *активный* и *пассивный*. В активном режиме после установки управляющего соединения FTP-сервер сам пытается установить соединение с клиентом для передачи данных. Если клиент расположен за брандмауэром (тем более если он использует подключение с использованием NAT), то сервер установить такое соединение не в состоянии. Чтобы решить эту проблему был разработан пассивный режим FTP.

Согласно правилам пассивного режима клиент и сервер по управляющему соединению «договариваются» о номере порта на сервере для соединения передачи данных, а само такое соединение устанавливает клиент.

Еще одна особенность протокола FTP — это возможность использования *текстового* и *двоичного* режима передачи данных. Текстовый режим учитывает разницу в оформлении текстовых файлов, принятом в различных операционных системах. При использовании текстового режима при копировании файлов между компьютерами под управлением разных операционных систем будут удаляться лишние символы в признаках конца строки (или добавляться недостающие).

Если в текстовом режиме будет копироваться двоичный файл, то с большой вероятностью в процессе копирования такой файл будет испорчен, так как символы конца строки (символы с кодом 10 и 13, которые могут присутствовать и в структуре двоичного файла) будут «откорректированы» в соответствии с правилами оформления текста. Не следует забывать включать двоичный режим копирования файлов, если используемый вами клиент по умолчанию использует текстовый.

Проблема двоичного и текстового режимов не возникнет, если вы копируете текстовые файлы в какой-либо кодировке UNICODE (например, обмениваетесь файлами в кодировке UTF-8 между своим компьютером и веб-сервером). Вне зависимости от выбранного режима скопированный файл будет корректным для любой операционной системы.

Сервер FTP обычно создается на компьютере, работающем под управлением Linux или FreeBSD. При этом существует большое число программных решений для создания такого сервера — от простых приложений, обеспечивающих FTP-доступ для выполнения административных операций, до сложных программных систем, предназначенных для создания крупных файловых архивов Интернета, поддерживающих работу со значительным количеством пользователей.

4.5. Удаленный доступ к консоли через Telnet и SSH

Telnet (*TErminaL NETwork*) — сетевой протокол для реализации текстового интерфейса по сети. Существует множество применений протокола Telnet, самым востребованным из которых является удаленный доступ к интерфейсу командной строки операционных систем (доступ к удаленной консоли). Используя Telnet, пользователи могут подключаться к

удаленным компьютерам, получая доступ к их консоли на своей локальной машине.

Протокол Telnet предлагает самую простую модель безопасности, не предполагающую шифрование данных. В этой связи более безопасным является протокол *SSH* (*Secure Shell — безопасная оболочка*), который, как и протокол Telnet, позволяет организовать удаленный доступ к консоли, однако предполагает установку защищенных соединений (включая безопасную авторизацию и шифрование пересылаемых данных). Подключение к серверу по протоколу SSH осуществляется на 22-й порт, а по протоколу Telnet – на 23-й.

Для подключения к удаленному компьютеру по протоколам SSH и Telnet надо воспользоваться соответствующим клиентом, указать адрес удаленного компьютера и порт, а после начала соединения – свой логин и пароль. После выполнения этих операций вы сможете работать с командной строкой удаленного компьютера так же, как и за его локальной консолью.

Протоколы Telnet и SSH предъявляют очень низкие требования к каналам связи, так как пересылают лишь команды пользователя и экранные символы, выдаваемые в качестве ответа. Эти протоколы удобно использовать для управления удаленными серверами, а также управления множеством серверов с одного рабочего места администратора.

Настройка протоколов Telnet и SSH на компьютерах под управлением Linux и FreeBSD заключается, как правило, лишь в установке разрешения их использования для удаленных соединений. В качестве клиентов могут использоваться одноименные утилиты командной строки в операционных системах Linux и FreeBSD или специальные приложения, такие как Putty для Windows. В связи с небезопасностью протокола Telnet в настоящее время рекомендуется разрешать и использовать лишь протокол SSH.

В целях обеспечения безопасности в операционных системах Linux и FreeBSD через удаленное подключение запрещается авторизация с использованием учетных данных суперпользователя (root). В этой связи удаленные подключения всегда следует устанавливать от имени обычного пользователя, которому разрешены удаленные подключения. При необходимости выполнения административных операций — переключаться в режим суперпользвоателя или использовать механизм sudo.

Вопросы и задания

Служба DNS

Опишите принципы внутренней организации службы DNS.

Что такое домен и зона DNS? Что общего у домена и зоны? В чем проявляются различия?

Как осуществляется связь нескольких серверов DNS?

Чем отличаются авторитетные и неавторитетные ответы сервера DNS?

Что такое рекурсивная и нерекурсивная процедура распознавания?

Что такое прямое и обратное преобразование DNS? В каких случаях применяется каждое из них?

Назовите типы ресурсных записей зоны DNS. Кратко опишите назначение записей каждого типа.

Электронная почта

Опишите общие принципы организации службы электронной почты Интернета.

Какова структура адреса электронной почты? Что обозначает каждая из частей этого адреса?

Как определяется маршрут доставки электронного письма? В чем проявляется связь служб электронной почты и DNS?

Для чего используется сервер электронной почты? Какое участие принимает сервер при отправке и получении письма?

В чем особенности схем передачи электронной почты с использованием нескольких почтовых серверов? Для чего могут применяться дополнительные серверы?

Какова структура сообщения электронной почты? Какая информация может указываться в заголовке письма?

Назовите протоколы, которые используются для пересылки электронной почты. Каково назначение и в чем особенности этих протоколов?

Опишите проблемы безопасности, которые следует учитывать при настройке службы электронной почты.

Служба веб

Опишите общее предназначение службы веб. Какие сетевые компоненты обеспечивают работу данной службы (серверы и клиенты)?

Какой протокол используется для обмена информацией между серверами и клиентами веб? Что служит указателем?

Из каких трех частей состоит сообщение протокола HTTP? Опишите назначение каждой из частей.

Какие коды состояния может возвращать сервер веб, отвечая на запрос клиента?

Опишите особенности технической реализации сервера веб. Что такое платформа LAMP?

Возможно ли создание защищенных соединений с сервером веб? Как реализуются такие соединения?

Файловая служба на основе протокола FTP

Для чего предназначен протокол FTP? В чем его сходство и различие с протоколом HTTP в плане организации доступа к удаленным файлам?

Чем отличаются режимы анонимного доступа к серверу FTP и доступа на основе авторизации?

Что такое пассивный и активный режимы работы сервера FTP? Какой из этих режимов возможно использовать при подключении клиентов, использующих NAT?

Почему копирование файлов с сервера FTP может осуществляться в двоичном или текстовом режиме? Какой из режимов необходимо выбирать для передачи данных?

Удаленный доступ к консоли

Для чего применяются протоколы удаленного доступа Telnet и SSH? Каковы их общие черты? В чем проявляется различие этих протоколов?

Раздел 5. Локальные сети на основе Windows

Операционная система Windows имеет встроенную поддержку компьютерных сетей, начиная с версии Windows for Workgroups 3.1 (октябрь 1992 г.). С этой версии все ОС Windows позволяют создавать компьютерные сети без установки дополнительного программного обеспечения. Однако модели и технологии построения сетей по мере развития Windows изменялись. Так, например, протокол TCP/IP в качестве основного на клиентских версиях Windows стал использоваться только в 1996 году (Windows 95 OSR 2). В 2000 году существенно была обновлена доменная модель компьютерной сети (линейка ОС Windows 2000). В 2006 году в качестве обязательного сетевого компонента появился протокол IPv6 (Windows Vista).

В настоящее время локальные сети на основе Windows базируются на протоколах IPv4 и IPv6, глубоко интегрированы с Интернетом. Windows позволяет создавать сети разного масштаба, обеспечивает развитую инфраструктуру для создания сетевых приложений и самых разнообразных информационных систем, имеет удобные средства администрирования. Несмотря на то что существуют и другие решения для построения локальных сетей (например, от компании Novell и Apple), большинство современных локальных сетей базируется на технологиях Windows (даже в том случае, когда используются и другие ОС).

Данный раздел посвящен современным технологиям построения локальных сетей на основе Windows. Эти технологии определяются характеристиками Windows как многопользовательской системы, моделями одноранговых и доменных локальных сетей, способами управления сетью на основе домена. Важным вопросом является также организация системных сервисов Windows-сетей. Такие сервисы также рассматриваются в данном разделе.

5.1. ОС Windows как многопользовательская система

Windows является многопользовательской операционной системой, что в значительной степени закладывается в модель построения и локальных сетей. В этой связи, чтобы впоследствии лучше понимать различные решения, принятые в сетях на основе Windows, кратко рассмотрим

особенности организации многопользовательской работы в данной операционной системе.

Реализация многопользовательской работы в ОС Windows опирается на механизм учетных записей пользователей и групп. Такие учетные записи создаются как на локальных компьютерах, так и в доменах Windows.

Учетная запись *пользователя* содержит сведения, необходимые для идентификации пользователя и определения его прав в операционной системе и компьютерной сети. Учетная запись пользователя содержит имя учетной записи, пароль, принадлежность к группам, отображаемое имя пользователя, параметры учетной записи и многое другое.

Учетная запись *группы* — это набор учетных записей пользователей. Одни группы могут включать в свой состав другие, что позволяет создавать иерархические структуры учетных записей (подобно тому, как создаются структуры файлов и папок на носителях информации).

Учетные записи пользователей и групп позволяют:

- создать для каждого пользователя свое программное окружение (рабочую среду);
- ограничить пользователей в доступе к папкам и файлам;
- разрешить или запретить пользователям запуск программ или выполнение определенных операций.

Права и ограничения могут назначаться как на отдельных пользователей, так и на группы. Более того, создание надежной и гибкой системы назначения прав пользователям — это основное назначение групп. Хорошее правило в Windows — описать нужные права и ограничения для какой-то группы, а потом включить в эту группу всех пользователей, для которых данные настройки необходимо применить.

Сразу после установки Windows создаются следующие пользователи и группы:

- пользователи:
  - администратор;
  - гость;
- группы:
  - администраторы;
  - опытные пользователи;
  - пользователи;
  - гости.

Эти пользователи и группы являются локальными, они создаются и хранятся на рабочих станциях. Наряду с этим учетные записи пользователей и групп могут создаваться и в домене Windows (подробнее про это будет сказано позже). В частности, это группы «администраторы домена», «пользователи домена», «гости домена», которые создаются и хранятся на сервере локальной сети, а на каждом отдельном компьютере входят в соответствующие локальные группы.

Перечисленные выше группы являются основными для Windows, но не единственными, создаваемыми при установке. Чаще всего используются записи групп «администраторы» и «пользователи».

Администраторы имеют полный контроль над компьютером. Они могут изменять настройки, устанавливать программы, создавать новых пользователей, запускать все установленные приложения.

Пользователи компьютера ограничены в части изменения параметров компьютера – они могут лишь запускать установленные приложения, менять параметры окружения в рамках своего профиля, сохранять файлы.

Опытные пользователи занимают промежуточное положение между администраторами и пользователями. Они, например, могут создавать учетные записи новых пользователей, но в дальнейшем изменять только те записи, которые создали сами.

Гости имеют те же права, что и пользователи, однако за одним, но очень важным исключением — все изменения, которые произвели гости, удаляются в момент завершения сеанса работы. Таким образом, гости не могут сохранять файлы и менять параметры своего программного окружения на долгое время (лишь до первого выключения компьютера).

Администраторы компьютера могут создавать новые учетные записи пользователей и групп. Как правило, в процессе установки Windows запрашивается создание как минимум одной учетной записи пользователя — владельца компьютера. Эта учетная запись также получает права администратора.

Помимо локальных и глобальных (доменных) групп, существуют также и специальные группы. Эти группы нигде не хранятся, принадлежность к ним определяется из контекста. К специальным группам относятся:

- прошедшие проверку;
- анонимные пользователи;
- локальные пользователи;
- сетевые пользователи;

- создатель-владелец;
- все.

Например, обращаясь к группе «все», можно указать параметры доступа для всех пользователей без исключения, а через группу «прошедшие проверку» определить только тех, кто указал свой логин и пароль.

Зарегистрированные в системе учетные записи пользователей и групп используются при разграничении прав доступа — в *списках контроля доступа* (ACL, Access Control List). Списки контроля доступа применяются к файлам, папкам, сетевым ресурсам, параметрам реестра, объектам групповых политик и др. При помощи этих списков для каждого пользователя (напрямую или опосредованно) можно определить уровень доступа к информации, а также перечень допустимых операций.

Так, для файлов и папок предлагается стандартный и расширенный наборы *атрибутов* доступа (табл. 5.1.1).

Таблица 5.1.1

Стандартные атрибуты доступа	**Расширенные атрибуты доступа**
• Полный доступ • Изменение • Чтение и выполнение • Список содержимого папки • Чтение • Запись	• Создание файлов (папок) • Удаление • Чтение разрешений • Чтение атрибутов • Смена разрешений • Смена владельца • …

Для каждого атрибута применительно к конкретному пользователю (или группе) можно указать значения: «Разрешить», «Запретить». При этом следует учитывать, что значения атрибутов доступа имеют накопительный характер, а запрет всегда имеет приоритет. Возможно также наследование атрибутов, предполагающее, что файлы и папки автоматически получают те же права доступа, что и родительская папка.

Например, для некоторого пользователя в списках контроля доступа к файлу указано «Разрешить» только для атрибута «Чтение». В этом случае пользователь сможет только просмотреть файл, но не сможет его изменить, удалить, поменять атрибуты и др. Но если этот пользователь входит в группу, для которой указано «Разрешить» для

атрибутов «Чтение» и «Запись», то пользователь сможет и изменять файлы. Такое поведение обеспечивается за счет накопительного характера атрибутов доступа.

Приоритет запрета означает, что в случае, когда возникает конфликт значений для какого-то атрибута (одновременно указано «Разрешить» и «Запретить»), то для данного атрибута в итоге останется значение «Запретить». Например, если для пользователя указано «Разрешить» для атрибутов «Чтение» и «Запись», но для группы, в которую входит пользователь, указано «Запретить» для атрибута «Запись», то пользователь сможет только просматривать файл.

Значение «Запретить» используется гораздо реже, чем «Разрешить». Обычно к этой возможности прибегают для того, чтобы надежно блокировать доступ к ресурсам в случае, когда пользователи могут входить сразу в несколько групп.

Управление рабочей средой пользователя

Рабочая среда пользователя состоит из настроек рабочего стола и других параметров Windows, настроек доступных приложений, а также документов пользователя. Указанные настройки и документы хранятся в *профиле пользователя* — папке специального формата, которая «закреплена» за конкретным пользователем. Эта папка хранится на локальном компьютере либо на сервере (перемещаемый профиль).

Локальные профили пользователей в современных версиях Windows хранятся в папке Users, которая в русифицированных версиях операционной системы имеет и второе название — пользователи. Содержимое этой папки включает в себя профили пользователей, которые хотя бы один раз работали на компьютере (как правило, имя папки профиля пользователя совпадает с логином пользователя), а также папки Default User и All Users.

Профиль пользователя содержит множество папок, основными из которых являются:

- Application Data;
- Local Settings;
- Главное меню;
- Рабочий стол;
- Мои документы.

Папки Application Data и Local Settings содержат данные конкретных приложений и локальные настройки. Иногда эти папки могут использоваться и для установки программ (например, Google Chrome). Если программа рассчитана на установку в профиль пользователя, а не в папку Program Files, то ее может установить и простой пользователь, не обладающий правами администратора. Работать с этой программой сможет, однако, только сам пользователь. Другие пользователи компьютера к этой программе доступ получить не смогут.

В профиле пользователя хранится также файл NTUSER.DAT — это фрагмент системного реестра, в котором размещаются пользовательские настройки (ветка HKEY_CURRENT_USER).

Содержимое профиля пользователя доступно только для самого пользователя и администратора. Это, в частности, означает, что другие пользователи (не имеющие прав администратора) не могут получить доступ к пользовательским данным, хранящимся на рабочем столе или в папке Мои документы.

Профиль пользователя создается при первом входе в систему путем создания копии папки Default User. Как было замечено выше, копия этой папки получает имя, соответствующее имени учетной записи пользователя. Папка All Users, в свою очередь, содержит компоненты, которые добавляются к профилям каждого пользователя Windows. Например, это ярлыки главного меню и рабочего стола для приложений, доступных всем пользователям компьютера.

В Windows могут использоваться не только локальные, но и перемещаемые (сетевые) профили пользователей. Каждый раз при включении компьютера перемещаемый профиль копируется с сервера на локальную машину, а при выключении — с локальной машины на сервер. В этом случае, вне зависимости от того, на каком компьютере пользователь в данный момент работает, он получает то же окружение (файлы, настройки, локальные программы), что и в прошлый сеанс работы. Профиль перемещается по сети вслед за пользователем, которому приходится менять свой рабочий компьютер.

Достоинством технологии перемещаемого профиля является также резервирование данных (они всегда хранятся как минимум в двух местах – на сервере локальной сети, а также на компьютере, где работал пользователь). Недостатком — ощутимые задержки при включении и выключении компьютера (из-за необходимости копирования файлов), а также дополнительная нагрузка на сеть.

5.2. Рабочая группа и домен Windows

Итак, ОС Windows имеет все необходимые компоненты для построения сетей. При этом существуют две модели построения сетей на основе Windows — это модель *рабочей группы* и модель *домена*. Основное отличие этих моделей проявляется в способе взаимодействия компьютеров между собой, а также управления сетью. Модель рабочей группы — это одноранговая сеть. Домен Windows всегда предполагает наличие специального сервера — контроллера домена.

Рабочая группа

Рабочая группа – это простая модель. В такой сети все компьютеры равноправны – как правило, это рабочие компьютеры пользователей, на которых некоторые ресурсы (папки и принтеры) открыты для доступа из сети.

Важно, что все компьютеры рабочей группы имеют свои наборы учетных записей пользователей. Проверка прав пользователей всегда осуществляется по наборам учетных записей на локальных компьютерах.

Рассмотрим в качестве примера рабочую группу, в которой имеются четыре компьютера (рис. 5.2.1): KROSH, BARASH, LOSYASH и NUSHA. На каждом из этих компьютеров имеются локальные базы учетных записей пользователей (Denis, Oleg, Roman и др.). Отдельные компьютеры рабочей группы имеют ресурсы, которые доступны из сети (сетевые папки public, install, music, а также сетевой принтер).

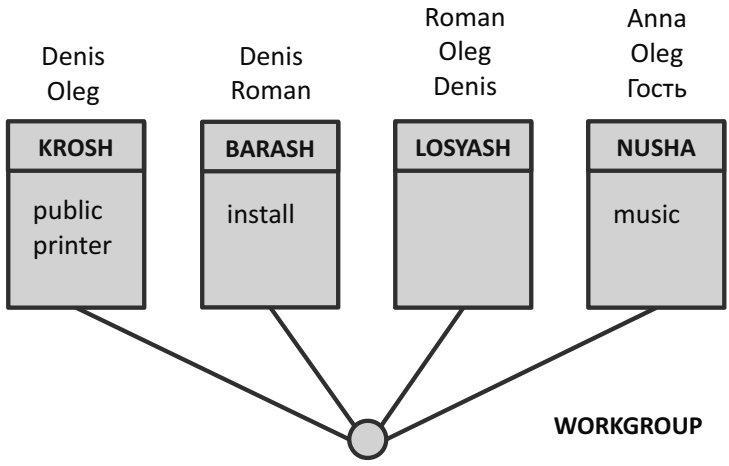


Рис. 5.2.1. Структура рабочей группы (пример)

Как осуществляется проверка прав пользователя при обращении к ресурсам этих компьютеров из сети? Предположим, что все сетевые ресурсы открыты для полного доступа. Тогда в данной рабочей группе возможны следующие типичные ситуации.

1. Пользователь с учетной записью Denis, работая на компьютере KROSH, обращается к папке install на компьютере BARASH. Мы видим, что на компьютере BARASH также есть учетная запись Denis. Если пароли этих учетных записей совпадают, то пользователь Denis сразу же получит доступ к папке install. Если пароли не совпадают, то пользователю надо будет ввести пароль пользователя Denis, который ранее был указан на компьютере BARASH.
2. Пользователь Oleg на компьютере KROSH обращается к папке install на компьютере BARASH. Как видим, данного пользователя на компьютере BARASH нет. Это означает, что пользователю Oleg надо будет представиться как Denis или Roman и ввести соответствующий пароль.
3. Пользователь Roman на компьютере BARASH обращается к папке music на компьютере NUSHA. Мы видим, что пользователя Roman на этом компьютере нет, но есть пользователь Гость, учетная запись которого используется при анонимных обращениях из сети. Это означает, что пользователь Roman автоматически получит доступ к папке music (без ввода пароля), такое обращение будет для компьютера NUSHA анонимным — как обращение пользователя Гость.

Как следует из описания типичных ситуаций, в рабочей группе Windows существуют три стратегии настройки доступа к сетевым ресурсам. Чтобы организовать сетевой доступ, на всех компьютерах можно:

1) создать разные учетные записи и проводить авторизацию пользователя при *каждом* обращении к сетевому ресурсу, вводя логин и пароль учетной записи, зарегистрированной на удаленном компьютере;
2) создать одинаковые наборы учетных записей с одинаковыми наборами паролей, чтобы избежать ввода данных авторизации при каждом обращении к ресурсам сети;
3) на компьютерах с сетевыми ресурсами включить гостевую запись и обращаться к этим ресурсам с одинаковыми правами доступа для всех пользователей.

Все имеющиеся стратегии обладают существенными недостатками. Так, в первом случае всем пользователям компьютерной сети надо будет знать все пароли от всех сетевых компьютеров, к которым они хотят получать доступ, и каждый раз вводить соответствующие данные при сетевом обращении.

Во втором случае при наличии достаточно большого числа пользователей и компьютеров значительно усложняется задача администрирования сети — необходимо создавать большое число учетных записей, а также следить за соответствием паролей. Такая простая операция, как смена пароля пользователя, становится трудноосуществимой, так как менять пароль необходимо на всех компьютерах сети.

В третьем случае невозможно реализовать защиту информации на основе разграничения доступа, так как удаленная работа с сетевыми ресурсами будет производиться анонимно (от имени учетной записи «Гость»).

Таким образом, рабочая группа, отличаясь простотой, не позволяет эффективно создавать большие сети. По рекомендации компании Microsoft, модель рабочей группы следует использовать в сетях, объединяющих до 20 компьютеров.

Наряду с указанными выше недостатками модель рабочей группы обладает и преимуществами. Это низкая стоимость всей сети и простота настройки отдельных машин, а также достаточно высокая отказоустойчивость (в рабочих группах отсутствует единая точка отказа — здесь нет компьютера, поломка которого может нарушить работоспособность всей сети).

Для создания рабочей группы подойдут компьютеры с любой версией Windows, даже самой простой. Членами рабочей группы могут быть домашние и профессиональные версии клиентских Windows, а также компьютеры под управлением Windows Server. Для создания такой сети необходимо указать имя рабочей группы на всех компьютерах (по умолчанию обычно используется имя WORKGROUP). Остальные настройки рабочей группы связаны с настройкой доступа к сетевым ресурсам каждой отдельной машины.

Начиная с Windows 7, существует также возможность создания *домашних групп.* Домашняя группа — это часть рабочей группы, защищенная единым паролем (рис. 5.2.2). Пароль задается при

создании домашней группы и для каждого компьютера вводится один раз в процессе присоединения к домашней группе.

Домашние группы позволяют открывать доступ к ресурсам компьютера только для «доверенных» компьютеров — участников домашней группы. Другие пользователи не могут получить доступ к таким ресурсам, если владелец не предоставит соответствующее разрешение.

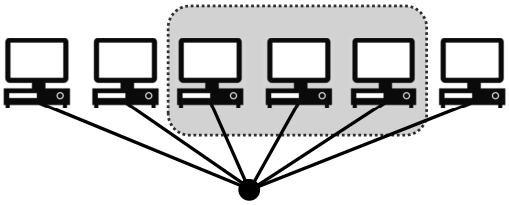


Рис. 5.2.2. Домашняя группа в структуре рабочей группы

Домашние группы, таким образом, упрощают управление доступом к сетевым ресурсам в небольших сетях. Использование домашних групп не является обязательным.

Домен Windows

Домен Windows — это модель построения локальной компьютерной сети, предполагающая наличие сервера (контроллера домена) и централизованного управления всеми компьютерами сети. В домене существует общая база пользователей, настраивается общая политика безопасности. Домен управляется как единый объект, все компьютеры домена могут контролироваться сервером.

Рассмотрим в качестве примера сеть, в которой, как и в прошлый раз, имеются компьютеры KROSH, BARASH, LOSYASH и NUSHA, а также пользователи Denis, Oleg, Roman и Anna. Данная сеть, однако, будет устроена как домен, т.е. будет содержать и сервер — контроллер домена (рис. 5.2.3).

Как видно на рисунке, существенное отличие домена Windows от рабочей группы заключается в том, что в домене имеется централизованная база пользователей, которая хранится на сервере — на *контроллере домена*. Такой подход позволяет упростить управление записями пользователей, а также обеспечить *единый вход* в сеть. Пользователи, имеющие учетную запись в домене, могут *войти в систему на любом компьютере*, так как авторизация осуществляется на основе учетной записи, хранящейся в сети.

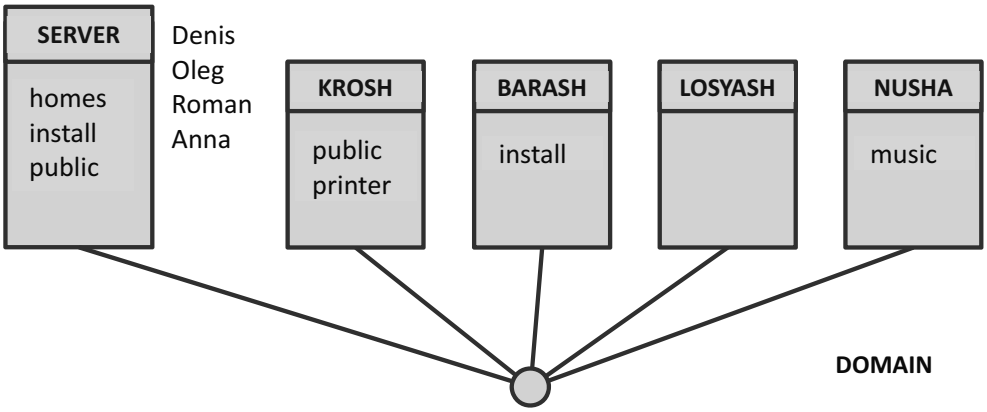


Рис. 5.2.3. Структура домена Windows (пример)

Единый вход предполагает, что пользователь только один раз вводит логин и пароль — при включении своего компьютера (в процессе авторизации). В дальнейшем это учитывается и при обращении к сетевым ресурсам — пользователь, прошедший проверку в домене, повторно не будет проходить проверку при обращении к компьютерам сети. Доступ к сетевым ресурсам осуществляется от имени того пользователя, который проходил авторизацию в домене.

Наличие централизованной базы пользователей домена не отменяет локальные учетные записи на пользовательских компьютерах. Выбор типа учетной записи осуществляется при включении компьютера – пользователю предлагается выбрать «Войти в компьютер» или «Войти в домен». При использовании локальной учетной записи («Войти в компьютер») преимущества доменного доступа к ресурсам компьютерной сети оказываются недоступными.

Еще одна особенность домена Windows заключается в том, что доменная модель предполагает и централизованное управление рабочими станциями, входящими в домен. Например, администратор домена может управлять различными настройками рабочего окружения на компьютерах домена (настройки рабочего стола, пользовательских папок, параметров сетевого доступа, системных приложений и др.), задавать ограничения, касающиеся правил доступа и безопасности компьютерной сети (ограничения, касающиеся возможности авторизации пользователей на компьютерах, времени доступа, правил смены паролей и др.), управлять перечнем установленных приложений и др. Администратор домена имеет

возможность доступа ко всем файлам и папкам, хранящимся на компьютерах пользователей.

Централизованное управление реализуется в основном через настройку *политик безопасности домена*, а также *групповых политик*. Отдельной возможностью централизованного управления является механизм *сценариев входа и выхода* пользователей, назначаемых администратором и выполняемых на рабочих станциях в компьютерной сети.

Как видим, домен предлагает более развитые решения для управления пользователями и компьютерами в сети. Доменные сети благодаря подобным инструментам могут быть значительно более крупными, чем рабочие группы. В доменах могут присутствовать сотни и тысячи компьютеров, в том числе расположенные в разных сегментах локальных сетей. Домен Windows является удачным выбором для построения корпоративных сетей.

Современная модель домена Windows использует службу каталогов Active Directory для именования, хранения и выборки информации в распределенной среде. Особенности организации данной службы мы подробно рассмотрим в следующем параграфе, здесь лишь кратко скажем, что с практической точки зрения для создания домена Windows требуется:

1) установка и настройка одного или нескольких серверов — контроллеров домена. Контроллер домена должен работать под управлением серверной версии Windows (Windows Server 2008, Windows Server 2012 или др.);
2) установка и настройка на рабочих станциях профессиональных версий клиентских Windows (Professional, Enterprise, Ultimate). Начальные и домашние версии Windows (Core, Starter, Home) входить в домен Windows не могут;
3) приобретение лицензий клиентского доступа (Client Access License, CAL) в соответствии с количеством имеющихся у вас рабочих станций (или пользователей) в компьютерной сети.

В целях обеспечения надежности и отказоустойчивости в каждом домене рекомендуется создавать как минимум два сервера — контроллера домена. Данные серверы будут дублировать информацию домена, что обеспечит сохранность данных в случае выхода из строя одной из машин, а также работоспособность сети в случае возникновения каких-либо проблем сетевого доступа.

Несколько контроллеров домена позволяют также распределить нагрузку из сети. Это является актуальным в случае, когда домен основывается на нескольких территориально обособленных сегментах сети, связанных между собой низкоскоростными каналами.

Создание домена Windows не является единственной причиной приобретения и установки серверных версий Windows. Иногда Windows Server используется и в одноранговых сетях, а также в доменах Windows, но не в роли контроллера домена. Такие серверы называются автономными (standalone).

Например, автономный сервер Windows может использоваться для создания сетевых служб (DHCP, DNS или др.), как сервер баз данных, файловый сервер и др. Клиентские версии Windows в данном случае не подойдут, т.к. в них не реализованы многие сетевые сервисы, а также есть ограничение на количество одновременных подключений (допускается лишь до 10 подключений из сети).

5.3. Сетевой каталог Active Directory

Служба каталогов Active Directory — это средство именования, хранения и выборки информации в распределенной среде. Active Directory является технологической основой для доменов Windows. В службе каталогов хранятся учетные записи пользователей, компьютеров, информация о файлах, приложениях политиках безопасности и др.

Каталог Active Directory имеет иерархическую структуру, совместимую с LDAP (Lightweight Directory Access Protocol — облегченный протокол доступа к каталогам). Active Directory также глубоко интегрирован с DNS, а в качестве основного протокола аутентификации использует Kerberos.

Active Directory с точки зрения администратора

Как уже было указано выше, служба каталогов Active Directory обеспечивает современную реализацию доменов Windows. С точки зрения администратора-практика, развертывание Active Directory (создание домена) означает, что в компьютерной сети:

1) создается один или несколько контроллеров домена (на основе Windows Server);

2) на рабочие станции устанавливаются профессиональные версии Windows. Эти компьютеры добавляются в домен;
3) учетные записи пользователей создаются на контроллере домена. Пользователи получают возможность работы на любом компьютере домена с использованием своих учетных записей;
4) авторизация пользователей производится лишь один раз — в момент включения компьютера (входа в систему). В процессе такой авторизации:
    - пользователь на каком-то компьютере домена вводит логин и пароль, а также указывает, что входит в домен;
    - происходит поиск контроллера домена через DNS;
    - на основе обмена информацией с контроллером домена происходит аутентификация пользователя (используется протокол Kerberos);
    - после успешной аутентификации пользователю назначаются права, что завершает процесс авторизации (пользователь входит в систему и может обращаться к любым ресурсам домена без повторного ввода пароля);
5) появляется возможность использования групповых политик (политик безопасности домена). Эти политики настраиваются на сервере (контроллере домена) и применяются на всех компьютерах домена в момент включения или авторизации пользователя;
6) администратор домена получает полный контроль над рабочими станциями (включая возможность доступа ко всем файлам, хранящимся на компьютерах пользователей);
7) появляется возможность создавать и использовать приложения, использующие ресурсы Active Directory.

Таким образом, Active Directory обеспечивает:

- единую регистрацию в сети;
- централизованное управление;
- использование «сложных» приложений, опирающихся на инфраструктуру всей сети.

В домене Windows аутентификация пользователей производится при помощи протокола Kerberos. Это сетевой протокол, который предлагает механизм взаимной аутентификации клиента и сервера, учитывающий тот факт, что начальный обмен информацией между клиентом и сервером происходит в незащищенной среде.

Протокол Kerberos создает надежную основу организации безопасного взаимодействия пользователей в компьютерной сети. Он достаточно сложно устроен, однако в домене Windows от администратора выполнения каких-либо обязательных настроек не требует. Единственное, что требуется, — аккуратная настройка времени на всех компьютерах вашей сети. Если разница во времени у клиента и сервера будет слишком велика (как правило, более 5 минут), то аутентификация по протоколу Kerberos будет невозможна.

Чтобы разница во времени не создавала проблем, в доменах Windows реализована автоматическая синхронизация времени рабочих станций с контроллером домена. Проверить выполнение синхронизации, а также принудительно установить время можно при помощи команд w32tm и net time.

Структурная организация Active Directory

Сетевой каталог может содержать большое количество элементов, от надежности работы этого каталога будет зависеть работоспособность всей сети – домена Windows. Кроме этого, может меняться и структура организации, которой принадлежит домен (создаваться новые подразделения, удаленные офисы, уточняться зоны ответственности разных администраторов и др.). Сетевой каталог должен следовать за такими изменениями, обеспечивая необходимую конфигурацию компьютерной сети. В этой связи домены Windows могут иметь различную структурную организацию, что проявляется в аспекте организации работы нескольких контроллеров домена, а также группировки различных доменов в единый сетевой каталог.

Несколько контроллеров домена

Ранее мы уже отмечали, что в домене Windows рекомендуется создавать как минимум два контроллера домена. Такое решение обеспечивает высокую надежность домена за счет резервирования служб и информации, а также повышение производительности путем распределения нагрузки.

Все контроллеры домена в сети считаются равноправными, они содержат одну и ту же информацию сетевого каталога. Равноправность контроллеров домена обеспечивается за счет *репликации* — механизма, при котором изменения какого-либо элемента на одном контроллере домена переносятся и на остальные.

Заметим, что, в отличие о службы DNS или старой модели доменов Windows NT, где также возможно дублирование серверов, механизм репликации Active Directory позволяет учитывать изменения на *любом* контроллере домена, распространяя эти изменения и на другие контроллеры. В Active Directory, таким образом, отсутствуют понятия основного и резервного контроллеров домена. Хотя в некоторых случаях отдельные контроллеры все же могут иметь в домене особую роль (подробнее об этом будет сказано ниже).

Администратор домена может гибко управлять настройками репликации (топология, расписание и др.), что в ряде случаев требуется для учета особых конфигураций компьютерной сети, сложной структуры домена.

Так, домен Windows может создаваться в сети, территориально разделенной на обособленные фрагменты. В этом случае домен целесообразно разделить на *сайты*. Сайт в указанном понимании — это часть домена, имеющая в своем составе как минимум один контроллер домена и соединенная с другими частями домена относительно медленными или нестабильными каналами связи.

Разделение домена на сайты позволяет, таким образом, учесть особенности физической организации домена. Клиенты одного сайта будут обращаться только к «своему» контроллеру домена, а репликация между сайтами при соответствующей настройке будет осуществляться по экономичному сценарию.

Вместе с тем, несмотря на равноправность контроллеров домена, некоторые операции все же требуют определения одного исполнителя (уникальность сервера, выполняющего операцию). Такие операции называют FSMO (Flexible single-master operations — операции с одним исполнителем), а соответствующие контроллеры домена — *основными контроллерами операций* (говорят, что контроллер домена выполняет соответствующую *роль*).

Существуют пять ролей FSMO.

1. *Владелец схемы* (Schema Master). Отвечает за внесение изменений в *схему каталога* Active Directory (подробнее про схему каталога будет сказано ниже).
2. *Владелец именования доменов* (Domain Naming Master). Отвечает за операции, связанные с именами доменов Active Directory.

3. *Владелец относительных идентификаторов* (Relative ID Master). Отвечает за выделение уникальных идентификаторов объектам домена, а также за корректность перемещения объектов из одного домена в другой.
4. *Эмулятор основного контроллера домена* (Primary Domain Controller Emulator, PDC Emulator). Обеспечивает совместимость доменов Active Directory со старыми доменами Windows, эмулируя основной контроллер домена для приложений, разработанных в соответствии с требованиями доменов Windows NT.
5. *Владелец инфраструктуры* (Infrastructure Master). Хранит данные о пользователях из других доменов, входящих в локальные группы своего домена.

Роли Schema Master и Domain Naming Master являются уникальными для *леса* доменов, а остальные роли — для каждого домена отдельно. Администраторы могут сами назначать, какой из контроллеров домена должен выполнять ту или иную роль. Если этот контроллер домена в силу каких-либо причин становится неработоспособным, то существует механизм *захвата* роли FSMO, позволяющий администратору восстановить нормальную работу домена.

Группировка доменов

В зависимости от структуры сети и принципов ее администрирования сетевой каталог Active Directory может объединять несколько доменов — *дерево доменов* (domain tree) или *лес* (forest).

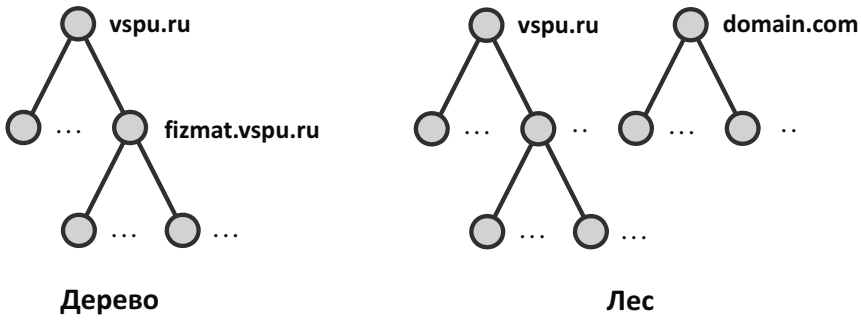


Рис. 5.3.1. Дерево и лес доменов

Дерево доменов представляет собой структуру, объединяющую домены, имеющие смежные имена. Лес — это группа деревьев, т.е. структура, объединяющая домены без смежных имен. Наглядно дерево и лес доменов представлены на рисунке 5.3.1.

Принципы группировки и именования доменов Windows соответствуют представлениям о доменах в сети Интернет. Такая ситуация не случайна, так как в Active Directory используется именование доменов на основе службы DNS. В плане назначения имен понятия интернет-домена и домена Windows совпадают.

В каждом домене дерева или леса обязательно создается свой контроллер домена. Для поиска и единой авторизации определяется также *глобальный каталог* (Global catalog, GC) — контроллер домена, который хранит полную копию всех объектов каталога своего домена и частичную копию объектов других доменов. Именно через сервер глобального каталога осуществляется аутентификация пользователей, которые зарегистрированы в некотором домене дерева или леса, но не в текущем домене.

Роль глобального каталога, как и роли FSMO, определяет особый статус некоторых контроллеров домена по отношению к остальным. Глобальный каталог, однако, не требует уникальности исполнителя. Эта роль может быть назначена нескольким контроллерам домена Windows.

Отметим также, что связь между доменами, не входящими в одно дерево или лес, можно также установить на основе *доверительных отношений* (trusts). Доверительные отношения — это механизм, при котором пользователи одного домена могут получать доступ к ресурсам другого домена.

Например, настроив двусторонние доверительные отношения между доменами двух организаций, мы получим компьютерную сеть, в которой сотрудники одной организации смогут проходить авторизацию и работать на компьютерах другой организации (и наоборот).

В дереве или лесе доменов доверительные отношения устанавливаются автоматически. Это двусторонние отношения между родительскими и дочерними доменами в структуре одного дерева или такие же отношения

между корневыми доменами разных деревьев в лесу. Благодаря транзитивности доверительных отношений эти отношения устанавливаются и между остальными доменами дерева или леса.

Внутренняя структура каталога Active Directory

Выше мы рассмотрели структурную организацию Active Directory — способы создания единого каталога на основе многих доменов и серверов. В данном разделе рассмотрим внутреннюю структуру сетевого каталога, определяющую способы организации и хранения данных.

Так, каталог Active Directory состоит из *элементов*, содержащих *атрибуты*, связанные с некоторым реальным *объектом*.

Существуют три категории объектов:

1) учетные записи пользователей и компьютеров;
2) ресурсы (папки, принтеры и др.);
3) службы.

Например, учетная запись пользователя (пользователь в данном случае — это объект) будет представлена в виде элемента, состоящего из набора атрибутов — имени, фамилии, описания, номера комнаты, номера телефона и др. (перечень атрибутов определяется *объектным классом*).

Структуру сетевого каталога могут также определять *организационные единицы* (OU, Organizational Units) — это специализированные объекты для группировки других объектов. Организационные единицы создаются администратором, они позволяют разделять домен на зоны административного управления, представлять элементы каталога в упорядоченном виде.

Наряду с понятием организационной единицы в Active Directory существует и понятие *контейнера*. Контейнеры и организационные единицы похожи по своему назначению (в связи с этим существует и некоторая неоднозначность терминологии), однако контейнеры создаются автоматически в процессе установки сетевого каталога, а организационные единицы могут создаваться и администраторами домена.

Основными контейнерами являются Computers и Users. В первый из них помещаются учетные записи компьютеров, а во второй — пользователей домена. При установке домена также автоматически создается и одна организационная единица Domain Controllers, куда помещаются учетные записи всех контроллеров домена.

Набор правил, описывающих структуру дерева элементов, объектные классы и типы атрибутов, называется *схемой каталога*. Схема каталога хранится в самом каталоге и ее можно изменять (создавать новые объектные классы, атрибуты и др.). Схема каталога гарантирует целостность хранимых данных.

Именование элементов каталога

Для именования элементов каталога используются различающиеся или канонические имена. Например, к учетной записи пользователя Alexander в домене fizmat.vspu.ru можно обратиться по следующим именам:

Различающееся имя: cn=Alexander, ou=Users, dc=fizmat, dc=vspu, dc=ru
Каноническое имя: //fizmat.vspu.ru/Users/Alexander

Заметим, что можно использовать относительные имена, если надо определить элемент внутри его контейнера. В данном случае к учетной записи пользователя Alexander можно обратиться по следующему относительному имени:

cn=Alexander

Каждый элемент каталога также имеет *глобально уникальный идентификатор* (GUID, Globally Unique Identifier), который назначается автоматически. Именно этот идентификатор используется операционной системой для распознавания элементов. Пример глобально уникального идентификатора приводится ниже:

{6F9619FF-8B86-D011-B42D-00CF4FC964FF}

Групповые политики

Групповая политика — это набор параметров и правил, в соответствии с которыми производится настройка рабочей среды Windows. Групповая политика создается в домене (т.е. на сервере — контроллере домена) в виде *объекта групповой политики* (GPO, Group Policy Object), связанного, как правило, с доменом или организационной единицей. Применяется политика — на всех компьютерах домена в соответствии с назначенной областью распространения.

Например, через групповые политики можно определить настройки рабочей среды пользователя (настройки фона и значков рабочего стола, параметры сети, расположение папок Мои документы, Мои рисунки и др.), перечень установленных программ (включая автоматическую установку отсутствующих программ), сценарии входа и выхода, параметры безопасности и др.

Набор параметров групповых политик соответствует стандартным настройкам ОС Windows и включенных в ее состав прикладных программ. В каждый новый выпуск Windows Server добавляются и новые параметры, необходимые для учета изменений в клиентских Windows. Возможно также и обновление шаблонов групповых политик без обновления самого сервера, а также установка новых шаблонов, необходимых для настройки программного обеспечения, не входящего в состав Windows.

Правила и параметры объектов групповой политики состоят из двух частей:

- конфигурация компьютера;
- конфигурация пользователя.

В первом случае в групповой политике определяются настройки всего компьютера в целом (операционной системы, системных служб, устройств, сети, безопасности и др.). Эти параметры применяются в момент включения компьютера, еще до авторизации пользователя.

Во втором случае определяются настройки программного окружения пользователя (параметры рабочей среды, прикладных программ, перенаправление папок и др.). Эти параметры применяются в момент авторизации пользователя (в процессе входа в систему).

Важной особенностью настроек пользователя в объекте групповой политики является то, что эти настройки применяются в момент, когда уже известно имя пользователя и его права. Эти данные можно использовать, чтобы персонифицировать настройки разных пользователей (создавая, например, сценарии входа и выхода, учитывающие имя пользователя при запуске разных программ).

По умолчанию в процессе развертывания домена создается групповая политика Default Domain Policy. Эта политика относится ко всему домену и

ее можно изменять. Можно также добавлять новые политики — к домену, контейнеру или организационной единице (но не к конкретному элементу).

Следует понимать, что в каждом случае может быть назначено несколько объектов групповой политики. Если возникают конфликты назначенных параметров, то применяется политика, которая находится «ближе» к объекту или имеет более высокий приоритет (для политик одного уровня — относящихся к одному и тому же контейнеру).

Например, если в групповой политике, назначенной для контейнера Users, указывается картинка рабочего стола images1.jpg, а в контейнере Users есть организационная единица «Читатели библиотеки», где групповой политикой определена картинка images2.jpg, то в итоге читатели библиотеки будут получать вторую картинку, т.к. она к ним расположена «ближе». Подобные конфликты в групповых политиках могут возникать и в других ситуациях – это не является ошибкой, важно лишь понимать приоритет применения политик.

Несмотря на то что групповые политики назначаются лишь группам объектов сетевого каталога, область применения этих политик может также определяться и при помощи:

1) списков контроля доступа (ACL). Подобно тому как эти списки используются для определения уровня доступа к файлам и папкам, их можно использовать и для определения применимости групповой политики к группе безопасности или конкретному пользователю. Через списки контроля доступа, таким образом, групповые политики можно «назначать» отдельным группам безопасности или пользователям домена;
2) фильтров WMI (Windows Management Instrumentation — инструментарий управления Windows). В этом случае можно гибко анализировать характеристики компьютеров при применении групповых политик — учитывать версии операционных систем, параметры аппаратного обеспечения компьютера и др.

Например, через фильтры WMI можно указать, что такие-то параметры групповой политики должны применяться только для компьютеров под управлением версии операционной системы, не меньше, чем Windows 8, а такой-то программный пакет должен автоматически устанавливаться только на компьютерах, где есть как минимум 4 Гб оперативной памяти.

Таким образом, групповые политики, позволяют полностью автоматизировать процесс настройки рабочих станций в домене Windows. Фактически, такая настройка будет связана только с установкой на рабочие станции операционных систем и включением этих компьютеров в домен. В дальнейшем через механизм групповых политик на компьютерах в автоматическом режиме могут быть установлены необходимые приложения, настроены различные параметры операционной системы.

Подводя итог данному разделу, скажем, что служба каталогов Active Directory обеспечивает мощные и гибкие возможности организации работы компьютерных сетей в соответствии с моделью домена Windows. Эта служба с успехом может использоваться в корпоративных сетях, обеспечивая единую регистрацию и управление, высокий уровень безопасности, широкие возможности по масштабированию сети.

5.4. Системные службы в локальных сетях Windows

Выше мы рассмотрели особенности реализации службы Active Directory как технологической основы доменов Windows, а также службы DNS и DHCP как две важнейшие службы, которые являются системными в компьютерах сетях. Вместе с тем наряду с этими службами в локальных сетях Windows реализованы и другие службы, обеспечивающие сервисы, специфичные именно для рассматриваемого нами вида сетей. К основным из таких служб можно отнести следующие.

1. WINS.
2. Службу обозревателя (Browser Service).
3. Распределенную файловую систему DFS.
4. Службу маршрутизации и удаленного доступа.
5. Службу терминалов.

Кратко рассмотрим назначение и особенности реализации каждой из указанных служб. Все эти службы могут быть развернуты на компьютере под управлением Windows Server.

Служба WINS

WINS (Windows Internet Name Service, служба имен Интернета Windows) — это служба регистрации и разрешения имен компьютеров, которая сопоставляет NetBIOS-имена компьютеров с IP-адресами.

По сути и своему назначению служба WINS — это старый аналог службы DNS, которая использовалась в качестве основной службы имен в локальных сетях до 2000 года. Как и DNS, служба WINS предполагает наличие в локальной сети WINS-сервера, на котором ведется список компьютеров и назначенных им IP-адресов. Рабочие станции сети могут обращаться к серверу WINS для получения IP-адресов тех машин, для которых им известны только NetBIOS-имена.

После обновления стандарта DNS необходимость в службе WINS отпала. Распознавание имен компьютеров локальной сети, равно как и узлов Интернета, реализуется в настоящее время на основе DNS. Тем не менее возможность использования WINS сохранилась и в современных версиях Windows. Такая поддержка была оставлена для обеспечения совместимости — возможности использования сетей, где одновременно используются как современные компьютеры, так и старые, работающие под управлением версий Windows, выпущенных до 2000 года.

Служба обозревателя

Основное назначение *службы обозревателя* (Browser Service) заключается в составлении списка компьютеров, доступных в настоящее время в локальной сети, а также предоставлении этого списка клиентам, просматривающим сеть через сетевое окружение (Сетевое окружение → Вся сеть). Служба обозревателя была впервые реализована в самой первой версии Windows, ориентированной на сетевую работу (Windows for Workgroups 3.1), с самого начала рассчитана на использование в сетях, где может отсутствовать сервер.

Согласно архитектуре этой службы для ведения списка компьютеров назначается главный обозреватель (Master Browser) сети, а также один или несколько резервных обозревателей (Backup Browser). Процедура назначения обозревателей осуществляется через выборы, которые могут проводиться в момент включения или выключения компьютеров. Как правило, на роль обозревателей выбирается контроллер домена либо (в его отсутствие) — компьютер со старшей версией ОС.

Обновление списка производится через запросы рабочих станций, которые широковещательным способом рассылаются в момент включения или выключения компьютера. Обновление обязательно производится на главном обозревателе, после чего списки обновляются и на резервных обозревателях. Как главный, так и резервные обозреватели в дальнейшем используются для получения информации о доступных компьютерах всеми остальными компьютерами сети.

Таким образом, служба обозревателя может работать как в доменных, так и в одноранговых сетях. Она не требует специальной настройки со стороны администратора — выбор обозревателей, составление списков, их предоставление рабочим станциям осуществляются автоматически.

Архитектура службы обозревателя, предполагающая настройку и функционирование службы в автоматическом режиме, не всегда позволяет обеспечить стабильность работы, актуальность и достоверность предоставляемой информации.

Проблемы могут возникать из-за аварийных выключений компьютеров в сети, задержек, связанных с процедурами выбора обозревателей и обновления списков доступных машин, ограничений распространения информации лишь одним сегментом локальной сети и др. При возникновении таких проблем вы не сможете обращаться к компьютерам через сетевое окружение (хотя сами компьютеры будут доступны в сети) либо вам будут предлагаться компьютеры, работать с которыми невозможно.

Служба обозревателя не рекомендуется к использованию в больших сетях. Поиск необходимых сетевых ресурсов предлагается планировать на основе Active Directory или службы DFS.

Распределенная файловая система DFS

DFS (Distributed File System, распределенная файловая система) — сетевая служба, которая используется для упрощения доступа и управления файлами, физически распределенными по сети. Данная служба позволяет создавать в компьютерной сети ресурсы, объединяющие сетевые папки разных серверов.

Например, папки public, install и music на компьютерах KROSH, BARASH и NUSHA (рис. 5.4.1), можно представить в виде вложенных папок некоторой одной общей папки (в приведенном примере папки dfs) на компьютере SERVER. В этом случае ко всем папкам, физически

расположенным на нескольких компьютерах, можно будет обращаться по единому имени \\SERVER\dfs.

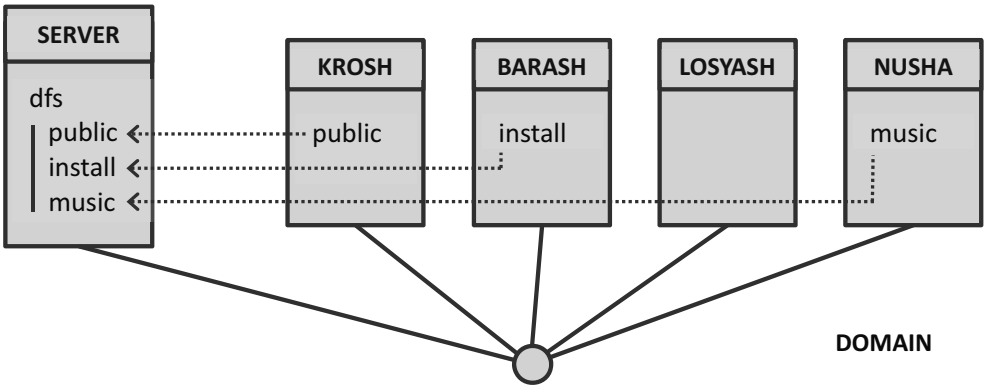


Рис. 5.4.1. Пример объединения папок при помощи DFS

Согласно терминологии распределенной файловой системы DFS, папки \\KROSH\public, \\BARASH\install и \\NUSHA\music называют целевыми папками, а \\SERVER\dfs\public (\\DOMAIN\dfs\public) и др. — ссылками DFS.

Заметим, что DFS может быть реализована двумя способами:

- с изолированным корнем;
- с доменным корнем.

В первом случае папка со ссылками DFS доступна как сетевой ресурс некоторого конкретного сервера (\\SERVER\dfs). Во втором случае, допустимом, как понятно из названия, в домене Windows, к папке DFS можно обращаться не по имени сервера, а по имени домена. В данном случае – \\DOMAIN\dfs.

Подобная организация доступа к папкам в компьютерной сети значительно упрощает работу как пользователям, так и администраторам. Пользовали не должны запоминать имена многочисленных компьютеров, пользоваться инструментом Вся сеть, сохранять ссылки на все ресурсы, которые им необходимы. Администраторы получают возможность вносить изменения в структуру сети (заменять компьютеры, переносить сетевые папки на другие серверы), не беспокоясь о том, что это из-за изменения сетевых имен приведет к нарушению работы каких-то служб или создаст неудобства пользователям.

Кроме этого, служба DFS поддерживает также механизм репликации — можно создавать несколько целевых папок для одних и тех же ссылок DFS. В этом случае пользователи, обратившиеся к такой папке, будут перенаправлены на один из серверов, где хранится копия целевой папки. Такой механизм обеспечивает надежность работы с сетевым ресурсом (папка будет представлена в сети, даже если какие-то физические серверы, где расположены данные, будут недоступны), а также повышение производительности за счет распределения нагрузки на несколько машин.

Служба маршрутизации и удаленного доступа

Служба маршрутизации и удаленного доступа (RRAS, Routing and Remote Access Service) поддерживает связь удаленных пользователей или сетей. Она используется в случаях:

- подключения локальной сети к Интернету (прямая маршрутизация или NAT);
- подключения компьютера к удаленной локальной сети или другому компьютеру через Интернет (модем или VPN);
- объединения территориально разделенных фрагментов компьютерной сети.

Служба маршрутизации и удаленного доступа, таким образом, реализует на основе Windows Server рассмотренные нами ранее способы подключения локальных сетей к Интернету, а также VPN-соединения компьютеров и сетей. В частности, именно эта служба используется для создания сервера общего доступа на основе NAT, а также сервера VPN. В последнем случае большим преимуществом будет легкая интеграция VPN-сервера и домена Windows, что позволит использовать при удаленных подключениях учетные записи пользователей, зарегистрированных в домене.

Служба терминалов

Служба терминалов обеспечивает доступ к отдельным приложениям или рабочему столу Windows Server через компьютерную сеть. Данная служба создает возможность работы с удаленным компьютером как с локальными. Все действия при терминальном доступе выполняются на удаленном сервере (запуск программ, сохранение файлов, работа с аппаратными устройствами и др.), а по сети передаются только сведения,

вводимые с помощью клавиатуры и мыши, а также отображающиеся на экране.

В среде Windows предполагаются два режима работы службы терминалов:

- режим администрирования;
- режим приложений.

В первом случае допускается одновременное подключение к серверу не более двух пользователей. Как следует из названия, режим используется для управления удаленным сервером – его настройки и выполнения других административных операций.

Во втором случае количество пользователей не ограничено, однако требуется дополнительное лицензирование сервера. Режим приложений может использоваться для быстрого развертывания программ в корпоративной сети, снижения нагрузки на сеть, построения сетей на основе тонких клиентов.

Заметим, что в обоих случаях разные пользователи могут работать на компьютере в одно и то же время – каждый пользователь будет видеть только свой сеанс. Это отличает службу терминалов, реализованную в Windows Server, от технологии удаленного рабочего стола в клиентских версиях Windows.

Подключиться к удаленному серверу можно при помощи инструмента «Подключение к удаленному рабочему столу», входящему в перечень стандартных программ всех современных версий Windows. Подобные программы есть и для других операционных систем (в том числе для мобильных устройств). Подключение к серверу терминалов во всех случаях осуществляется с использованием протокола RDP (Remote Desktop Protocol).

Возможность терминальной работы с сервером Windows широко используется в облачной платформе компании Microsoft — Microsoft Azure. Данная платформа позволяет использовать виртуальные машины с Windows Server (и рядом других операционных систем), запущенные в облаке на базе сети глобальных дата-центров Microsoft.

Фактически, вместо приобретения физической машины для создания сервера в своей компьютерной сети вам предлагается приобрести (арендовать) виртуальный сервер с нужными характеристиками, работа с которым будет производиться через подключение к удаленному рабочему столу.

Преимущества такого подхода заключаются в снижении затрат на создание и обслуживание сервера, наличии удобных возможностей управлении ресурсами машины в зависимости от текущих нагрузок, отсутствии проблем физического размещения, электроснабжения, охлаждения и обеспечения сохранности сложного оборудования.

5.5. Консоль управления и журнал событий

Настройка многочисленных служб и параметров Windows, как рассмотренных нами, так и многих других, осуществляется с использованием универсального инструмента — *консоли управления Microsoft* (MMC, Microsoft Management Console).

MMC — это средство Windows, которое предоставляет системным приложениям графический интерфейс. Сама настройка операционной системы, конкретных приложений и служб производится при помощи *оснасток* MMC.

Доступ к оснасткам можно получить:

1) через ссылки в разделе «Администрирование» панели управления или главного меню, а также через контекстное меню различных объектов Windows;

2) через программу «Консоль управления» (mmc.exe), которая позволяет получить доступ ко всем имеющимся на компьютере оснасткам;

3) через командную строку, открывая необходимую оснастку по ее прямому имени (например, compmgmt.msc — оснастка «Управление компьютером»).

Унифицированный способ работы с оснастками позволяет создать в Windows единую среду управления. При этом консоль управления обеспечивает доступ к параметрам не только локального компьютера, на котором открываются соответствующие оснастки. Имея необходимые права, через консоль управления Microsoft вы сможете управлять и удаленным компьютером.

Еще одним инструментом администратора, незаменимым для наблюдения за работоспособностью системы и устранения возникших неполадок, является *журнал событий* (Event Log).

Журнал событий Windows — это стандартный способ протоколирования различных сообщений от служб и операционной системы в целом о важных программных и аппаратных событиях. Журнал событий объединяет сообщения от разных служб и компонентов Windows в одном

хранилище, что позволяет проводить диагностику системы, поддерживать безопасность и устранять ошибки.

Журнал событий разделяется на отдельные файлы (журналы). К основным из них относятся:

- *«Приложения»* — события приложений и служб (например, статистика работы приложений);
- *«Безопасность»* — события, связанные с безопасностью системы (например, вход и выход из системы);
- *«Система»* — события операционной системы и ее компонентов (например, неудачи при запусках служб или инициализации драйверов).

Выше представлен далеко не полный перечень журналов событий. Для разных версий и конфигураций Windows этот перечень может дополняться своими компонентами. Существует также возможность создания и дополнительных журналов.

Сообщения, которые фиксируются в журнале событий, могут относиться к одному из предопределенных типов:

- *Информация* — успешные операции, которые важны для мониторинга системы (например, успешное завершение репликации);
- *Предупреждение* — проблемы, которые не требуют немедленного вмешательства, но могут привести к другим ошибкам (например, достижение порогового значения дисковой квоты);
- *Ошибка* — существенные проблемы, приводящие к потере функциональности или данных (например, невозможность запуска службы);
- *Аудит успеха* — события безопасности, которые происходят при успешном обращении к аудируемым ресурсам (например, успешный вход в систему);
- *Аудит отказа* — события безопасности, которые происходят при неуспешном обращении к аудируемым ресурсам (например, попытка входа с указанием ошибочного пароля или попытка открыть файл, не имея соответствующих прав доступа).

В описании каждого события, помимо, собственно, описания ситуации, указывается источник, дата и время, тип, код события и др. Более подробно о возникшей проблемной ситуации, ее причинах и способах устранения, как

правило, можно узнать на сайте технической поддержки Microsoft (http://support.microsoft.com). Для поиска такой информации используйте код события.

Журнал событий Windows реализован в виде одноименной службы. Просмотр информации журнала событий осуществляется через оснастку «Просмотр событий» консоли управления Microsoft. Эта оснастка доступна в разделе «Управление» объекта «Компьютер», а также в перечне оснасток раздела «Администрирование» панели управления. Помимо этого, как и другие оснастки MMC, просмотр событий можно вызвать и из командной строки (eventvwr.msc).

Вопросы и задания

Windows как многопользовательская система

Опишите основные характеристики Windows как многопользовательской системы.

Что такое учетные записи пользователя и группы? Как применяются записи пользователей и групп для настройки параметров безопасности?

В чем принципиальное отличие записей администратора, опытного пользователя, пользователя и гостя?

Что такое специальные группы безопасности? Для чего они применяются?

Назовите стандартные и дополнительные атрибуты доступа к файлам и папкам.

Что означает накопительный характер атрибутов доступа? Как проявляется приоритет запрета над разрешением?

Что такое профиль пользователя? Какие компоненты содержатся в профиле?

Где хранится профиль пользователя? Что такое перемещаемый профиль и в чем заключаются особенности работы с таким профилем?

Рабочая группа и домен Windows

Опишите основные принципы организации сети как рабочей группы Windows.

Каким образом в рабочей группе осуществляется управление доступом к сетевым ресурсам? В чем достоинства и недостатки такого подхода?

Что такое домашняя группа Windows? Для решения каких задач предназначены домашние группы?

Что такое домен Windows? Какие преимущества имеют доменные сети по отношению к сетям на основе рабочих групп?

Где хранятся учетные записи пользователей в домене Windows? Как осуществляется авторизация пользователей и управление доступом к сетевым ресурсам?

Что такое контроллер домена Windows? Какие функции выполняет контроллер домена? Какое количество контроллеров может присутствовать в домене?

Сетевой каталог Active Directory

Опишите принципы организации сетевого каталога Active Directory. Для чего предназначен сетевой каталог?

Какую структуру имеет сетевой каталог? Что такое дерево и лес доменов? Что такое сайт Active Directory?

Какова внутренняя структура Active Directory? Поясните такие понятия, как атрибут, элемент, объектный класс, объект, организационная единица сетевого каталога. Что такое схема каталога?

Каким образом можно получить доступ к элементу каталога? Назовите допустимые способы именования элементов.

Что такое групповая политика? Из каких двух частей состоит объект группой политики?

Как используются групповые политики для управления доменом? Каким образом можно уточнить перечень объектов, к которым применяется групповая политика?

Системные службы в локальных сетях Windows

Для чего предназначена служба WINS? Почему эта служба считается устаревшей? Как в настоящее время решаются задачи, ранее возлагавшиеся на службу WINS?

Что такое служба обозревателя, в каких случаях она применяется? Опишите общие принципы внутренней организации данной службы. Какие проблемы могут возникать в процессе ее работы?

Опишите предназначение и основные принципы внутренней организации службы DFS. В чем отличие развертывания этой службы на отдельном сервере и в домене Windows? Каким образом данная служба позволяет повысить производительность и отказоустойчивость работы сети?

Для чего предназначена служба маршрутизации и удаленного доступа? Опишите круг задач, решаемых с использованием данной службы.

Что такое служба терминалов? В каких двух режимах может работать данная служба?

Консоль управления и журнал событий

Что такое консоль управления Windows? В каких случаях она применяется?

Как можно получить доступ к оснасткам консоли управления? Назовите основные оснастки, с которыми работает администратор сервера.

Каким образом ОС Windows ведет протокол ошибок в системе, записывает предупреждения и сообщения различных приложений?

Какова структура журнала событий? Каким образом в журнале можно анализировать характер сообщений?

Раздел 6. Физическое построение локальных сетей

Предыдущие разделы пособия касались технологий построения локальных сетей на сетевом, транспортном и прикладном уровнях. Практическое построение локальной сети потребует, несомненно, и создания физической инфраструктуры, на основе которой реализуется физический и канальный уровень сети. В данном разделе рассматриваются технологии кабельных сетей Ethernet, беспроводных сетей Wi-Fi, а также виртуальных локальных сетей. Материалы раздела помогут вам разобраться в современных и перспективных направлениях развития технологий физического построения локальных сетей. Сведения практического характера, изложенные в разделе, пригодятся и для реального построения своей собственной сети.

6.1. Технологии и стандарты сетей Ethernet

Ethernet — это технология построения кабельных локальных сетей. Стандарты Ethernet описывают реализацию физического и канального уровней модели OSI. Первый стандарт Ethernet был опубликован в 1980 году, после этого времени технологии Ethernet много раз совершенствовались и изменялись.

Ethernet в момент своего появления не была самой совершенной технологией, однако ее отличала простота и низкая стоимость, что соответствовало запросам пользователей, предопределило коммерческий успех. Основную конкуренцию Ethernet составляли сети Token ring и ARCNET, однако они оказались менее успешными в коммерческом плане.

Новые поколения Ethernet лишены изначальных проблем безопасности, прогнозируемости и устойчивости локальных сетей. При этом, как и раньше, преимуществами Ethernet остаются производительность и невысокая стоимость оборудования. В результате Ethernet сейчас используется в подавляющем большинстве случаев.

Существующие альтернативы Ethernet применимы лишь к решению каких-либо узких и весьма специфичных задач. Например, это сети InfiniBand, которые разработаны для суперкомпьютеров и построения кластеров очень высокой производительности.

Сети Ethernet на разделяемой среде

Изначально Ethernet — это сеть на разделяемой среде с опознаванием несущей и обнаружением коллизий (метод CSMA/CD). Согласно стандарту сети Ethernet каждый узел имеет свой уникальный аппаратный адрес (MAC-адрес), используемый для идентификации отправителя и получателя. Адрес состоит из 6 байт и назначается сетевому адаптеру на заводе-изготовителе. Пример аппаратного адреса приводится ниже:

00-25-22-86-E1-38

Для того чтобы обеспечить уникальность аппаратных адресов, потребовалось создать координирующий комитет IEEE Registration Authority, который выдает диапазоны допустимых аппаратных адресов заводам-изготовителям. Конкретного производителя сетевого адаптера можно узнать по первым трем байтам аппаратного адреса.

Аппаратные адреса в силу своей уникальности и постоянства иногда используются в различных системах управления доступом. Такой способ, однако, не может обеспечить высокой надежности, так как замена аппаратных адресов весьма часто возможна и программным способом. Злоумышленник может подменить свой аппаратный адрес, «представившись» узлом, которому предоставлены какие-то особые привилегии.

Информация в сетях Ethernet передается кадрами. Формат кадра (табл. 6.1.1) включает в себя преамбулу (preamble), начальный ограничитель (SD), адрес отправителя (DA), адрес получателя (SA), идентификатор протокола (T), данные (Data) и контрольную сумму (FSC). Нижняя строка таблицы показывает размер соответствующего поля в байтах.

Кадры передаются без установки соединения и повторной доставки утерянных или искаженных кадров (указанные проблемы решаются на более высоких уровнях модели OSI).

Таблица 6.1.1

Preamble	SD	DA	SA	T	Data	FSC
		Заголовок MAC				
7	1	6	6	2	46-1500	4

Процесс отправки и получения кадров согласно методу CSMA/CD реализуется следующим образом.

Отправка кадров.

1. Кадр данных готовится для передачи.
2. Анализируется среда передачи — идет ли пересылка информации другими узлами?
3. Когда среда передачи освобождается, кадр данных пересылается в сеть.
4. В процессе пересылки кадра анализируется ситуация — была ли в это время какая-либо попытка передачи информации другим узлом? Если была, то это отмечается как коллизия (см. п. 5). В противном случае считается, что передача завершена успешно. После ожидания времени межкадрового интервала в сеть отправляется новый кадр, готовый для передачи.
5. В случае обнаружения коллизии станция-отправитель вычисляет время задержки (случайное число, которое увеличивается по мере возникновения последующих попыток пересылки кадра) и повторно отправляет кадр данных в сеть. Процесс повторяется до момента успешной отправки кадра данных либо до достижения предельного числа попыток повторной передачи (16 раз).

Таким образом, станция-отправитель пересылает свою информацию порциями в те моменты, когда сеть не используется другими узлами. При этом, однако, могут возникать ситуации, когда сразу несколько станций, зафиксировав свободное состояние среды передачи, пожелают одновременно воспользоваться этим для пересылки своей информации. В этом случае пересылка кадров данных становится невозможной, а сама ситуация отмечается как коллизия. Для исправления коллизий разные станции приостанавливают пересылку на некоторое время, после чего повторяют попытки передачи. Так как время ожидания выбирается случайным, с большой вероятностью разные станции начнут новую пересылку в разное время, в результате чего повторная коллизия для данных кадров данных не произойдет.

Простота реализации Ethernet на разделяемой среде заключается в том, что сеть не пытается предотвратить коллизии, а лишь имеет средства обнаружения таких ситуаций и их исправления путем повторной отправки информации. Это значительно удешевляет технологию (т.к. не требует специальных средств, обеспечивающих координацию

работы различных станций компьютерной сети), однако приводит к появлению дополнительного трафика (создается проблема снежного кома — дополнительный трафик увеличивает число коллизий, а те, в свою очередь, создают новый дополнительный трафик), не позволяет надежно прогнозировать время передачи и гарантировать стабильность этого времени в компьютерной сети.

Следует отметить, что такая ситуация не оказалась критичной в большинстве случаев применения Ethernet. Данному обстоятельству способствует изначально низкая удельная загруженность локальных сетей, а также отсутствие требований гарантированного времени доставки кадров данных в наиболее массовом секторе офисных локальных сетей.

Получение кадров.

1. Станция компьютерной сети, постоянно анализируя состояние среды передачи, фиксирует наличие приемного сигнала. Если такой сигнал есть, станция ожидает начальный ограничитель кадра и получает новую порцию данных.
2. Для каждого полученного кадра проверяется контрольная сумма и адрес назначения. Если контрольная сумма показывает ошибку либо адрес назначения не совпадает с адресом станции (или широковещательным адресом), кадр данных отбрасывается.
3. Те кадры данных, которые отброшены не были, передаются протоколам более высокого уровня для дальнейшей обработки.

Как видно из описания, в сетях Ethernet на разделяемой среде пересылаемые кадры данных получают все рабочие станции компьютерной сети. Эти станции, однако, должны отбросить те кадры, которые предназначены не им, даже если эти кадры были получены без ошибок. Данное обстоятельство, являющееся следствием использования единой разделяемой среды, создает ряд серьезных проблем, к которым можно отнести:

- проблемы безопасности, т.к. возможен перехват любых кадров данных вне зависимости от адресов их назначения;
- снижение производительности сети за счет того, что любая пара компьютеров, обмениваясь данными, «загружает» сразу всю сеть;
- выбор скорости передачи по самому «слабому» компьютеру во всей сети.

Коммутируемые сети Ethernet

Описанный выше метод передачи данных относится к первым поколениям сетей Ethernet. Это сети, основанные на коаксиальном кабеле (топология «шина») либо на более современном кабеле «витая пара» с использованием *концентратора* (физическая топология «звезда», но логическая топология «шина»). Новые поколения Ethernet, основанные на *коммутаторах*, позволяют реализовать другую схему передачи данных, исключающую появление коллизий и необходимость пересылки кадров данных абсолютно всем компьютерам сети.

Коммутатор (*switch*, *свич*) — это высокоскоростной многопортовый мост. Данное устройство предназначено для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов. Данные сегменты имеют как физическую, так и логическую топологию «звезда». Коммутаторы отдельных сегментов могут соединяться между собой, в результате чего возможно построение сетей древовидной топологии.

Коммутатор работает на канальном уровне модели OSI, он способен запоминать и анализировать MAC-адреса пересылаемых пакетов. Когда коммутатору требуется переслать очередной кадр данных, он его направляет не всем остальным компьютерам сети, а лишь на тот свой порт, к которому подключен компьютер-получатель. В результате этого коммутируемые сети Ethernet принципиально меняют схему передачи данных, так как в них создаются независимые виртуальные каналы связи между парами станций в компьютерной сети. При этом каждый компьютер на физическом уровне обменивается информацией лишь с одним устройством сети — коммутатором, к которому он подключен. Последнее обстоятельство позволяет полностью избежать возникновения коллизий.

Маршрут следования кадров данных определяется коммутаторами на основе имеющихся таблиц продвижения. В подавляющем большинстве случаев такие таблицы строятся коммутаторами автоматически на основе наблюдения за трафиком (используется метод «затопления» сети). В результате этого коммутатор способен работать сам, не требуя какой-либо предварительной настройки.

Таким образом, коммутируемые сети Ethernet позволили преодолеть наиболее серьезные проблемы сетей на основе разделяемой среды. К достоинствам коммутируемых сетей Ethernet можно отнести:

- отсутствие коллизий;

- локализацию передаваемых данных лишь в пределах пары компьютеров — отправителя и получателя;
- возможность одновременной пересылки данных между различными парами компьютеров локальной сети;
- наличие полного дуплексного (Full-duplex) режима работы, при котором кадры данных могут одновременно отправляться и приниматься;
- возможность выбора скорости передачи на основе наименьшей из пары компьютеров, а не всех имеющихся компьютеров сети.

Оборудование сетей Ethernet

Итак, для построения локальной сети на основе современных стандартов Ethernet требуется наличие сетевых адаптеров, один или несколько коммутаторов, а также кабель для физического соединения этих устройств.

Сетевые адаптеры, как правило, интегрированы с системной платой компьютера и являются одним из интерфейсов, обеспечивающим подключение внешних устройств. Если на компьютере нет требуемого встроенного сетевого адаптера, то такой адаптер можно установить в виде платы расширения либо устройства USB. Допускается одновременная установка и нескольких адаптеров — такое решение, как правило, применяется на серверных компьютерах, что требуется для подключения сервера к разным сетям, либо увеличения пропускной способности путем агрегирования каналов. Внешний вид гнезда сетевого адаптера для подключения кабеля «витая пара» представлен на рисунке 6.1.1.

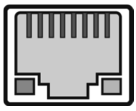


Рис. 6.1.1. Гнездо сетевого адаптера
для подключения кабеля «витая пара»

Выбирая сетевой адаптер, вам придется принимать во внимание следующие обстоятельства.

1. Желаемая *скорость передачи информации*. В настоящее время наиболее популярным стандартом для вновь создаваемых сетей является Gigabit Ethernet (скорость передачи 1 Гбит/с), однако все

еще актуальным является и стандарт Fast Ethernet (100 Мбит/с), а также возможно использование и более современных стандартов, таких как 10G Ethernet (10 Гбит/с).

2. *Интерфейс платы расширения*, поддерживаемый системной платой компьютера (PCI, PCI Express, ExpressCard или др.). Ошибка в выборе интерфейса не позволит физически установить новый адаптер либо приведет к снижению производительности системы (если из нескольких имеющихся интерфейсов выбран менее скоростной).
3. Характеристики уже имеющегося оборудования. Очевидно, что нет смысла устанавливать оптоволоконный сетевой адаптер там, где используется кабель «витая пара», однако стоит учитывать и другие, не столь очевидные параметры, как, например, категория используемой витой пары, типы разъемов оптоволоконного кабеля, перечень скоростей, поддерживаемых коммутатором и др.
4. Характер создаваемой системы. Например, при создании сервера с большой нагрузкой разумно использовать специальный сетевой адаптер, который сможет обеспечить высокую производительность, а также даст возможность провести особую настройку доступа к сети (поддержка VLAN, агрегирование каналов и др.).

Сетевой коммутатор является центральным сетевым устройством, именно от его характеристик во многом будут зависеть параметры быстродействия и структурной организации компьютерной сети. Самой понятной характеристикой коммутатора, принимаемой во внимание при выборе того или иного устройства, является *количество портов* – общее число разъемов, к которым можно подключить сетевые устройства. Как правило, такое количество исчисляется значениями в 4, 5, 8, 16, 24, 48 единиц. На рисунке 6.1.2. представлен коммутатор с 16 портами.

Рис. 6.1.2. Сетевой коммутатор

Другая важная и понятная характеристика — это *базовая скорость передачи данных*, которая означает скорость работы каждого из имеющихся портов. Чаще всего будет поддерживаться сразу несколько скоростей (происходит автоматический выбор наиболее высокой скорости передачи, поддерживаемой как коммутатором, так и подключенным устройством). В отдельный случаях — некоторые порты коммутатора могут поддерживать более высокую скорость, чем остальные. Такие коммутаторы дают возможность организовать высокоскоростное подключение к внешней сети или к серверу, сохраняя при этом стоимость устройства в более низком ценовом диапазоне.

Базовую скорость передачи данных следует отличать от *внутренней пропускной способности* коммутатора. Внутренняя пропускная способность — это скорость передачи информации по системной шине коммутатора. Часто она бывает ниже, чем совокупная пропускная способность всех портов (особенно если портов много).

В этой связи если сразу несколько компьютеров, подключенных к разным портам коммутатора, начнут интенсивно обмениваться информацией, то фактическая скорость передачи может оказаться ограниченной не базовой скоростью передачи, а пропускной способностью коммутатора. Таким образом, на данный параметр следует обращать внимание при создании высоконагруженных сетей.

Существует большое количество и других параметров, отличающих одни коммутаторы от других. Среди всего многообразия, в дополнение к уже описанным характеристикам, выделим лишь три характеристики, которые обычно также оказывают существенное влияние на выбор того или иного устройства:

1) наличие или отсутствие дополнительных интерфейсов (например, портов для SFP-трансиверов, которые обеспечивают подключение оптоволоконного кабеля и др.);
2) тип исполнения корпуса коммутатора (коммутаторы для установки в телекоммуникационную стойку, а также коммутаторы настольного исполнения);
3) наличие возможностей ручного управления (неуправляемые и управляемые коммутаторы), а также мониторинга коммутатора через компьютерную сеть.

Наличие ручного управления коммутатором дает широкие возможности гибкой настройки структуры и параметров доступа в локальной сети.

Так, *неуправляемые коммутаторы* — простые автономные устройства, которые работают исключительно на основе автоматически создаваемых таблиц продвижения кадров. Такие устройства не требуют настройки, они сразу способны выполнять свою функцию, обеспечивая логическое соединение компьютеров в соответствии с имеющейся физической топологией.

Управляемые коммутаторы также способны работать в автономном режиме, однако в дополнение к этому позволяют производить и расширенную настройку. Такая настройка может быть связана с указанием каких-либо правил физического доступа к узлам компьютерной сети, привязкой конкретных аппаратных адресов к портам коммутатора, созданием логически разделенных сегментов, организацией виртуальных сетей (VLAN), анализом трафика и др. Управляемый коммутатор, таким образом, позволяет применять особые правила следования трафика в компьютерной сети, фактически создавая новую логическую структуру сети на основе имеющейся физической инфраструктуры.

Как было сказано ранее, помимо коммутатора (switch, свич), в качестве связывающего устройства в локальной сети может также использоваться и *концентратор* (hub, хаб). Концентратор — это более простое устройство, которое работает на физическом уровне модели OSI. Несмотря на физическую топологию «звезда», концентратор логически может обеспечить лишь топологию «шина». В этой связи данное устройство является устаревшим и в новых сетях Ethernet не применяется.

С коммутатором Ethernet могут путать также и интеллектуальное устройство — *маршрутизатор* (см. раздел 3.2). Данному обстоятельству способствует то, что маршрутизатором часто называют также устройство, соединяющее в одном корпусе несколько устройств — собственно маршрутизатор, коммутатор и (зачастую) точку доступа беспроводной сети. Такое устройство действительно позволяет создать локальную сеть, однако функции собственно маршрутизатора в этом случае будут не востребованы. Маршрутизатор в подобных совмещенных устройствах применяется в тех случаях, когда надо обеспечить доступ к сети Интернет.

Кабель в сетях Ethernet является средой передачи, он обеспечивает связь сетевых узлов. Принципиальным решением при выборе кабеля будет выбор типа кабеля — *витая пара* или *оптоволокно*.

Витая пара — это простое и недорогое решение, которое применяется для соединения устройств, как правило, на расстоянии до 100 метров со скоростью передачи данных до 1 Гбит/с. Оптоволоконный кабель необходим там, где требуется реализовать более протяженную линию связи (до десятков километров) либо получить более высокую скорость передачи (10 Гбит/с и выше).

Первое поколение сетей Ethernet было рассчитано на *коаксиальный* кабель, который выпускался в двух исполнениях – как «толстый» и «тонкий» коаксиал. Коаксиальный кабель Ethernet по своему устройству аналогичен кабелю антенны телевизора (центральная жила и внешний экран-проводник), он позволял создать сеть с шинной топологией. Данный тип кабеля, равно как и шинная топология, в современных сетях Ethernet не применяется, поэтому подробно рассматривать такой тип кабеля и соответствующее оборудование на страницах данного пособия мы не будем.

Кабель «витая пара» представляет собой совокупность нескольких пар скрученных между собой проводников (рис. 6.1.3). Проводники изолированы и имеют особую цветовую маркировку.

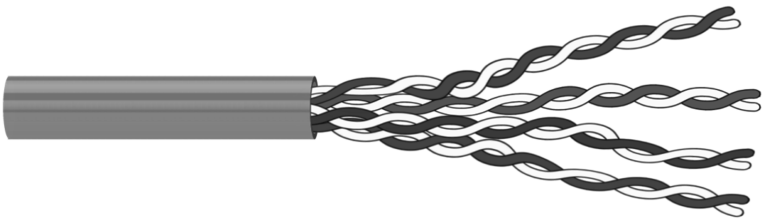


Рис. 6.1.3. Кабель «витая пара»

Скручивание проводников производится с целью уменьшения электромагнитных помех от внешних источников, а также взаимных наводок внутри самого кабеля между парами проводников. При этом скручивание различных пар производится с различным шагом, что уменьшает взаимное влияние внутри кабеля и не связанных между собой проводников. В итоге простое решение скручивания проводников позволяет существенно

увеличить протяженность кабеля, повысить скорость передачи, снизить уровень помех.

Витая пара, используемая в локальных сетях Ethernet, имеет 4 пары, т.е. 8 проводников. Несмотря на это, однако, в сетях Fast Ethernet (100 Мбит/с) для передачи данных используются только 2 пары — 4 проводника. Оставшиеся проводники могут использоваться для других целей, например организации электропитания сетевых устройств (технология PoE — Power over Ethernet). В сетях Gigabit Ethernet и более новых используются 4 пары, т.е. все 8 проводников.

Существуют разные виды исполнения витой пары. Прежде всего такой кабель различается по *категориям*. Чем выше категория кабеля, тем большими возможностями будет обладать сеть (более высокие скорость и расстояние передачи). Так, старые поколения сетей Ethernet могли создаваться на основе витой пары 3-й категории. В современных сетях используется кабель категорий 5 или 5e. Существуют также стандарты витой пары категорий 6, 7 и 8 (в том числе с уточнениями версий этих категорий), такой кабель применим в сетях 10G Ethernet и выше. Улучшение качества связи с ростом категории кабеля достигается за счет применения материалов с улучшенными физическими характеристиками, а также за счет экранирования кабеля и его отдельных проводников.

Заметим, что неэкранированная витая пара называется UTP (Unshielded twisted pair), а экранированная — F/UTP, STP, S/FTP, SF/UTP (в зависимости от способа экранирования всего кабеля и отдельных пар его проводников).

Помимо категории, витая пара различается по типу исполнения — кабель для внутренней (внутри помещений) или внешней прокладки (уличной прокладки, прокладки вне помещений). В последнем случае кабель будет иметь дополнительную защиту от высокой и низкой температуры, атмосферных воздействий (влажность, химическое воздействие почвы, солнечный свет) и механических повреждений. Как правило, это достигается применением более прочной и устойчивой внешней оболочки, экранированием кабеля, а также добавлением в структуру кабеля специальных жил, затрудняющих повреждение при сильных изгибах и растяжении.

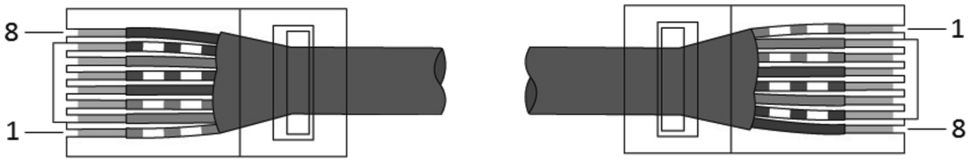


Рис. 6.1.4. Коннекторы 8P8C разъема RJ45

Кабель «витая пара» предполагает использование специальных разъемов – RJ45 (рис. 6.1.4). Разъем — это стандартизированный физический интерфейс, который включает в себя описание вилки (коннектора), розетки (гнезда), а также схемы их коммутации. Коннектор разъема RJ45 называется 8P8C, однако на практике названием RJ45 обозначают и сами коннекторы, что не совсем корректно, однако используется повсеместно.

Монтаж разъемов (обжим кабеля) должен проводиться по правилам, определяемым стандартами TIA/EIA-568A и TIA/EIA-568B. Так, *прямой кабель*, применяемый для соединения компьютера и коммутатора, должен с двух концов обжиматься по одинаковым стандартам (чаще используется стандарт TIA/EIA-568B). Для соединения двух компьютеров требуется *перекрестный кабель* (crossover cable, кроссовер). В сетях Fast Ethernet для этого один конец кабеля должен обжиматься по стандарту TIA/EIA-568A, а другой — TIA/EIA-568B.

В таблицах 6.1.2 и 6.1.3 представлены схемы обжима кабеля по двум используемым стандартам.

Таблица 6.1.2

TIA/EIA-568A	
1	зелено-белый
2	зеленый
3	оранжево-белый
4	синий
5	сине-белый
6	оранжевый
7	коричнево-белый
8	коричневый

Таблица 6.1.3

TIA/EIA-568B	
1	оранжево-белый
2	оранжевый
3	зелено-белый
4	синий
5	сине-белый
6	зеленый
7	коричнево-белый
8	коричневый

Для сетей Gigabit Ethernet описанный выше перекрестный кабель не подойдет, так как в таких сетях используются все 8 проводников и раскладка перекрестного кабеля должна быть иной. Впрочем, сетевые устройства Gigabit Ethernet обычно способны автоматически распознавать тип кабеля и переключаться на нужную схему внутренней разводки. В этом случае для любого подключения подойдет прямой кабель.

Перекрестная схема подключения требуется и для соединения двух коммутаторов. Для этого, однако, перекрестный кабель не используется. Правильная схема подключения достигается использованием особого порта коммутатора для подключения к внешнему коммутатору либо использованием коммутаторов с автоматическим определением типа подключения.

Таким образом, в прямом кабеле, где оба конца обжаты по одинаковой схеме, выполняется правило прямого соответствия контактов первого и второго разъема (первый контакт — с первым, второй — со вторым и т.д.). Особые требования к порядку следования проводников (порядку цветов) определяются тем, что контакты сигналов приема и передачи идут непоследовательно, поэтому необходимо использовать особый порядок цветов, чтобы прямой и инверсный сигналы передавались по одной паре свитых проводников, взаимно компенсируя электромагнитные помехи (рис. 6.1.5).

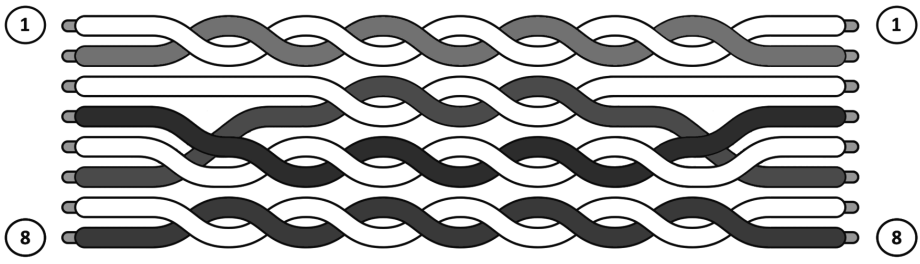


Рис. 6.1.5. Схема распределения проводников
при прямом обжиме витой пары

Монтаж коннекторов на витую пару производится при помощи специального обжимного инструмента — *кримпера*. Кримпер представляет собой обжимные клещи и позволяет выполнить все операции монтажа — обрезку кабеля, снятие оплетки, подрезку проводников, а также, собственно, сам обжим. Все монтажные операции производятся без пайки, склеивания и

других действий, требующих дополнительного инструмента, комплектующих и материалов.

Монтаж витой пары может также производиться с использованием розеток и коммутационных панелей (патч-панелей, кросс-панелей). Указанные элементы позволяют создать *структурированную кабельную систему* как элемент инфраструктуры здания (помещения). Эта инфраструктура может создаваться не только для локальных сетей, но также для телефонии, видеонаблюдения и др.

Кабель при создании стационарной сетевой инфраструктуры прокладывается в виде скрытой проводки в стенах, монтируется в кабельных каналах, протягивается за подвесным потолком и др. Активное оборудование (компьютеры, коммутаторы) подключаются к розеткам и коммутационным панелям при помощи соединительных шнуров — *патч-кордов* (patching cord), которые в данном случае обычно приобретаются готовыми (заводской, «литой» патч-корд).

Оптоволоконный кабель, как сказано ранее, является альтернативой витой паре и применяется там, где требуется получить высокую скорость передачи информации и (или) соединить узлы компьютерной сети, находящиеся на значительных расстояниях. Такой кабель состоит из нескольких гибких световодов, защищенных пластиковой оболочкой. В зависимости от исполнения кабеля, в его структуре могут быть дополнительные жилы и оплетки, защищающие кабель от повреждений. При соединении узлов компьютерной сети используются, как правило, два оптических проводника, обеспечивающие дуплексный режим передачи.

Высокие показатели оптоволоконных линий связи обеспечиваются физическими характеристиками распространения света в оптическом волокне (высокая несущая частота, малое затухание сигнала), а также неподверженностью оптоволоконного кабеля электромагнитным помехам. С другой стороны, оптоволоконный кабель обладает и недостатками, которые сдерживают его применение в локальных сетях:

- более высокой стоимостью кабеля и сетевых устройств по сравнению с аналогичными решениями на витой паре;
- сложностью монтажа оптоволоконных линий связи, требующего высокой квалификации и дорогостоящего оборудования.

Не останавливаясь подробно на описании многообразия разных видов оптоволоконного кабеля, скажем, что такой кабель принципиально

разделяется на два вида — *одномодовый* и *многомодовый* оптоволоконный кабель.

Одномодовое оптическое волокно очень тонкое, диаметр его сердцевины составляет от 7 до 10 микрон. Благодаря малому диаметру оптическое излучение распространяется в одной моде (в виде одного светового пучка), а значит, слабо подвержено искажению. При использовании такого волокна передача данных возможна на расстояние до 100 километров, причем со скоростями, измеряемыми гигабитами в секунду.

Многомодовое оптическое волокно, применяемое для построения линий связи, имеет диаметр 50 или 62,5 микрон. Оно дешевле и проще в монтаже, однако проигрывает одномодовому оптоволокну в показателях скорости и расстояния. Тем не менее эти показатели значительно лучше, чем у витой пары. Например, в сетях Fast Ethernet (100 Мбит/с) с использованием многомодового оптоволокна передача данных возможна на расстояние до 10 километров. В сетях Gigabit Ethernet (1 Гбит/с) стандарт определяет длину непрерывного сегмента многомодового оптоволокна в 550 метров.

Другое различие существующих видов оптоволоконного кабеля связано с типом его исполнения. Так, с учетом многообразия решаемых задач, на рынке предлагаются кабели для прокладки внутри помещений, для внутренней и внешней прокладки, уличный подвесной кабель, кабель для систем кабельной канализации и др. Для соединения оптического оборудования в пределах одного помещения или серверной стойки существует также кабель для патч-кордов (соединительных шнуров). Патч-корды могут предлагаться и в виде готовых изделий, где необходимые коннекторы оптических разъемов установлены заводским способом.

В отличие от витой пары, где существует единый общепризнанный стандарт, для оптоволоконного кабеля существует множество стандартов оптических разъемов — ST, FC, SC, LC и др. Такая ситуация обусловлена противоречивыми требованиями к характеристикам соединений (надежность, компактность исполнения, невысокая стоимость и др.), а также стремлением производителей оборудования к совершенствованию своей продукции для оптоволоконных сетей.

Монтаж оптических коннекторов возможен как клеевым, так и бесклеевым способом (коннекторы быстрого монтажа). Операция монтажа предполагает вклеивание (закладку) оптического кабеля в гнездо коннектора и последующую шлифовку (существуют разные виды шлифовки, которые не всегда совместимы между собой).

Монтаж оптоволоконной кабельной системы, как правило, предполагает применение сварки, когда отдельные сегменты оптоволоконного кабеля надежно соединяются путем сплавления оптического волокна. Для сварки используется специальное и весьма недешевое оборудование — *сварочный аппарат*, *скалыватель*, инструменты для *снятия оплетки* и *очистки лака*. Помимо этого, чтобы защитить хрупкое соединение, необходимо использовать *муфты* или *кросс-панели*, в которых оба сегмента оптического кабеля будут надежно зафиксированы, а место соединения закрыто от воздействий со стороны.

Сварка, в частности, применяется для монтажа *пигтейлов* (Pig tail, «поросячий хвостик») — отрезков кабеля, оконеченных с одной стороны коннектором необходимого типа. Такой способ монтажа широко применяется в местах соединения внешних линий оптоволоконной связи с имеющимся активным оборудованием локальной сети.

Подключение оптоволоконного кабеля возможно к самым разнообразным сетевым устройствам (компьютерам, маршрутизаторам, коммутаторам и др.) при наличии у последних соответствующих портов. При этом, учитывая многообразие типов оптических разъемов, весьма часто применяется способ подключения через модули SFP.

SFP-модуль — это компактный сменный приемопередатчик (трансивер), выполняющий роль переходника между коннектором оптоволоконного кабеля и соответствующим SFP-портом активного устройства. Такая технология, широко используемая в коммутаторах, обеспечивает не только гибкость выбора типа разъемов оптоволокна, но и позволяет решать другие задачи построения сетевой инфраструктуры, например организации сверхвысокоскоростных линий связи на основе витой пары (10G Ethernet) или стекирования коммутаторов (соединения нескольких коммутаторов в логически единой устройство с большим количеством портов).

На практике также широко применяется такое устройство, как *медиаконвертер*, позволяющее связать сегменты витой пары и оптического волокна. Например, медиаконвертер позволяет получить оптический сигнал от провайдера Интернета и передать этот сигнал дальше посредством витой пары (рис. 6.1.6). Такой способ обеспечивает подключение оптоволоконной линии связи к имеющемуся оборудованию с наименьшими затратами и без существенных изменений уже существующей локальной сети.

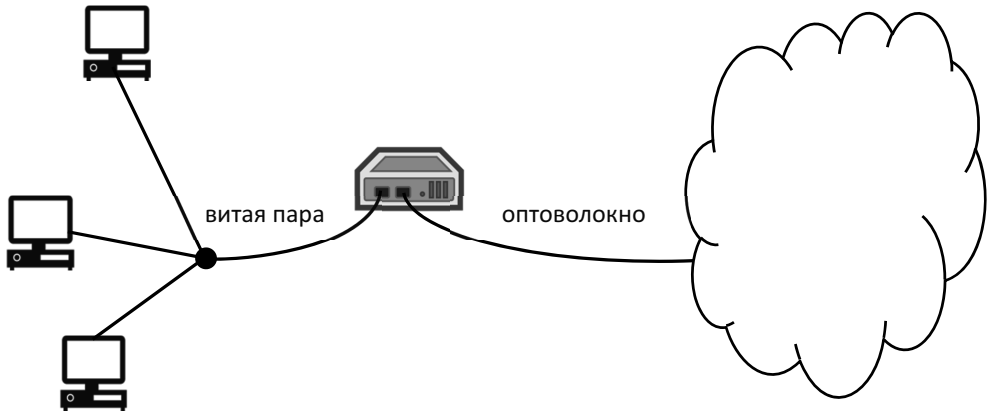


Рис. 6.1.6. Схема подключения медиаконвертера

Стандарты сетей Ethernet

В завершение раздела приведем характеристики наиболее известных разновидностей сетей Ethernet, использовавшихся ранее, а также актуальных и в настоящие дни (табл. 6.1.4). Каждая такая разновидность определяется своим стандартом, а также носит обобщенное название, характеризующее достижимую скорость передачи в компьютерной сети.

Таблица 6.1.4

Стандарт	Год	Тип кабеля	Расстояние
Ethernet, 10 Мбит/с			
10BASE5	1983	Коаксиальный, ~10 мм («толстый»)	500 м
10BASE2	1985	Коаксиальный, ~5 мм («тонкий»)	185 м
10BASE-T	1990	Витая пара (категория 3 или 5)	100 м
Fast Ethernet, 100 Мбит/с			
100BASE-TX	1995	Витая пара (категория 5)	100 м
100BASE-FX	1995	Многомодовое оптоволокно	2 км
100BASE-SX	2001	Многомодовое оптоволокно	300 м
100BASE-LX(BX)10	2004	Одномодовое оптоволокно	10 км

Продолжение табл. 6.1.4

Стандарт	Год	Тип кабеля	Расстояние
Gigabit Ethernet, 1 Гбит/с			
1000BASE-SX	1998	Многомодовое оптоволокно	550 м
1000BASE-LX	1998	Многомодовое оптоволокно	550 м
1000BASE-LX	1998	Одномодовое оптоволокно	5 км
1000BASE-T	1999	Витая пара (категории 5, 5e, 6 или 7)	100 м
1000BASE-LX(BX)10	2004	Одномодовое оптоволокно	10 км
1000BASE-ZX (LH)	2004	Одномодовое оптоволокно	70–120 км
10G Ethernet, 10 Гбит/с			
10GBASE-SR (LR, ER, ZR и др.)	2002	Различные варианты многомодового и одномодового оптоволокна	300 м – 80 км
10GBASE-T	2006	Витая пара (категории 6, 6a или 7)	55–100 м
40GbE и 100GbE, 40 и 100 Гбит/с			
40GBASE-T	2010	Витая пара (категория 8)	30 м
40GBASE-xx, 100GBASE-xx	2010, 2011	Различные варианты многомодового и одномодового оптоволокна	100 м – 40 км

6.2. Беспроводные сети Wi-Fi

Технологии Ethernet, описанные в предыдущем разделе, предлагают кабельные решения для построения локальных сетей. Альтернативой таким сетям в настоящее время являются *беспроводные* локальные сети (Wireless LAN, WLAN), использующие вместо кабеля радиоэфир. В подавляющем большинстве случаев такие сети создаются как сети Wi-Fi — беспроводные локальные сети, основанные на стандартах IEEE 802.11.

Название Wi-Fi (Wireless Fidelity — беспроводная точность) было придумано для привлечения внимания к новой технологии по аналогии с популярным стандартом акустического оборудования Hi-Fi (High Fidelity — высокая точность). В настоящее время от такой трактовки отказались и термин «Wi-Fi» никак не расшифровывается.

Термин Wi-Fi означает технологию и семейство стандартов беспроводных локальных сетей, а также является торговой маркой консорциума Wi-Fi Alliance — группы производителей оборудования для беспроводных сетей, которая ведет разработку стандартов Wi-Fi,

а также занимается тестированием оборудования и выдачей сертификатов на соответствие стандартам.

К достоинствам беспроводных сетей следует отнести:

1) *мобильность пользователей.* Данная характеристика очевидным образом вытекает из самой сути беспроводного подключения — отсутствия кабеля, ограничивающего пользователя в выборе места подключения и изменения этого места в процессе работы. Особую актуальность данное качество приобретает при использовании мобильных пользовательских устройств, не имеющих подключения и к сетям электропитания. Беспроводные сети в данном случае предлагают качественно новый уровень обслуживания клиентов, недостижимый с применением кабельных технологий;
2) *отсутствие необходимости монтажа кабельной системы.* Эта характеристика выгодно отличает беспроводные локальные сети от своих кабельных аналогов в тех случаях, когда монтаж кабельной системы является затруднительным или нецелесообразным в силу тех или иных причин. Например, это могут быть причины, связанные с невозможностью, крайней нежелательностью или высокой стоимостью проведения монтажных кабельных работ (высокая сложность монтажа, нарушение внешнего вида, конфликт интересов с собственником помещения и др.), потребностью лишь временного создания сети (на время проведения конференции, реализации проекта или др.), отсутствием времени и материалов для создания полноценной кабельной системы;
3) *простота подключения пользовательских устройств.* Беспроводные сети упрощают такое подключение, так как не требуют выполнения каких-либо операций физического подключения, а также избавляют пользователей и администраторов сети от необходимости согласования параметров используемых кабелей, разъемов подключения и др.

Наряду с достоинствами беспроводные сети обладают и недостатками, сдерживающими полное вытеснение кабельных технологий:

1) *низкая скорость передачи данных по сравнению с кабельными сетями аналогичных поколений.* Несмотря на постоянное развитие беспроводных сетей, их характеристики тем не менее всегда уступают аналогичным характеристикам развивающимся в те же годы кабельным сетям. Так, по скорости передачи данных

современные беспроводные сети значительно превосходят сети Ethernet первых поколений, но современным сетям Ethernet они тем не менее существенно уступают;

2) *высокая уязвимость сети в плане обеспечения безопасности*. Данный недостаток обусловлен тем, что радиоэфир, используемый для беспроводной передачи данных, является открытой средой, доступной для прослушивания третьей стороной. Данная проблема решается шифрованием трафика, однако это применимо не всегда и в любом случае не исключает принципиальной возможности перехвата пересылаемых данных;
3) *низкая предсказуемость зоны покрытия сети*. На распространение сигнала беспроводной сети влияет множество факторов — затухание и отражение сигнала из-за различных препятствий (стен, предметов мебели и др.), помехи от других электронных приборов и электрической проводки, а также соседних беспроводных сетей. С учетом этих факторов достаточно сложно предсказать зону покрытия беспроводной сети, а значит, гарантировать качество подключения в пределах некоторой территории, оптимально спланировать сеть точек подключения к беспроводной сети для расширения зоны покрытия;
4) *создание помех другим устройствам и сетям передачи данных.* Так как оборудование сетей Wi-Fi осуществляет передачу данных через радиоэфир, то такая передача может оказывать негативное влияние на другие электронные устройства и сети передачи данных. По этой причине, в частности, во многих странах законодательно жестко регулируется перечень частот, используемых сетями Wi-Fi (в разных странах этот перечень может несколько различаться), ограничиваются мощности передатчиков и области применения указанных сетей.

Режимы работы сетей Wi-Fi

Наиболее простой режим работы беспроводной сети — это режим *ad hoc* (*лат*. — по месту), который предполагает установление соединений «точка — точка» непосредственно между оконечным оборудованием без использования специальных сетевых устройств. Например, в режиме ad hoc можно напрямую связать два ноутбука, соединить планшетный компьютер с ноутбуком и др.

В сеть ad hoc можно объединить и более двух устройств. Такое соединение, однако, потребует установку соединения каждого узла сети с каждым другим, т.е. будет выполнено по полносвязной топологии. Учитывая особенности радиоэфира как единой разделяемой среды, соединение большого числа узлов в режиме ad hoc будет сопровождаться значительным снижением производительности. В связи с указанными обстоятельствами, а также с тем, что поддержка сетей ad hoc не является обязательной в современных стандартах Wi-Fi, такие сети большой популярность в настоящее время не пользуются.

Наряду с режимом ad hoc, соединение устройств пользователя без использования дополнительных связывающих устройств возможно также на основе более современной технологии *Wi-Fi Direct*. Эта технология применяется для соединения компьютеров, а также подключения различного периферийного оборудования — принтеров, мультимедийных проекторов, веб-камер и др.

Wi-Fi Direct обеспечивает более высокую производительность и безопасность соединения, чем сети ad hoc, так как фактическое соединение осуществляется по схеме, где роль связывающего устройства выполняет одно из подключаемых устройств.

Другой режим работы сетей Wi-Fi, основанный уже на применении специального оборудования, называется *инфраструктурным.* Беспроводные сети в инфраструктурном режиме создаются на основе одной или нескольких *точек доступа* (Access Point, AP) — базовых станций беспроводной Wi-Fi сети. Точка доступа выполняет роль беспроводного концентратора, обеспечивая объединение беспроводных устройств путем парных соединений «точка доступа — компьютер», что позволяет создать беспроводную сеть с «физической» топологией «звезда» (логическая топология — «шина»).

Инфраструктурный режим нацелен на создание беспроводной сети, обеспечивающей высокую скорость подключения, разнообразные способы авторизации, а также надежное шифрование пересылаемых данных. Такие сети могут создаваться на основе как одной, так и нескольких точек доступа. Эти точки могут подключаться к стационарной кабельной сети, а также соединяться между собой через радиоэфир.

Наиболее простой способ организации беспроводной сети в инфраструктурном режиме представлен на рисунке 6.2.1.

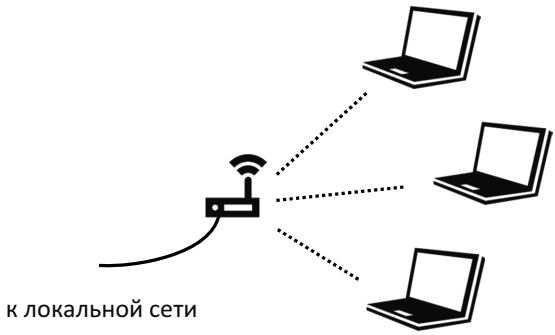


Рис. 6.2.1. Сеть Wi-Fi на основе одной точки доступа

Как было сказано выше, точка доступа позволяет создать беспроводную сеть с «физической» топологией «звезда», но с логической топологией «шина». Последнее обстоятельство связано с особенностям радиоэфира как единой разделяемой среды. Как и в сетях Ethernet, применение множественного доступа к разделяемой среде потребовало осуществить разработку особых методов доступа.

Стандартом Wi-Fi предполагается использование метода CSMA/CA — множественный доступ с обнаружением несущей и предотвращением коллизий. В отличие от метода CSMA/CD, используемого в Ethernet, в данном случае реализован механизм, позволяющий избежать коллизий передаваемых пакетов данных. Достигается это тем, что станция, желающая начать передачу, сначала отправляет в сеть jam-сигнал, информирующий остальные станции о своем намерении, и лишь затем пересылает данные.

В беспроводных сетях, таким образом, коллизиям подвержены не пакеты данных, а jam-сигналы, объем которых в общем трафике существенно меньше. Это повышает общую производительность сети за счет снижения вероятности коллизий и повторных передач, однако вносит дополнительные задержки для каждого конкретного сеанса передачи данных.

Создание беспроводных сетей с большой зоной покрытия требует использования множества точек доступа, распределенных на некоторой территории. Эти точки, подключенные к единой сети, могут функционировать в автономном режиме (*автономные точки доступа*), а также создаваться как *точки доступа под общим управлением*. В последнем случае появляется возможность централизованной настройки точек доступа, автоматического управления точками в процессе работы (настройки

частотных каналов и мощности), балансировки нагрузки, роуминга беспроводных клиентов и др. Для создания сети управляемых точек доступа требуется специальный коммутатор.

Помимо собственно режима Access Point (AP), точки доступа могут работать и в других режимах:

- моста (Bridge);
- беспроводного повторителя (Wireless Repeater);
- распределенной беспроводной системы (Wireless Distribution System, WDS).

Режим *моста* (Bridge) используется в тех случаях, когда точка доступа ко внешней сети подключается не через кабель, а через радиоэфир. Режим моста, таким образом, позволяет радиоканалом соединить удаленные фрагменты стационарных кабельных сетей (рис. 6.2.2).

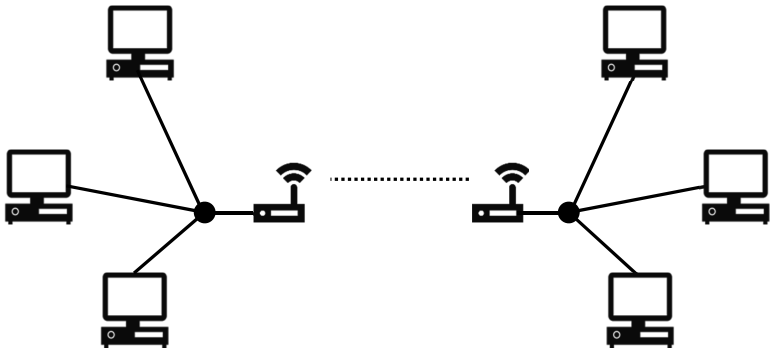


Рис. 6.2.2. Соединение точек доступа в режиме моста

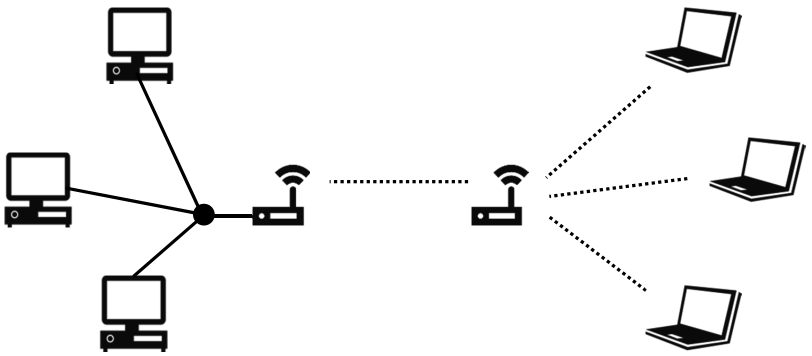


Рис. 6.2.3. Подключение точки доступа в режиме «AP + Bridge»

В случае когда точка доступа использует комбинированный режим «AP + Bridge» («точка доступа + мост»), создается сеть, в которой точка доступа, получая сигнал через радиоэфир, передает его дальше своим беспроводным клиентам. Схема подключения такой точки доступа представлена на рисунке 6.2.3.

Если две точки доступа, соединяемые в режиме моста, находятся на значительном расстоянии друг от друга, для усиления сигнала может использоваться дополнительная точка доступа, работающая в режиме *повторителя* (Wireless Repeater). Такая точка доступа располагается между исходными точками доступа и выполняет роль ретранслятора (рис. 6.2.4). При необходимости может использоваться несколько точек-повторителей для увеличения расстояния.

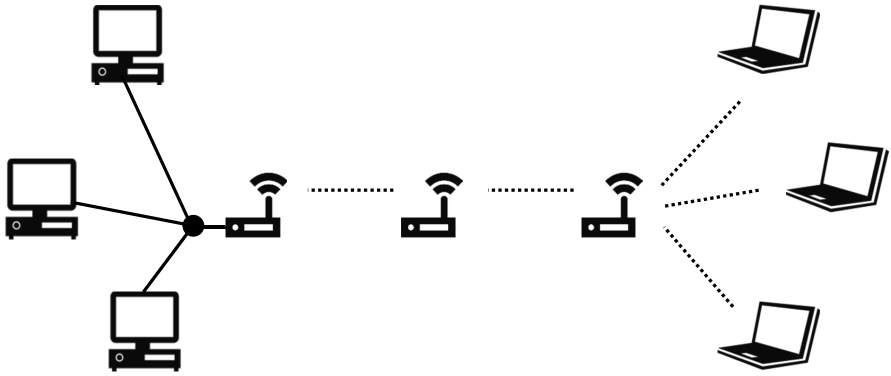


Рис. 6.2.4. Соединение точек доступа через точку-повторитель

Режим *распределенной беспроводной системы* (WDS) предлагает технологию, которая позволяет расширить зону покрытия беспроводной сети путем беспроводного соединения нескольких точек доступа в логически единую сеть. Все точки доступа в режиме WDS используют один частотный канал, одинаковые методы шифрования, а также сохраняют и учитывают информацию о «привязке» клиентов к точкам доступа в пересылаемых кадрах. В результате этого появляется возможность создания не только парных соединений точек доступа (как в режиме моста), но и более сложных конфигураций для реализации в полной мере распределенной беспроводной системы. Режим WDS, таким образом, позволяет соединить несколько территориально разделенных сегментов стационарной кабельной сети, а также обеспечить зону Wi-Fi покрытия на значительной территории с применением исключительно беспроводных технологий.

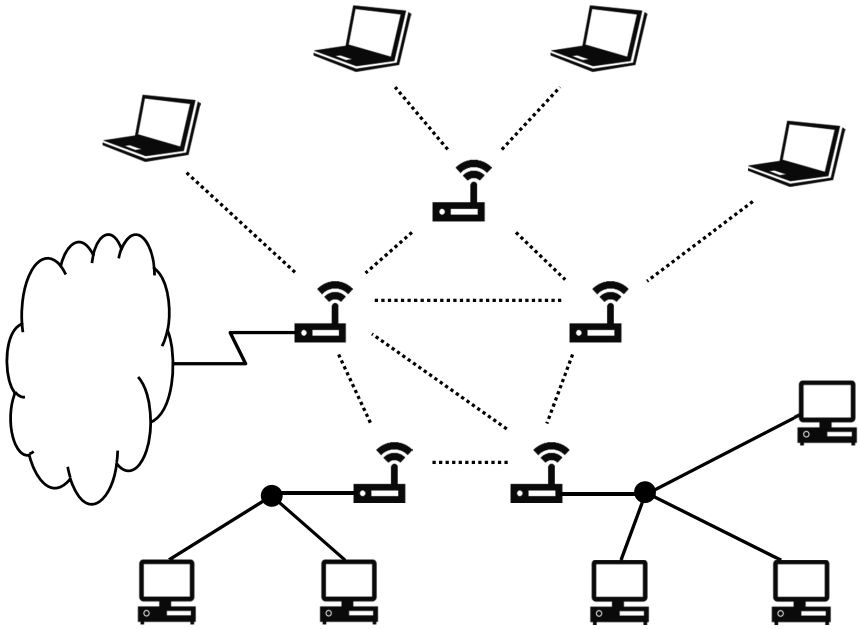


Рис. 6.2.5. Пример построения сети в режиме WDS

Пример схемы построения беспроводной сети в режиме WDS приводится на рисунке 6.2.5. В данной сети обеспечивается возможность подключения беспроводных клиентов на большой территории, соединяются территориально удаленные сегменты кабельной сети, обеспечивается выход всех подключенных устройств к сети Интернет.

Проблемой построения сетей в режиме WDS является отсутствие детального стандарта на разработку соответствующего оборудования. В результате функция WDS на разных устройствах реализуется по-разному и построение сети обычно возможно лишь с применением оборудования одного производителя.

Различие оборудования разных производителей может проявляться и в отношении других режимов работы точек доступа. Несмотря на наличие стандартов, могут отличаться названия режимов и их сочетания, поддерживаемые оборудованием. Однако если точки доступа разных производителей поддерживают требуемый стандартизированный режим, то проблем их совместимости, как правило, не возникает.

Настройка точки доступа в режиме Access Point

Несмотря на множество режимов работы, чаще всего точка доступа будет выступать базовой станцией, обеспечивающей подключение клиентов к беспроводной сети. Как правило, такая точка доступа будет подключена кабелем к внешнему коммутатору, а в качестве клиентов будут выступать компьютеры или мобильные устройства пользователей, оборудованные адаптером беспроводной сети (рис. 6.2.1).

Для настройки такой точки доступа потребуется указать как минимум следующие параметры:

- имя сети (SSID);
- частотный канал;
- параметры безопасности.

К дополнительным параметрам точки доступа, настраиваемым в зависимости от ситуации, можно отнести номер стандарта передачи данных в беспроводной сети (скорости передачи), мощность сигнала, параметры сервера DHCP и др.

Так, *имя сети* (Service Set Identifier, SSID) — это идентификатор, который позволяет клиентам обнаружить беспроводную сеть, получить параметры этой сети для установки соединений. Как правило, идентификаторы доступных беспроводных сетей отображаются на устройствах пользователей в разделе сетевых подключений. Эти же идентификаторы впоследствии используются и для хранения параметров подключений (включая пароли и другие параметры, использовавшиеся когда-либо для успешного подключения).

Идентификатор сети передается в радиоэфир при помощи специальных сигнальных пакетов каждые 100 миллисекунд. При необходимости точка доступа может скрывать свой идентификатор (используется как элемент обеспечения безопасности), а соседние точки доступа могут использовать одинаковые идентификаторы (позволяет создать сеть на большой территории).

Частотный канал — это номер от 1 до 13, который обозначает полосу частот, используемых для пересылки данных. Каждая точка доступа использует какой-либо один канал, на который настраиваются и беспроводные клиенты. Проблема выбора канала становится актуальной тогда, когда в пределах одной зоны обслуживания расположено сразу

несколько точек доступа. Если такие точки используют частотные каналы с одинаковыми номерами, то это существенно снижает скорость передачи, так как разные сети Wi-Fi вынуждены использовать общую разделяемую среду.

Кроме этого, выбирая частотный канал, следует учитывать фактор взаимного влияния соседних каналов друг на друга — наложения используемых диапазонов частот. В этой связи каналы соседних точек доступа должны не просто не совпадать, а достаточно сильно удаляться друг от друга. Полностью непересекающимися каналами являются, например, 1, 6 и 11.

Каналы с номерами от 1 до 13 разрешены к использованию в Европе, России, Китае и большинстве других стран. В странах Северной Америки разрешены только каналы с номерам от 1 до 11. Для нас это означает, что беспроводное устройство, предназначенное для работы, например, в США, не сможет использовать каналы 12 и 13.

С другой стороны, существуют также страны, где разрешается использовать и 14-й канал. К этим странам относится Япония. В этой связи беспроводное оборудование, предназначенное для внутреннего рынка Японии, не может быть сертифицировано для других стран.

Таким образом, настраивая точки доступа, надо выбрать разные каналы, отстоящие друг от друга не менее чем на 5 единиц. Если точек доступа много и «развести» их полностью не удается, то для повторного использования следует указывать каналы с наименьшей загрузкой и более слабым сигналом. При настройке можно, как правило, выбрать и режим автоматического определения канала. В этом случае канал будет определен точкой доступа самостоятельно в момент начала ее работы.

Номера каналов от 1 до 13 справедливы для сетей, работающих на частоте 2,4 ГГц. Однако для построения беспроводных сетей может использоваться и частотный диапазон 5 ГГц, который находит все более широкое применение в новых стандартах Wi-Fi.

Сети Wi-Fi с частотой 5 ГГц имеют свой перечень доступных каналов. В нашей стране в таких сетях разрешено использовать каналы с номерами от 34 до 64.

Параметры безопасности также относятся к обязательным настройкам точки доступа беспроводной сети, так как характер среды передачи позволяет третьим лицам без большого труда перехватывать пересылаемые

данные. К настройкам безопасности беспроводной сети относится указание технологии обеспечения безопасности, назначение ключа доступа и описание некоторых других параметров в зависимости от выбранной технологии.

Защита беспроводных сетей предполагает аутентификацию пользователей, шифрование и проверку целостности пересылаемых данных. В случае когда технологии защиты не применяются, сеть создается открытой, доступ к ней можно получить без пароля. Такие сети считаются небезопасными, так как отсутствие аутентификации, означает отсутствие защиты, а значит, и шифрования пересылаемых данных. Все, что отправляется через открытую беспроводную сеть, может быть получено в незашифрованном виде некоторой третьей стороной путем прослушивания радиоэфира.

В ранних поколениях сетей Wi-Fi использовалась технология защиты WEP (Wired Equivalent Privacy). Данная технология в настоящее время считается устаревшей и не рекомендуется к использованию, так как в связи с выявленными уязвимостями не обеспечивает должного уровня защиты. Технология WEP тем не менее обычно поддерживается современным оборудованием, что позволяет обеспечить совместимость со старыми устройствами, а также дает возможность защищать соединения при подключении слабых устройств.

В качестве замены WEP выступают технологии защиты беспроводных сетей WPA и WPA2 (Wi-Fi Protected Access). Данные технологии поддерживают расширяемый протокол аутентификации EAP (Extensible Authentication Protocol), а также надежное шифрование. При этом в более новой и рекомендуемой к использованию технологии WPA2 реализован стойкий алгоритм шифрования AES, а в WPA — усовершенствованный алгоритм, ранее применявшийся в WEP.

Протокол EAP, обеспечивающий аутентификацию, предполагает предъявление пользователем свидетельства, подтверждающего его право для доступа в сеть. В самом простом варианте это может быть ключ доступа к сети, указанный в настройках точки доступа (для того чтобы получить доступ в сеть, пользователь должен ввести этот ключ на своем устройстве). Данный способ аутентификации получил название Pre Shared Key (WPA-PSK, WPA2-PSK).

В более сложных конфигурациях для аутентификации в беспроводной сети могут использоваться централизованные базы пользователей, предоставляемые сервером RADIUS. Например, роль такого сервера может выполнять контроллер домена Windows. Доступ к беспроводной сети в этом

случае будет предоставляться по учетным записям (логину и паролю) пользователей домена.

Еще один способ аутентификации в беспроводной сети может быть основан на сертификатах, которые надежно подтверждают подлинность пользователя или компьютера. В случае использования сертификатов пароли не используются, для настройки соединения требуется получить и сохранить на компьютере файл-сертификат, который будет предъявляться автоматически в процессе подключения к сети.

К методам обеспечения безопасности беспроводной сети также относят сокрытие SSID и ведение контроля доступа по MAC-адресам. В первом случае защита обеспечивается тем, что беспроводная сеть не обнаруживается на устройствах пользователей в списках подключений. Для подключения к сети надо знать ее SSID, который требуется явно указать в процессе настройки.

Контроль доступа по MAC-адресам позволяет ограничить доступ к беспроводной сети на основе белых или черных списков MAC-адресов беспроводных клиентов. Этот способ не предполагает шифрования данных и не может считаться надежным способом аутентификации из-за того, что MAC-адреса на устройствах пользователей могут быть изменены.

Как первый, так и второй способ защиты не стоит рассматривать как основной. Надежно защитить беспроводную сеть позволяют только технологии WPA и WPA2.

Среди различных дополнительных параметров точки доступа выделим настройку сервера DHCP для динамической настройки сетевых параметров подключаемых устройств.

Настройка такого сервера требуется в случае, когда аналогичный сервер отсутствует в локальной сети. При настройке требуется указать диапазон доступных адресов, а также другие параметры, назначаемые клиентам. Если в сети создается несколько серверов DHCP, то требуется следить, чтобы диапазоны адресов не пересекались.

Настройка точки доступа осуществляется, как правило, через веб-интерфейс. Обычно требуется подключить настраиваемую точку напрямую к компьютеру, обратиться к ней через браузер по адресу IP, пройти авторизацию и выполнить необходимые настройки. Для дальнейшего управления точкой доступа требуется, как правило,

присвоить ей новый адрес IP (в соответствии с правилами локальной сети), а также задать новый пароль.

В случае если адрес и пароль для точки доступа утеряны, то существует возможность сброса к заводским настройкам. Для этого на включенной точке доступа надо нажать кнопку Reset и удерживать ее в таком состоянии несколько секунд. Заводские параметры (адрес и пароль) часто указываются на корпусе точки доступа. В любом случае их можно узнать из сопроводительной документации.

Оборудование сетей Wi-Fi

Итак, для создания беспроводной сети на основе стандарта Wi-Fi требуется одна или несколько точек доступа, а также клиентские устройства, оснащенные адаптерами Wi-Fi.

Поддержку Wi-Fi в настоящее время имеют многие цифровые пользовательские устройства – ноутбуки, неттопы, смартфоны, планшеты, телевизоры, домашние кинотеатры, игровые консоли и др. Адаптер Wi-Fi весьма часто является неотъемлемой частью данных устройств, поэтому технических сложностей выбора и установки клиентского оборудования беспроводной сети, как правило, не возникает.

Если адаптер Wi-Fi отсутствует на устройстве, то проблема решается установкой внешнего адаптера, выполненного в виде платы расширения (для стационарных компьютеров), либо устройства USB (для ноутбуков, телевизоров, домашних кинотеатров и др.).

Выбор точки доступа является более сложной задачей, от правильного решения которой будут зависеть возможности созданной вами сети. При выборе точки доступа приходится учитывать множество различных параметров, существенное значение из которых могут иметь следующие.

1. *Стандарт Wi-Fi*, *поддерживаемый точкой доступа.* Обычно, выбирая точку доступа, в первую очередь обращают внимание на желаемую скорость передачи, которая определяется тем или иным стандартом. Помимо скорости, от стандарта будет зависеть также надежность и безопасность беспроводной сети, размеры зоны покрытия и др. В каждом случае поддержка более нового стандарта обеспечивает какие-то преимущества и перспективы развития сети, ограничением в выборе более нового стандарта может стать лишь стоимость оборудования.

2. Различные *характеристики мощности точки доступа*, описываемые, в частности, мощностью передатчика, количеством и коэффициентом усиления антенн, поддерживаемым режимом многопоточной передачи и др. Высокие показатели мощности актуальны для создания беспроводных сетей в средних и больших офисах, местах общего доступа, производственных помещениях и др. Для домашнего применения и малых офисов высокая мощность, наоборот, может оказаться недостатком, так как возрастает уровень помех для рядом расположенных беспроводных сетей.
3. *Перечень специфических технологий*, *поддерживаемых точкой доступа.* Например, критерием выбора точки доступа может оказаться поддержка технологии множественных сетей (Multiple SSID, гостевые сети), виртуальных локальных сетей (VLAN), питания через кабель Ethernet (Power over Ethernet, PoE), централизованного управления при помощи коммутатора, мониторинга посредством SNMP и др. Как правило, такие технологии востребованы в сетях организаций, где есть потребность применения специальных решений при создании беспроводных сетей.
4. *Тип исполнения корпуса точки доступа.* Данный параметр позволяет понять, насколько хорошо подходит точка доступа для физического размещения в вашей сети. Учитывая многообразие возможных способов размещения, изготовители предлагают и различные конструктивные решения, позволяющие выбрать наиболее подходящий вариант. Так, вы можете выбрать точку доступа для настольного размещения, крепления на стене, монтажа в подвесном потолке, размещения на улице и др. В зависимости от условий планируемого размещения точки доступа могут иметь дополнительную защиту от механических воздействий, пыли, влаги, больших перепадов температур и даже ударов молний.
5. *Наличие дополнительных сетевых устройств*, *конструктивно расположенных в одном корпусе с точкой доступа.* К таким устройствам относятся маршрутизатор, коммутатор, DSL-модем, принт-сервер и др. В совокупности с точкой доступа указанные устройства позволяют решать более общие задачи, чем просто создание ячейки беспроводной сети. Совмещенные устройства хорошо подходят для малых сетей, где они позволяют уменьшить количество физических единиц оборудования, упростить настройку сети и снизить ее стоимость.

Обычно отдельные характеристики точек доступа «группируются» производителями по моделям, предназначенным для тех или иных областей применения. Например, это могут быть точки доступа для дома и малого офиса, которые чаще всего создаются в виде совмещенного устройства (беспроводного маршрутизатора), имеют небольшую мощность, малый перечень специфичных технологий, а также оформлены для размещения на столе. Мощные точки доступа для корпоративного сектора исполняются в виде самостоятельного устройства с большим перечнем специфических технологий (Multi-SSID, VLAN, PoE и др.). Такие устройства размещаются в прочном корпусе для крепления на стене или на потолке.

Помимо адаптеров и точек доступа, к беспроводному оборудованию относят также антенны, которые непременно используются при создании беспроводной сети. Такие антенны могут быть внутренними и внешними. В комплектах реализуемого беспроводного оборудования всегда имеется необходимый набор антенн.

Вместе с тем существуют и специальные антенны, которые могут применяться вместо штатных на точках доступа, а также на адаптерах беспроводной сети. Замена штатной антенны может потребоваться для расширения зоны покрытия (увеличения дальности связи), а также более удобного размещения антенны вне зависимости от места размещения самого устройства.

Увеличение дальности связи достигается за счет применения антенн с более высоким коэффициентом усиления, а также использования направленных антенн, которые способны концентрировать сигнал, передавая его лишь в одном направлении. Более удобное размещение антенны также способствует улучшению качества работы, так как позволяет выбрать место с лучшим уровнем сигнала, «обойти» какое-либо препятствие, создать зону покрытия вне помещения, где расположена точка доступа и др.

В зависимости от используемых антенн дальность связи в сетях Wi-Fi может сильно различаться. Так, в сетях 802.11g при использовании оборудования со стандартными антеннами дальность связи на расчетной скорости 54 Мбит/с составляет, как правило, 20 метров в помещениях и 80 метров вне помещений. Мощная ненаправленная антенна может обеспечить соответствующую дальность на этой же скорости, например, в 100 и 250 метров. Направленная антенна в сетях с расчетной скоростью 54 Мбит/с позволит «приблизиться» к 1 километру, а на скорости 1 Мбит/с — к 10 километрам.

Стандарты Wi-Fi

В завершение раздела беспроводных локальных сетей приведем характеристики наиболее популярных стандартов Wi-Fi, использовавшихся ранее, а также актуальных в настоящие дни (табл. 6.2.1).

Таблица 6.2.1

Стандарт	Год	Частотный диапазон	Скорость
IEEE 802.11	1997	2,4 ГГц	2 Мбит/с
IEEE 802.11b	1999	2,4 ГГц	11 Мбит/с
IEEE 802.11g	2003	2,4 ГГц	54 Мбит/с
IEEE 802.11n	2009	2,4 ГГц, 5 ГГц	600 Мбит/с
IEEE 802.11ac	2014	5 ГГц	6,77 Гбит/с

Следует отметить, что заявленная скорость передачи является лишь теоретически достижимой и относится к уровню физической передачи. Реальная скорость может быть существенно ниже из-за большого объема служебной информации, пересылаемой в сетях Wi-Fi, деления среды передачи между несколькими пользователями, наличия помех от других устройств и др.

Кроме этого, теоретически достижимая скорость рассчитывается с учетом возможностей *многопоточной* передачи (технология MIMO — Multiple Input, Multiple Output). Так, в сетях IEEE 802.11n скорость 600 Мбит/с достигается за счет применения сразу четырех антенн, каждая из которых обеспечивает поток в 150 Мбит/с. Если клиентское устройство технологию MIMO не поддерживает, то даже теоретически достижимой скоростью передачи будет 150 Мбит/с. Аналогичная ситуация наблюдается и применительно к стандарту 802.11ac, где допускается совместное использование до 8 антенн.

Таким образом, в зависимости от фактического количества антенн и режима их работы максимально достижимая скорость конкретных беспроводных устройств, поддерживающих стандарты 802.11n и 802.11ac, может быть существенно ниже, чем заявлено в таблице 6.2.1.

6.3. Виртуальные локальные сети

Ethernet и Wi-Fi предлагают технологии канального уровня, в связи с чем пересылаемые кадры данных могут перемещаться между всеми узлами сети. На практике, однако, весьма часто возникают ситуации, когда распространение трафика требуется как-то ограничить, что может делаться с целью повышения безопасности, а также уменьшения загрузки сети.

Например, при подключении к Интернету жильцов многоквартирного дома через сеть Ethernet каждому абоненту необходимо предоставить доступ именно к Интернету, но не к компьютерам других абонентов этой сети. Другой пример — создание открытых зон беспроводного доступа к Интернету в какой-либо организации. В этом случае беспроводные клиенты, получив доступ к Интернету, должны быть ограничены в доступе к ресурсам самой локальной сети (служебным ресурсам организации). Еще один пример, иллюстрирующий проблемы загрузки сети служебным широковещательным трафиком, — это сети крупных организаций, в которых из-за большого числа компьютеров весьма часто будут возникать рассылки в соответствии с требованиями протоколов ARP, DHCP и др. Разделение таких сетей на зоны распространения широковещательного трафика (*широковещательные домены*) позволяет ограничить области «действия» специальных сервисов, снизить общую загрузку сети.

Ограничение трафика на канальном уровне делается при помощи технологии *виртуальных локальных сетей* (VLAN, Virtual Local Area Network). Виртуальная локальная сеть — это группа узлов локальной сети, трафик которой на канальном уровне полностью изолирован от других узлов сети. Компьютеры одной виртуальной локальной сети взаимодействуют между собой так, как они взаимодействовали бы, будучи подключенными к своей собственной физической сети. Отличие виртуальных сетей здесь будет проявляться лишь в том, что таких сетей можно сделать сразу много, опираясь на одну физическую инфраструктуру локальной сети.

Виртуальные локальные сети, таким образом, позволяют получить некоторые преимущества, недостижимые лишь с использованием физически создаваемых локальных сетей:

1) *гибкость планирования структуры сети.* Виртуальные локальные сети позволяют создавать новые группы узлов без прокладки кабеля и установки нового оборудования. Имеется возможность менять группировку сетевых узлов путем простой настройки коммутатора, без физического переподключения и перемещения устройств. Виртуальные сети позволяют логически реализовать требуемую

топологию локальной сети, основанную на имеющейся физической топологии;

2) *высокая безопасность сети.* Технологии виртуальных локальных сетей позволяют ограничить перемещение трафика уже на канальном уровне, полностью исключив возможность доступа к определенным узлам или перехвата пересылаемых кадров;
3) *ограничение широковещательных сообщений.* Виртуальные локальные сети позволяют контролировать перемещение широковещательного трафика, ограничивать зоны его распространения для уменьшения загрузки сети.

Существуют разные способы организации виртуальных локальных сетей. Как правило, виртуальные локальные сети создаются на основе *управляемых коммутаторов*, где возможно применение одной из двух распространенных технологий: 1) виртуальная сеть на базе порта (Port-based VLAN); 2) виртуальная сеть на базе тега (Tag-based VLAN).

Виртуальная сеть на базе порта — это технология, которая позволяет в настройках коммутатора явно указать — между каким портами коммутатора возможно следование трафика. Такой способ настройки дает возможность изолировать друг от друга несколько групп компьютеров, подключенных к одному коммутатору. Так, на рисунке 6.3.1 представлена конфигурация, где в настройках коммутатора разрешено следование трафика лишь между портами 1, 5, 6 и 1, 7, 8. Результатом такой настройки является создание двух виртуальных локальных сетей — A и B. Компьютеры каждой из сетей могут обмениваться информацией между собой, а также получать доступ к узлам Интернета. При этом сами сети полностью изолированы друг от друга – обмен информацией между этими сетями полностью исключен.

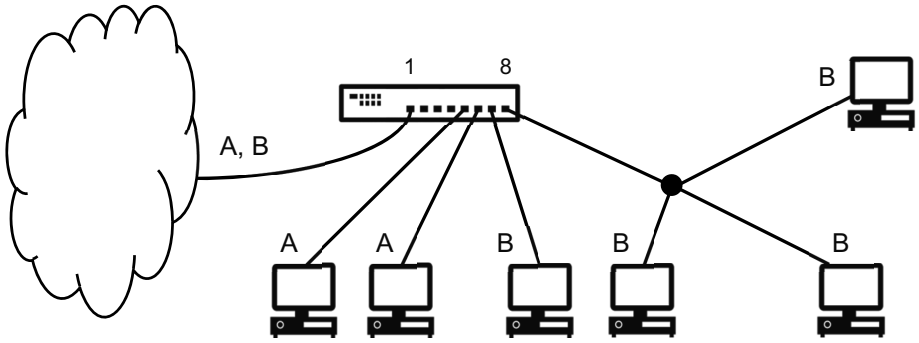


Рис. 6.3.1. Создание двух виртуальных
локальных сетей на основе Port-based VLAN

Технология Port-based VLAN, несмотря на простоту, имеет и существенные недостатки. Например, она не позволяет создавать виртуальные сети на основе нескольких коммутаторов — когда узлы, подлежащие группировке, территориально разделены, в связи с чем подключены к разным коммутаторам локальной сети. Данного недостатка лишена вторая технология виртуальных сетей — Tag-based VLAN.

Tag-based VLAN (*виртуальная сеть на базе тега*) — это технология, описанная в стандарте IEEE 802.1Q. Данная технология предполагает учет принадлежности кадра к той или иной виртуальной локальной сети, что делается через добавление к кадру дополнительной информации — специального маркера (тега), в котором указан идентификатор виртуальной локальной сети (VID, VLAN ID — число в диапазоне от 0 до 4095). Добавление нового тега, таким образом, меняет структуру заголовка кадра (именно для этого потребовалась стандартизация). Сами кадры называются *маркированными* или *тегированными* (tagged).

Тег занимает 4 байта, в связи с чем на данную величину увеличивается и общий размер пересылаемых кадров. Если технология Tag-based VLAN применяется в сетях, где также используется и старое оборудование, то это может оказаться проблемой, так как увеличенные кадры не всегда будут обрабатываться корректно. Решение проблемы может заключаться в уменьшении MTU (Maximum Transmission Unit, максимальный размер блока данных) на всех устройствах локальной сети. В сетях Ethernet этот размер составляет 1500 байт. Для надежной поддержки Tag-based VLAN, таким образом, требуется установить MTU в 1496 байт.

Общее правило виртуальных сетей на базе тегов заключается в том, что трафик в локальной сети должен пересылаться лишь между теми портами коммутаторов, которые приписаны к соответствующим виртуальным сетям. Для достижения этого коммутаторы, поддерживающие технологию Tag-based VLAN, проводят анализ заголовков кадров и выполняют следующие действия:

1) если кадр не маркирован (не имеет тега), но следует через порт, приписанный к некоторой виртуальной сети, то такой кадр сначала маркируется номером этой сети, а лишь потом пересылается на другой порт коммутатора или далее в сеть;
2) если кадр маркирован и следует через порт, приписанный к некоторой виртуальной сети, то кадр пересылается без изменений (если маркер кадра соответствует номеру некоторой виртуальной

сети, которая связана с рассматриваемым портом) либо отбрасывается (если маркер кадра не соответствует перечню виртуальных сетей, к которым приписан порт коммутатора);

3) если кадр маркирован, но следует во внешнюю сеть через порт, не приписанный к виртуальным сетям, то маркер у такого кадра удаляется;
4) немаркированные кадры через порты, не приписанные виртуальным сетям, следуют без каких-либо изменений.

Пример организации двух виртуальных сетей на основе Tag-based VLAN представлен на рисунке 6.3.2. Буквами A и B на данном рисунке обозначены виртуальные сети, которые маркируются тегами с VID 2 и 3. Соединение коммутаторов осуществляется через *транковые* порты (trunk, магистраль) — это те порты, которые приписаны сразу к нескольким виртуальным сетям.

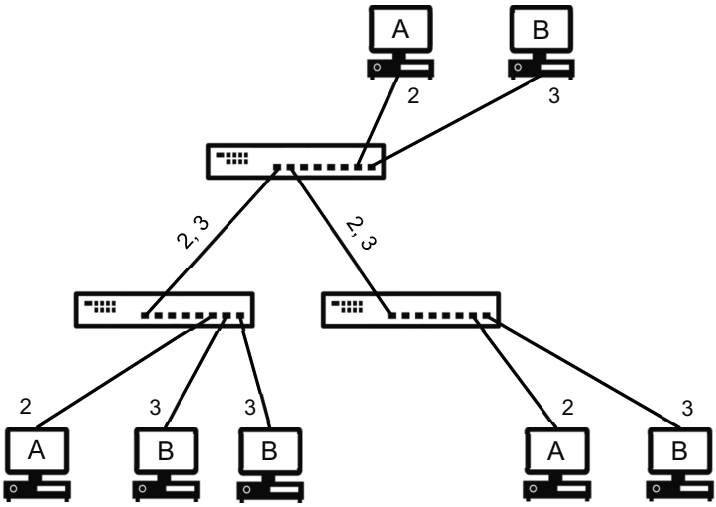


Рис. 6.3.2. Создание двух виртуальных
локальных сетей на основе Tag-based VLAN

Обмен информацией в локальной сети, представленной на рисунке 6.3.2, возможен только в пределах виртуальных сетей A или B. Для создания такой конфигурации в настройках всех коммутаторов указана «привязка» соответствующих портов к виртуальным сетям с VID 2 и 3.

Локальная сеть может создаваться с использованием как управляемых, так и неуправляемых коммутаторов. Как правило, неуправляемые коммутаторы корректно обрабатывают кадры с метками виртуальных сетей, не удаляя эти метки в процессе пересылки. Это означает, что при построении виртуальных сетей отдельные управляемые коммутаторы могут соединяться через неуправляемые, а к маркированным портам управляемых коммутаторов могут подключаться неуправляемые коммутаторы для дальнейшего расширения сети.

Виртуальные локальные сети могут создаваться не только на основе управляемых коммутаторов. Обработка маркированного трафика возможна также и на другом оборудовании — точках доступа, маршрутизаторах, сетевых адаптерах с поддержкой VLAN.

Так, создание беспроводных сетей на *точках доступа*, поддерживающих VLAN, позволяет разграничивать уровни доступа к ресурсам локальной сети для стационарных и беспроводных устройств. Например, в локальной сети организации возможно создание беспроводной сети, которая будет обеспечивать доступ только к Интернету, но не к внутренним ресурсам локальной сети (актуально для создания общедоступных беспроводных сетей).

Сетевые адаптеры с поддержкой VLAN дают возможность более гибкой настройки сервера локальной сети — они позволяют по-разному обрабатывать обращение к себе с компьютеров разных виртуальных сетей. *Маршрутизаторы* с поддержкой VLAN могут применять правила маркировки кадров на основе критериев, относящихся к уровню протокола IP. Последнее обстоятельство позволяет, например, через один маршрутизатор обеспечить доступ к Интернету сразу для множества виртуальных сетей.

Пример построения локальной сети, где используется все перечисленное оборудование, приводится на рисунке 6.3.3. В данном случае создается сеть, где компьютеры отдельных виртуальных сетей A и B могут обмениваться информацией между собой, получать доступ к локальному серверу, а также к сети Интернет. Компьютеры виртуальной сети C (сеть беспроводных клиентов) получают доступ только к сети Интернет, локальные ресурсы беспроводным клиентам недоступны.

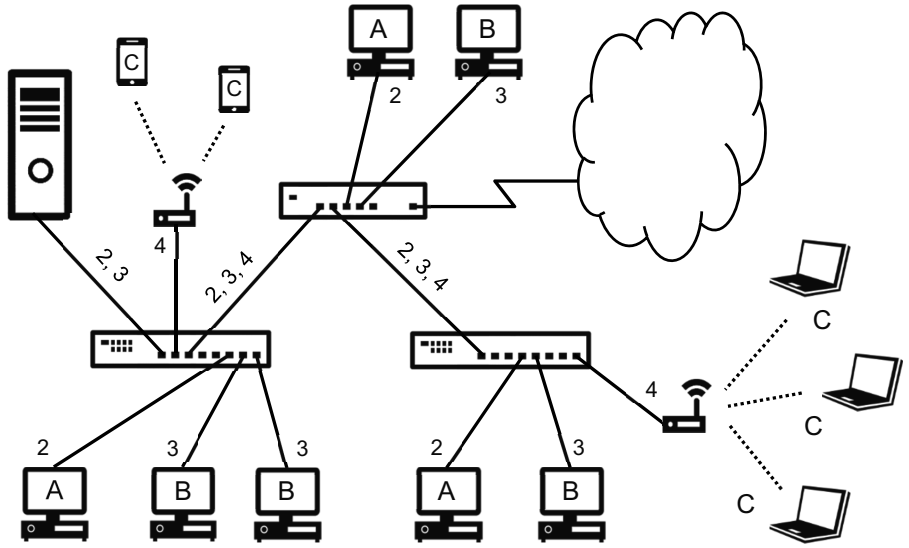


Рис. 6.3.3. Пример совместной настройки сетевых устройств разного типа для организации работы виртуальных сетей

На практике виртуальные локальные сети чаще всего создаются на базе имеющихся физических локальных сетей. Это, в свою очередь, означает, что лишь некоторые порты коммутатора будут отнесены к той или иной виртуальной сети, а через сам коммутатор будут следовать как маркированные, так и немаркированные кадры.

Обычно считается, что все немаркированные кадры относятся к некоторой одной виртуальной сети — Native VLAN (чаще всего она получает номер 1). Если немаркированный пакет приходит на порт коммутатора, не имеющий привязки к VLAN (untagged port), то кадр маркируется тегом с номером Native VLAN и далее обрабатывается как маркированный. Если маркированный кадр следует во внешнюю сеть через порт, отмеченный как untagged, то маркер из него удаляется. Кадр уходит в сеть как обычный, не относящийся к VLAN.

Таким образом, между портами коммутатора, не относящимися к виртуальным сетям, возможность пересылки немаркированных кадров сохраняется. Возможно ли принимать немаркированные кадры на порты, относящиеся к виртуальным сетям? Особенности поведения сетевых устройств в данном случае будут зависеть от их технической реализации либо от выполненных настроек, если они предусмотрены.

Вопросы и задания

Технологии и стандарты сетей Ethernet

Как называется технология, применяемая в настоящее время для построения локальных кабельных сетей? В чем особенность этой технологии?

Что такое коллизия в локальной сети, в каком случае она возникает? Какие решения приняты в Ethernet для разрешения коллизий?

В чем особенности и преимущества коммутируемых сетей Ethernet? Опишите основные принципы работы коммутатора.

Какой кабель применяется для построения сетей Ethernet? Назовите возможные типы используемого кабеля.

Опишите особенности внутреннего устройства витой пары. Каким образом используются проводники витой пары для передачи сигналов? Отличаются ли принципы организации связи по витой паре в сетях 100 и 1000 Гбит/с?

Какие разъемы используются для витой пары? Назовите порядок цветов, определяющий схему обжима разъемов витой пары.

В чем особенность и преимущества оптоволоконного кабеля? Чем отличается одномодовое и многомодовое оптоволокно? По каким другим признакам различается оптоволоконный кабель?

Какое оборудование применяется для построения сетей на основе оптического волокна?

Какие стандарты сетей Ethernet существуют? Опишите их основные характеристики.

Беспроводные сети Wi-Fi

Опишите достоинства и недостатки применения беспроводных технологий для построения локальных сетей.

Что такое инфраструктурный режим работы сети Wi-Fi?

Какое оборудование применяется для создания сетей Wi-Fi в инфраструктурном режиме?

Опишите особенности настройки точки доступа в режиме Access Point, Bridge, Access Point + Bridge, Wireless Repeater, WDS. В каких случаях применяется каждый из указанных режимов?

Назовите основные параметры настройки точки доступа в режиме Access Point. Поясните принципы выбора тех или иных значений для названных параметров.

Каким образом осуществляется защита беспроводных сетей? В чем отличие технологий защиты WEP, WPA и WPA2? Какая из этих технологий позволяет создать наиболее защищенную сеть?

Какие характеристики оборудования необходимо учитывать при выборе точки доступа?

Какие стандарты сетей Wi-Fi существуют? Опишите основные характеристики стандартов.

Виртуальные локальные сети

Что такое виртуальные локальные сети? В каких случаях применяются технологии виртуальных локальных сетей?

Опишите способы создания виртуальных локальных сетей на управляемом коммутаторе. Чем отличаются технологии создания VLAN на основе порта и тега?

Что такое маркированный и немаркированный трафик? Как обрабатывают такой трафик управляемые коммутаторы и другое оборудование локальных сетей, способное учитывать маркеры Tag-based VLAN?

Оглавление

Алексей Николаевич СЕРГЕЕВ

ОСНОВЫ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебное пособие

Редакция физико-математической литературы
Ответственный редактор *Н. В. Черезова*
Выпускающие *Т. А. Кошелева, Н. А. Крылова*

ЛР № 065466 от 21.10.97
Гигиенический сертификат 78.01.10.953.П.1028
от 14.04.2016 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lanbook.ru; www.lanbook.com
196105, Санкт-Петербург, пр. Юрия Гагарина, д. 1, лит. А.
Тел./факс: (812) 336-25-09, 412-92-72.
Бесплатный звонок по России: 8-800-700-40-71

ГДЕ КУПИТЬ

ДЛЯ ОРГАНИЗАЦИЙ:

Для того, чтобы заказать необходимые Вам книги, достаточно обратиться в любую из торговых компаний Издательского Дома «ЛАНЬ»:

по России и зарубежью
«ЛАНЬ-ТРЕЙД». 192029, Санкт-Петербург, ул. Крупской, 13
тел.: (812) 412-85-78, 412-14-45, 412-85-82; тел./факс: (812) 412-54-93
e-mail: trade@lanbook.ru; ICQ: 446-869-967
www.lanpbl.spb.ru/price.htm

в Москве и в Московской области
«ЛАНЬ-ПРЕСС». 109263, Москва, 7-я ул. Текстильщиков, д. 6/19
тел.: (499) 178-65-85; e-mail: lanpress@lanbook.ru

в Краснодаре и в Краснодарском крае
«ЛАНЬ-ЮГ». 350901, Краснодар, ул. Жлобы, д. 1/1
тел.: (861) 274-10-35; e-mail: lankrd98@mail.ru

ДЛЯ РОЗНИЧНЫХ ПОКУПАТЕЛЕЙ:

интернет-магазин
Издательство «Лань»: http://www.lanbook.com

магазин электронных книг
Global F5: http://globalf5.com/

Подписано в печать 11.07.16.
Бумага офсетная. Гарнитура Школьная. Формат 70×100 $^{1}/_{16}$.
Печать офсетная. Усл. п. л. 14,95. Тираж 200 экз.

Заказ № 191-16.

Отпечатано в полном соответствии
с качеством предоставленного оригинал-макета
в ПАО «Т8 Издательские Технологии».
109316, г. Москва, Волгоградский пр., д. 42, к. 5.