

Е. В. Котельников

**Сетевое администрирование
на основе
Microsoft Windows Server 2003**

Курс лекций

2007

Содержание

Предисловие	5
Лекция 1. Введение	6
План лекции.....	6
Понятие, цель и задачи сетевого администрирования.....	6
Семейство операционных систем Windows Server 2003	7
Инструменты администрирования.....	8
Резюме.....	9
Контрольные вопросы	10
Лекция 2. Стек протоколов TCP/IP	11
План лекции.....	11
Стек TCP/IP	11
История создания TCP/IP.....	11
Модель OSI.....	12
Структура TCP/IP.....	13
Документы RFC	14
Обзор основных протоколов	15
Утилиты диагностики TCP/IP.....	17
Резюме.....	19
Контрольные вопросы.....	20
Лекция 3. IP-адресация	21
План лекции.....	21
Адресация в TCP/IP-сетях.....	21
Типы адресов стека TCP/IP.....	21
Структура IP-адреса	22
Классы IP-адресов.....	23
Использование масок	25
Протокол IPv6	28
Особые IP-адреса	29
Протокол ARP	29
Резюме.....	31
Контрольные вопросы.....	31
Лекция 4. Маршрутизация	32
План лекции.....	32
Задача маршрутизации	32
Таблица маршрутизации	33
Принципы маршрутизации в TCP/IP	34
Создание таблиц маршрутизации	36
Протокол маршрутизации RIP	37
Протокол маршрутизации OSPF	37
Резюме.....	38
Контрольные вопросы.....	38

Лекция 5. Имена в TCP/IP	39
План лекции	39
Необходимость применения символьных имен	39
Система доменных имен	39
Служба DNS	41
Процесс разрешения имен	42
Записи о ресурсах	44
Утилита NSLOOKUP	44
Имена NetBIOS и служба WINS	45
Резюме	45
Контрольные вопросы	46
Лекция 6. Протокол DHCP	47
План лекции	47
Проблема автоматизации распределения IP-адресов	47
Реализация DHCP в Windows	47
Параметры DHCP	48
Адреса для динамической конфигурации	49
DHCP-сообщения	50
Принцип работы DHCP	50
Авторизация DHCP-сервера	52
Резюме	53
Контрольные вопросы	53
Лекция 7. Служба каталога Active Directory	54
План лекции	54
Понятие Active Directory	54
Структура каталога Active Directory	55
Объекты каталога и их именование	58
Иерархия доменов	59
Доверительные отношения	60
Организационные подразделения	62
Резюме	63
Контрольные вопросы	64
Лекция 8. Планирование и управление Active Directory	65
План лекции	65
Планирование Active Directory	65
Планирование логической структуры	66
Планирование физической структуры	68
Учетные записи	69
Группы пользователей	70
Групповые политики	71
Резюме	73
Контрольные вопросы	74
Лекция 9. Средства обеспечения безопасности	75
План лекции	75
Средства сетевой безопасности Windows Server 2003	75

Протокол аутентификации Kerberos	75
Термины, используемые в протоколе Kerberos	76
Основные этапы аутентификации	78
Этап регистрации клиента	79
Этап получения сеансового билета	81
Этап доступа к серверу	82
Протокол IPsec	83
Функции протокола IPsec	83
Протоколы AH и ESP	84
Протокол IKE	85
Резюме	86
Контрольные вопросы	86
Лекция 10. Удаленный доступ и виртуальные частные сети	87
План лекции	87
Удаленный доступ	87
Виды коммутируемых линий	88
Протоколы удаленного доступа	88
Протоколы аутентификации	90
Основные понятия и виды виртуальных частных сетей	91
Протоколы виртуальных частных сетей	93
Протокол RADIUS	93
Резюме	94
Контрольные вопросы	95
Библиографический список	96
ПРИЛОЖЕНИЯ	97
Приложение I. Документы RFC	97
Приложение II. Домены первого уровня	100
1. Домены организаций	100
2. Географические домены	100
Приложение III. Права пользователей	102
1. Привилегии	102
2. Права на вход в систему	102
3. Разрешения на доступ к объектам	103

Предисловие

Курс «Сетевое администрирование на основе Microsoft Windows Server 2003» предназначен для усвоения базовых теоретических знаний, формирования практических умений и навыков по внедрению, управлению и поддержке компьютерных сетей на базе операционной системы Microsoft Windows Server 2003.

В рамках курса предполагается изучение базовых понятий сетевого администрирования и стека протоколов TCP/IP, рассмотрение эффективных решений задач управления пользователями и ресурсами сети, освоение основных приемов и инструментов мониторинга компьютерной сети, овладение базовыми средствами обеспечения безопасности сети. В процессе изучения курса происходит воспитание творческого подхода к решению проблем, возникающих в процессе профессиональной деятельности специалиста.

Курс состоит из лекционной части и лабораторного практикума. В лекциях рассматриваются основные теоретические положения, необходимые для успешного освоения практических навыков и умений. Также приводятся библиографический список дополнительной литературы по тематике курса и три приложения.

Лабораторный практикум состоит из 10 лабораторных работ. Все работы выполняются на виртуальных машинах Microsoft Virtual PC в среде Microsoft Windows Server 2003. Каждая лабораторная работа предполагает выполнение самостоятельных экспериментов.

Для успешного освоения курса желательны базовые знания по основам компьютерных сетей, хотя все необходимые сведения приводятся в лекциях или при описании лабораторных работ.

Лекция 1. Введение

План лекции

- Понятие, цель и задачи сетевого администрирования.
- Семейство операционных систем Windows Server 2003.
- Инструменты администрирования.
- Резюме.
- Контрольные вопросы.

Понятие, цель и задачи сетевого администрирования

Целью создания любой компьютерной сети является предоставление доступа к её ресурсам. В качестве ресурсов могут рассматриваться данные (файлы и папки), устройства (принтеры, сканеры, модемы) и вычислительные возможности, обеспечиваемые процессорами.

Для того чтобы сеть эффективно, надежно и безопасно функционировала, необходимо квалифицированное управление. Вопросы управления ресурсами сети, а также её инфраструктурой составляют предмет *сетевого администрирования*.

Отметим различие между понятиями *сетевого* и *системного* администрирования. *Системное администрирование* подразумевает управление любой сложной программной системой, например системой управления базами данных, системой документооборота или операционной системой, при этом наличие сети необязательно. *Сетевое администрирование* связано с управлением сетью и сетевыми компонентами операционных систем. Для обозначения специалистов, независимо от сферы их деятельности (т. е. занимаются они управлением системами или сетями), применяется единый термин – *системный администратор*.

Итак, основная цель сетевого администрирования – обеспечение доступа к ресурсам сети. Для достижения этой цели администраторам приходится решать множество задач, которые могут быть разделены на следующие основные группы (см. рис. 1.1):

- задачи планирования – залогом успешной работы сети является продуманная организация всех её компонентов;
- задачи установки и настройки программного и аппаратного обеспечения – при наличии большого числа компьютеров в сети требуется решать такие задачи централизованно и с максимальной степенью автоматизации;
- задачи управления безопасностью – в современных сетях, в большинстве своем подключенных к Интернету, проблема обеспечения безопасности является крайне острой и требует комплексного решения;

- задачи управления производительностью – для решения этого типа задач следует осуществлять мониторинг процессов, происходящих в сети, и оперативно реагировать на выявившиеся проблемы с производительностью.



Рис. 1.1. Цель, задачи и объекты сетевого администрирования

Решение данных задач осуществляется применительно к трем группам объектов:

- серверы – компьютеры, предоставляющие доступ к ресурсам сети и посредством которых системный администратор управляет сетью;
- клиенты – компьютеры или пользователи, осуществляющие доступ к ресурсам сети;
- сетевая инфраструктура – набор аппаратных и программных средств, обеспечивающих функционирование сети (коммутаторы, маршрутизаторы, сетевые протоколы и т. д.).

Семейство операционных систем Windows Server 2003

В данном курсе теоретические положения иллюстрируются на примере операционных систем семейства Microsoft Windows Server 2003. Это семейство операционных систем является развитием Microsoft Windows

Server 2000 и сочетает в себе широкие возможности управления сетью, высокую производительность, эффективные средства обеспечения безопасности и удобство администрирования.

В семейство Windows Server 2003 входят следующие версии операционных систем:

- Windows Server 2003 Standard Edition (стандартная версия) – универсальная операционная система, способная решать задачи предоставления ресурсов и управления сетью в масштабах небольших и средних компаний. Поддерживает до четырех центральных процессоров и до четырех гигабайт оперативной памяти.
- Windows Server 2003 Enterprise Edition (корпоративная версия) – предоставляет расширенные возможности стандартной версии и обеспечивает высокую производительность и надежность за счет поддержки до 8 процессоров и до 32 Гб оперативной памяти. Предназначена для использования в средних и крупных организациях.
- Windows Server 2003 Datacenter Edition (версия для центра обработки данных) – наиболее мощная из всех операционных систем семейства. Поддерживает до 32 процессоров (минимум восемь) и до 64 Гб оперативной памяти. Может быть использована в качестве сетевого сервера или сервера базы данных большой корпорации.
- Windows Server 2003 Web Edition (версия для web-узлов) – облегченная версия операционной системы, предназначенная для поддержки веб-сайтов и веб-служб. В Web Edition не включены многие компоненты из более мощных версий. Поддерживает до двух процессоров и до двух гигабайт оперативной памяти.

Версии Standard Edition, Enterprise Edition и Datacenter Edition поддерживают одинаковый набор основных административных функций, поэтому в дальнейшем изложение будет вестись без указания версии. Принципиальным отличием версии Web Edition является отсутствие службы каталога Active Directory¹.

Инструменты администрирования

Операционная система Windows Server 2003 предоставляет системному администратору широкий набор инструментов для решения задач управления. Основными из этих инструментов являются следующие:

- консоль управления (Microsoft Management Console, MMC);
- мастера (Wizards);
- утилиты командной строки.

Консоль управления MMC² представляет собой унифицированную среду для выполнения административных задач. Администратор, имея в распоряжении такую среду, может помещать в неё одну или несколько

¹ Служба каталога Active Directory будет рассмотрена в лекции 7.

² Термин «консоль» означает «пульт управления».

утилит, называемых *оснастками* (snap-in), для решения текущей проблемы. Консоль управления позволяет одинаково отображать любые оснастки и использовать для управления ими похожие приемы.

Таким образом, смысл применения консоли управления в том, чтобы сделать среду выполнения административных утилит единообразной и удобной.

С той же целью в Windows Server 2003 применяются *мастера*. Мастер представляет собой программу, которая проводит администратора по всем этапам решения какой-либо задачи. На каждом этапе возможен выбор одного или нескольких способов решения или параметров настройки. Часто также мастера предоставляют возможность выбора параметров по умолчанию.

Использование мастеров позволяет сократить время установки и настройки компонентов операционной системы или время решения другой административной задачи. Кроме того, параметры по умолчанию чаще всего обеспечивают вполне работоспособный режим, хотя, возможно, и не самый эффективный.

Утилиты командной строки являются самыми старыми инструментами администрирования, ведущими свою историю от первых операционных систем без графического интерфейса. В то время альтернативы утилитам командной строки не было. Сегодня большинство задач управления можно решить без использования утилит, однако многие администраторы считают, что утилиты командной строки удобнее графического интерфейса. Кроме того, такой вид утилит, как утилиты диагностики стека протоколов TCP/IP, не имеют стандартного графического аналога (эти утилиты рассматриваются во второй лекции).

Большинство административных задач возможно решить, используя любой из представленных инструментов – консоль управления, мастер или утилиту командной строки. Выбор инструмента обуславливается, в основном, личными предпочтениями системного администратора.

Резюме

Основной целью сетевого администрирования является обеспечение эффективного, надежного и безопасного доступа к ресурсам сети. Главное лицо этого процесса – системный администратор, который решает задачи планирования, установки и настройки программного и аппаратного обеспечения, управления безопасностью и производительностью по отношению к клиентам, серверам и сетевой инфраструктуре.

Одна из наиболее современных и мощных платформ для организации сетевой среды – семейство операционных систем Microsoft Windows Server 2003, включающее версии Standard Edition, Enterprise Edition, Datacenter Edition и Web Edition. Эти операционные системы предоставляют набор удобных инструментов для решения административных задач. Основными инструментами являются консоль управления MMC, мастера и утилиты командной строки.

Контрольные вопросы

1. Какова основная цель сетевого администрирования?
2. Чем отличаются понятия сетевого администрирования и системного администрирования?
3. Назовите основные виды задач сетевого администрирования. Приведите примеры конкретных задач на каждый вид.
4. Чем отличаются версии операционных систем Microsoft Windows Server 2003?
5. Что такое оснастка (snap-in)?

Лекция 2. Стек протоколов TCP/IP

План лекции

- Стек TCP/IP.
- История создания стека TCP/IP.
- Модель OSI.
- Структура TCP/IP.
- Документы RFC.
- Обзор основных протоколов.
- Утилиты диагностики TCP/IP.
- Резюме.
- Контрольные вопросы.

Стек TCP/IP

Стек TCP/IP – это набор иерархически упорядоченных сетевых протоколов. Название стек получил по двум важнейшим протоколам – TCP (Transmission Control Protocol) и IP (Internet Protocol). Помимо них в стек входят ещё несколько десятков различных протоколов. В настоящее время протоколы TCP/IP являются основными для Интернета, а также для большинства корпоративных и локальных сетей.

В операционной системе Microsoft Windows Server 2003 стек TCP/IP выбран в качестве основного, хотя поддерживаются и другие протоколы (например, стек IPX/SPX, протокол NetBIOS).

Стек протоколов TCP/IP обладает двумя важными свойствами:

- платформонезависимостью, т. е. возможна его реализация на самых разных операционных системах и процессорах;
- открытостью, т. е. стандарты, по которым строится стек TCP/IP, доступны любому желающему.

История создания TCP/IP

В 1967 году Агентство по перспективным исследовательским проектам министерства обороны США (ARPA – Advanced Research Projects Agency) инициировало разработку компьютерной сети, которая должна была связать ряд университетов и научно-исследовательских центров, выполнявших заказы Агентства. Проект получил название ARPANET. К 1972 году сеть соединяла 30 узлов.

В рамках проекта ARPANET были разработаны и в 1980–1981 годах опубликованы основные протоколы стека TCP/IP – IP, TCP и UDP. Важным фактором распространения TCP/IP стала реализация этого стека в операционной системе UNIX 4.2 BSD (1983).

К концу 80-х годов значительно расширившаяся сеть ARPANET стала называться Интернет (Interconnected networks – связанные сети) и объединяла университеты и научные центры США, Канады и Европы.

В 1992 году появился новый сервис Интернет – WWW (World Wide Web – всемирная паутина), основанный на протоколе HTTP. Во многом благодаря WWW Интернет, а с ним и протоколы TCP/IP, получил в 90-е годы бурное развитие.

В начале XXI века стек TCP/IP приобретает ведущую роль в средствах коммуникации не только глобальных, но и локальных сетей.

Модель OSI

Модель взаимодействия открытых систем (OSI – Open Systems Interconnection) была разработана Международной организацией по стандартизации (ISO – International Organization for Standardization) для единообразного подхода к построению и объединению сетей. Разработка модели OSI началась в 1977 году и закончилась в 1984 году утверждением стандарта. С тех пор модель является эталонной для разработки, описания и сравнения различных стеков протоколов.

Модель OSI включает семь уровней: физический, канальный, сетевой, транспортный, сеансовый, уровень представления и прикладной.

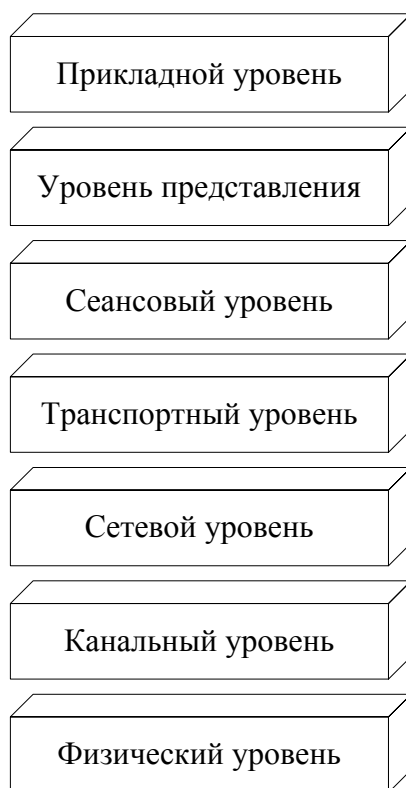


Рис. 2.1. Модель OSI

Рассмотрим кратко функции каждого уровня.

1. Физический уровень (physical layer) описывает принципы передачи сигналов, скорость передачи, спецификации каналов связи. Уровень реализуется аппаратными средствами (сетевой адаптер, порт концентратора, сетевой кабель).

2. Канальный уровень (data link layer) решает две основные задачи – проверяет доступность среды передачи (среда передачи чаще всего оказывается разделена между несколькими сетевыми узлами), а также обнаруживает и исправляет ошибки, возникающие в процессе передачи. Реализация уровня является программно-аппаратной (например, сетевой адаптер и его драйвер).

3. Сетевой уровень (network layer) обеспечивает объединение сетей, работающих по разным протоколам канального и физического уровней, в составную сеть. При этом каждая из сетей, входящих в единую сеть, называется *подсетью* (subnet). На сетевом уровне приходится решать две основные задачи – *маршрутизации* (routing, выбор оптимального пути передачи сообщения) и *адресации* (addressing, каждый узел в составной сети должен иметь уникальное имя). Обычно функции сетевого уровня реализует специальное устройство – *маршрутизатор* (router) и его программное обеспечение.

4. Транспортный уровень (transport layer) решает задачу надежной передачи сообщений в составной сети с помощью подтверждения доставки и повторной отправки пакетов. Этот уровень и все следующие реализуются программно.

5. Сеансовый уровень (session layer) позволяет запоминать информацию о текущем состоянии сеанса связи и в случае разрыва соединения возобновлять сеанс с этого состояния.

6. Уровень представления (presentation layer) обеспечивает преобразование передаваемой информации из одной кодировки в другую (например, из ASCII в EBCDIC).

7. Прикладной уровень (application layer) реализует интерфейс между остальными уровнями модели и пользовательскими приложениями.

Структура TCP/IP

В основе структуры TCP/IP лежит не модель OSI, а собственная модель, называемая DARPA (Defense ARPA – новое название Агентства по перспективным исследовательским проектам) или DoD (Department of Defense – Министерство обороны США). В этой модели всего четыре уровня. Соответствие модели OSI модели DARPA, а также основным протоколам стека TCP/IP показано на рис. 2.2.

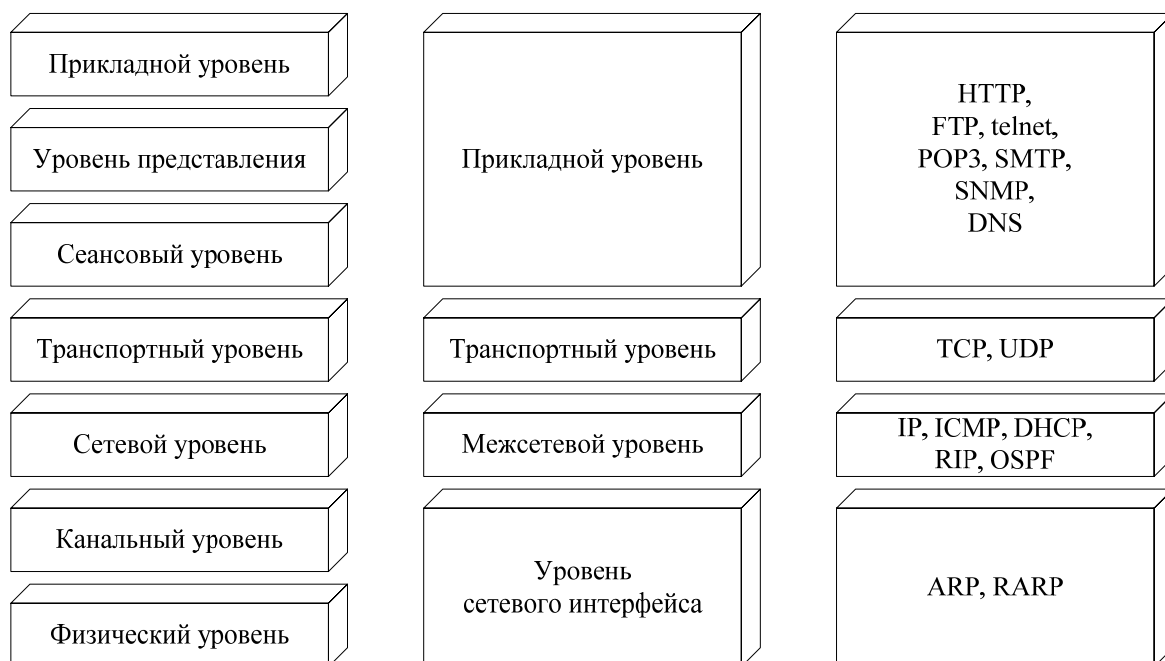


Рис. 2.2. Соответствие протоколов TCP/IP моделям OSI и DARPA

Следует заметить, что нижний уровень модели DARPA – уровень сетевых интерфейсов – строго говоря, не выполняет функции канального и физического уровней, а лишь обеспечивает связь (интерфейс) верхних уровней DARPA с технологиями сетей, входящих в составную сеть (например, Ethernet, FDDI, ATM).

Все протоколы, входящие в стек TCP/IP, стандартизованы в документах RFC.

Документы RFC

Утвержденные официальные стандарты Интернета и TCP/IP публикуются в виде документов RFC (Request for Comments – рабочее предложение). Стандарты разрабатываются всем сообществом ISOC (Internet Society – Сообщество Интернет, международная общественная организация). Любой член ISOC может представить на рассмотрение документ для его публикации в RFC. Далее документ рассматривается техническими экспертами, группами разработчиков и редактором RFC и проходит в соответствии с RFC 2026 следующие этапы, называемые уровнями готовности (maturity levels):

1) *черновик* (Internet Draft) – на этом этапе с документом знакомятся эксперты, вносятся дополнения и изменения;

2) *предложенный стандарт* (Proposed Standard) – документу присваивается номер RFC, эксперты подтвердили жизнеспособность предлагаемых решений, документ считается перспективным, желательно, чтобы он был опробован на практике;

3) *черновой стандарт* (Draft Standard) – документ становится черновым стандартом, если не менее двух независимых разработчиков реализовали и успешно применили предлагаемые спецификации. На этом этапе ещё допускаются незначительные исправления и усовершенствования;

4) *стандарт Интернета* (Internet Standard) – наивысший этап утверждения стандарта, спецификации документа получили широкое распространение и хорошо зарекомендовали себя на практике. Список стандартов Интернета приведен в RFC 3700. Из тысяч RFC только несколько десятков являются документами в статусе «стандарт Интернета».

Кроме стандартов документами RFC могут быть также описания новых сетевых концепций и идей, руководства, результаты экспериментальных исследований, представленных для информации и т. д. Таким документам RFC может быть присвоен один из следующих статусов:

- *экспериментальный* (Experimental) – документ, содержащий сведения о научных исследованиях и разработках, которые могут заинтересовать членов ISOC;
- *информационный* (Informational) – документ, опубликованный для предоставления информации и не требующий одобрения сообщества ISOC;
- *лучший современный опыт* (Best Current Practice) – документ, предназначенный для передачи опыта конкретных разработок, например реализаций протоколов.

Статус указывается в заголовке документа RFC после слова *Category* (Категория). Для документов в статусе стандартов (Proposed Standard, Draft Standard, Internet Standard) указывается название *Standards Track*, так как уровень готовности может меняться.

Номера RFC присваиваются последовательно и никогда не выдаются повторно. Первоначальный вариант RFC никогда не обновляется. Обновленная версия публикуется под новым номером. Устаревший и замененный документ RFC получает статус *исторический* (Historic).

Все существующие на сегодня документы RFC можно посмотреть, например, на сайте www.rfc-editor.org. В августе 2007 года их насчитывалось более 5000. Документы RFC, упоминаемые в этом курсе, приведены в Приложении I.

Обзор основных протоколов

Протокол IP (Internet Protocol) – это основной протокол сетевого уровня, отвечающий за адресацию в составных сетях и передачу пакета между сетями. Протокол IP является *дейтаграммным* протоколом, т. е. не гарантирует доставку пакетов до узла назначения. Обеспечением гарантий занимается протокол транспортного уровня TCP.

Протоколы RIP (Routing Information Protocol – протокол маршрутной информации) и *OSPF (Open Shortest Path First* – «первыми открываются кратчайшие маршруты») – протоколы маршрутизации в IP-сетях.

Протокол ICMP (Internet Control Message Protocol – протокол управляющих сообщений в составных сетях) предназначен для обмена информацией об ошибках между маршрутизаторами сети и узлом-источником пакета. С помощью специальных пакетов сообщает о невозможности доставки пакета, о продолжительности сборки пакета из фрагментов, об аномальных величинах параметров, об изменении маршрута пересылки и типа обслуживания, о состоянии системы и т. п.

Протокол ARP (Address Resolution Protocol – протокол преобразования адресов) преобразует IP-адреса в аппаратные адреса локальных сетей. Обратное преобразование осуществляется с помощью протокола *RARP (Reverse ARP)*.

TCP (Transmission Control Protocol – протокол управления передачей) обеспечивает надежную передачу сообщений между удаленными узлами сети за счет образования логических соединений. TCP позволяет без ошибок доставить сформированный на одном из компьютеров поток байт на любой другой компьютер, входящий в составную сеть. TCP делит поток байт на части – *сегменты* и передает их сетевому уровню. После того как эти сегменты будут доставлены в пункт назначения, протокол TCP снова соберет их в непрерывный поток байт.

UDP (User Datagram Protocol – протокол дейтаграмм пользователя) обеспечивает передачу данных дейтаграммным способом.

Далее рассматриваются протоколы прикладного уровня.

HTTP (HyperText Transfer Protocol – протокол передачи гипертекста) – протокол доставки web-документов, основной протокол службы WWW.

FTP (File Transfer Protocol – протокол передачи файлов) – протокол для пересылки информации, хранящейся в файлах.

POP3 (Post Office Protocol version 3 – протокол почтового офиса) и *SMTP (Simple Mail Transfer Protocol* – простой протокол пересылки почты) – протоколы для доставки входящей электронной почты (POP3) и отправки исходящей (SMTP).

Telnet – протокол эмуляции терминала¹, позволяющий пользователю подключаться к другим удалённым станциям и работать с ними со своей машины, как если бы она была их удалённым терминалом.

SNMP (Simple Network Management Protocol – простой протокол управления сетью) предназначен для диагностики работоспособности различных устройств сети.

¹ Терминал – это сочетание устройства ввода и устройства вывода, например клавиатура и дисплей.

Утилиты диагностики TCP/IP

В состав операционной системы Windows Server 2003 входит ряд утилит (небольших программ), предназначенных для диагностики функционирования стека TCP/IP. Каждый системный администратор должен знать эти утилиты и уметь применять их на практике.

Информацию о любой утилите можно вывести, набрав в командной строке имя утилиты с ключом «/?», например: `IPconfig /?`

IPconfig

Утилита предназначена, во-первых, для вывода информации о конфигурации стека TCP/IP, во-вторых, для выполнения некоторых действий по настройке стека.

При вводе названия утилиты в командной строке без параметров на экране отобразится информация об основных настройках TCP/IP (эти настройки рассматриваются в следующих лекциях):

- суффикс DNS (Connection-specific DNS Suffix);
- IP-адрес (IP Address);
- маска подсети (Subnet Mask);
- шлюз по умолчанию (Default Gateway).

Приведем основные ключи утилиты:

- **/all** – отображение полной информации о настройке стека TCP/IP на данном компьютере. Следует отметить, что при наличии нескольких сетевых адаптеров выводятся данные по каждому адаптеру отдельно. Наиболее важные сведения кроме представленных выше – физический адрес (MAC-адрес) сетевого адаптера (Physical Address) и наличие разрешения DHCP (DHCP Enabled).
- **/release** – освобождение IP-адреса (имеет смысл, если DHCP разрешен).
- **/renew** – обновление конфигурации TCP/IP (обычно выполняется, если DHCP разрешен).
- **/displaydns** – вывод на экран кэша имен DNS.
- **/flushdns** – очистка кэша имен DNS.
- **/registerdns** – обновление аренды DHCP и перерегистрация доменного имени в базе данных службы DNS.

Ping

Основная цель этой популярной утилиты – выяснение возможности установления соединения с удаленным узлом. Кроме того, утилита может обратиться к удаленному компьютеру по доменному имени, чтобы проверить способность преобразования символьного доменного имени в IP-адрес.

Принцип работы: утилита отправляет на удаленный узел несколько пакетов (число пакетов определяется ключом **-n**, по умолчанию четыре) по протоколу ICMP. Такие пакеты называются эхо-пакетами, т. е. требуют

ответа. Если удаленный узел доступен, он отвечает на каждый эхо-пакет своим пакетом, а утилита измеряет интервал между отправкой эхо-пакета и приходом ответа.

Нужно отметить, что отсутствие ответа может быть связано не с физической недоступностью удаленного компьютера, а с тем, что на нем установлено программное обеспечение, запрещающее отправку ответов на эхо-пакеты (брандмауэр – firewall).

Основные ключи:

- **-t** – пакеты отправляются до тех пор, пока пользователь не нажмет комбинацию CTRL+C.
- **-a** – определение доменного имени по IP-адресу.
- **-l <размер>** – максимальный размер пакета (по умолчанию 32 байта).
- **-w <таймаут>** – задание времени ожидания ответа в миллисекундах (по умолчанию 1000 миллисекунд = 1 секунда).

Tracert

Название утилиты произошло от Trace Route – отслеживание маршрута. Утилита позволяет решить следующие задачи:

- проследить путь прохождения пакета от данного компьютера до удаленного узла (отображаются промежуточные узлы-маршрутизаторы);
- выявить участки задержки пакетов;
- выявить места потери пакетов.

Принцип работы: утилита отправляет эхо-пакеты на заданный удаленный узел. Отличие между эхо-пакетами заключается в параметре, который называется «время жизни» (TTL – Time To Live). Этот параметр обозначает количество маршрутизаторов (процесс перехода пакета через маршрутизатор называется *hop* – прыжок), которое может пройти пакет, прежде чем попадет на заданный узел. Каждый маршрутизатор уменьшает время жизни на единицу. Если на каком-то маршрутизаторе TTL станет равным нулю, тот отбрасывает пакет и отправляет служебное сообщение на узел-источник.

Первый эхо-пакет посылается с временем жизни, равным единице. Первый маршрутизатор отбрасывает эхо-пакет и отправляет служебное сообщение, в котором содержится информации об имени и адресе маршрутизатора. Следующий эхо-пакет имеет TTL = 2 и отбрасывается уже на втором маршрутизаторе. Таким образом, эхо-пакеты отправляются с увеличением времени жизни на единицу, пока не придет ответ от заданного удаленного узла или время ожидания не будет превышено.

Основные ключи:

- **/h <maximum_hops>** – максимальное число хопов (маршрутизаторов) при поиске узла.
- **/w <таймаут>** – задание времени ожидания ответа в миллисекундах.

Netstat

Утилита отображает статистическую информацию по протоколам IP, TCP, UDP и ICMP, а также позволяет отслеживать сетевые соединения.

Основные ключи:

- /a – список всех подключений и прослушивающихся портов.
- /e – статистика для Ethernet.
- /n – список всех подключений и портов в числовом формате.
- /s – статистика для перечисленных четырех протоколов.
- <interval> – интервал в секундах, через который утилита выводит требуемую информацию (для прекращения вывода – CTRL+C).

Arp

Эта утилита работает с протоколами преобразования IP-адресов в MAC-адреса и обратно ARP и RARP. С её помощью можно выводить на экран таблицу соответствия IP-адресов и MAC-адресов (ARP-кэш), добавлять и удалять записи в ней.

Основные ключи:

- /a – отображение таблицы ARP или, если указан IP-адрес, запись только для этого адреса.
- /s – добавление записи в таблицу.
- /d – удаление записи из таблицы.

Hostname

Это самая простая утилита – она выводит на экран имя компьютера.

Резюме

Стек протоколов TCP/IP – это самый распространенный на сегодняшний день набор иерархически упорядоченных протоколов, применяемый как в локальных, так и в глобальных сетях. Важнейшие протоколы стека – IP, TCP и UDP – появились в начале 80-х годов в рамках проекта ARPANET, который являлся предшественником Интернета. В 90-е годы по мере развития Интернета роль стека TCP/IP сильно возросла.

Стек TCP/IP был разработан на основе модели сетевого взаимодействия DARPA, хотя между уровнями модели DARPA, международной семиуровневой моделью OSI и стеком TCP/IP может быть установлено соответствие. Стандарты протоколов TCP/IP отражены в свободно доступных документах RFC.

Основными протоколами стека являются IP, TCP, UDP, ICMP, ARP, протоколы маршрутизации RIP и OSPF, протоколы прикладного уровня HTTP, FTP, POP3, SMTP, telnet, SNMP.

Для диагностики и управления стеком TCP/IP в операционной системе Microsoft Windows Server 2003 существуют специальные утилиты – IPconfig, ping, tracert, netstat, arp, hostname и др.

Контрольные вопросы

1. Объясните, что означают свойства «платформонезависимость» и «открытость» применительно к стеку протоколов TCP/IP.
2. Что такое ARPANET?
3. Поясните, для чего предназначена модель OSI? Где она применяется?
4. Назовите функции канального, сетевого и транспортного уровней модели OSI.
5. Чем отличается модель DARPA (DoD) от модели OSI? Как вы думаете, почему?
6. Что такое RFC? В файлах какого формата издаются RFC?
7. Для чего используется протокол ICMP? Протокол ARP?
8. Поясните принцип работы утилиты ping.
9. Поясните принцип работы утилиты tracert.

Лекция 3. IP-адресация

План лекции

- Адресация в TCP/IP-сетях.
- Типы адресов стека TCP/IP.
- Структура IP-адреса.
- Классы IP-адресов.
- Использование масок.
- Протокол IPv6.
- Особые IP-адреса.
- Протокол ARP.
- Резюме.
- Контрольные вопросы.

Адресация в TCP/IP-сетях

Стек протоколов TCP/IP предназначен для соединения отдельных подсетей, построенных по разным технологиям канального и физического уровней (Ethernet, Token Ring, FDDI, ATM, X.25 и т. д.) в единую составную сеть. Каждая из технологий нижнего уровня предполагает свою схему адресации. Поэтому на межсетевом уровне требуется единый способ адресации, позволяющий уникально идентифицировать каждый узел, входящий в составную сеть. Таким способом в TCP/IP-сетях является *IP-адресация*. Узел составной сети, имеющий IP-адрес, называется *хост* (host).

Хороший пример, иллюстрирующий составную сеть, – международная почтовая система адресации. Информация сетевого уровня – это индекс страны, добавленный к адресу письма, написанному на одном из тысяч языков земного шара, например на китайском. И даже если это письмо должно пройти через множество стран, почтовые работники которых не знают китайского, понятный им индекс страны-адресата подскажет, через какие промежуточные страны лучше передать письмо, чтобы оно кратчайшим путем попало в Китай. А уже там работники местных почтовых отделений смогут прочитать точный адрес, указывающий город, улицу, дом и человека, и доставить письмо адресату, так как адрес написан на языке и в форме, принятой в данной стране.

Типы адресов стека TCP/IP

В стеке TCP/IP используются три типа адресов:

- локальные (другое название – аппаратные);
- IP-адреса (сетевые адреса);

– символьные доменные имена.

Локальный адрес – это адрес, присвоенный узлу в соответствии с технологией подсети, входящей в составную сеть. Если подсетью является локальная сеть Ethernet, Token Ring или FDDI, то локальный адрес – это MAC-адрес (MAC address – Media Access Control address). MAC-адреса назначаются сетевым адаптерам и портам маршрутизаторов производителями оборудования и являются уникальными, так как распределяются централизованно. MAC-адрес имеет размер 6 байт и записывается в шестнадцатеричном виде, например 00-08-A0-12-5F-72.

IP-адреса (IP address) представляют собой основной тип адресов, на основании которых сетевой уровень передает сообщения, называемые IP-пакетами. Эти адреса состоят из 4 байт, записанных в десятичном виде и разделенных точками, например 117.52.9.44. Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых адаптеров. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Символьные доменные имена (domain name) служат для удобства представления IP-адресов. Человеку неудобно запоминать числовые IP-адреса, поэтому была разработана специальная служба, DNS (Domain Name System), устанавливающая соответствие между IP-адресами и символьными доменными именами, например www.rambler.ru. Подробнее DNS и символьные имена будут рассмотрены в лекции 5.

Структура IP-адреса

IP-адрес представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемых октетами, например:

00010001 11101111 00101111 01011110

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94.

Следует заметить, что максимальное значение октета равно 1111111_2 (двоичная система счисления), что соответствует в десятичной системе 255_{10} . Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными. Пример: 172.16.123.1 – действительный адрес, 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона.

IP-адрес состоит из двух логических частей – номера подсети (ID¹ подсети) и номера узла (ID хоста) в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули. Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом:

ID подсети: 172.16.0.0.

ID хоста: 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N , то общее количество узлов равно $2^N - 2$. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях (см. ниже в этой лекции).

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно $2^{16} - 2 = 65534$ узлов.

Для определения того, какая часть IP-адреса отвечает за ID подсети, а какая за ID хоста, применяются два способа: с помощью классов и с помощью масок. *Общее правило*: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Классы IP-адресов

Существует пять классов IP-адресов: А, В, С, D и Е (см. рис. 3.1). За принадлежность к тому или иному классу отвечают первые биты IP-адреса. Деление сетей на классы описано в RFC 791 (документ описания протокола IP).

Целью такого деления являлось создание малого числа больших сетей (класса А), умеренного числа средних сетей (класс В) и большого числа малых сетей (класс С).

¹ ID – identifier (идентификатор).

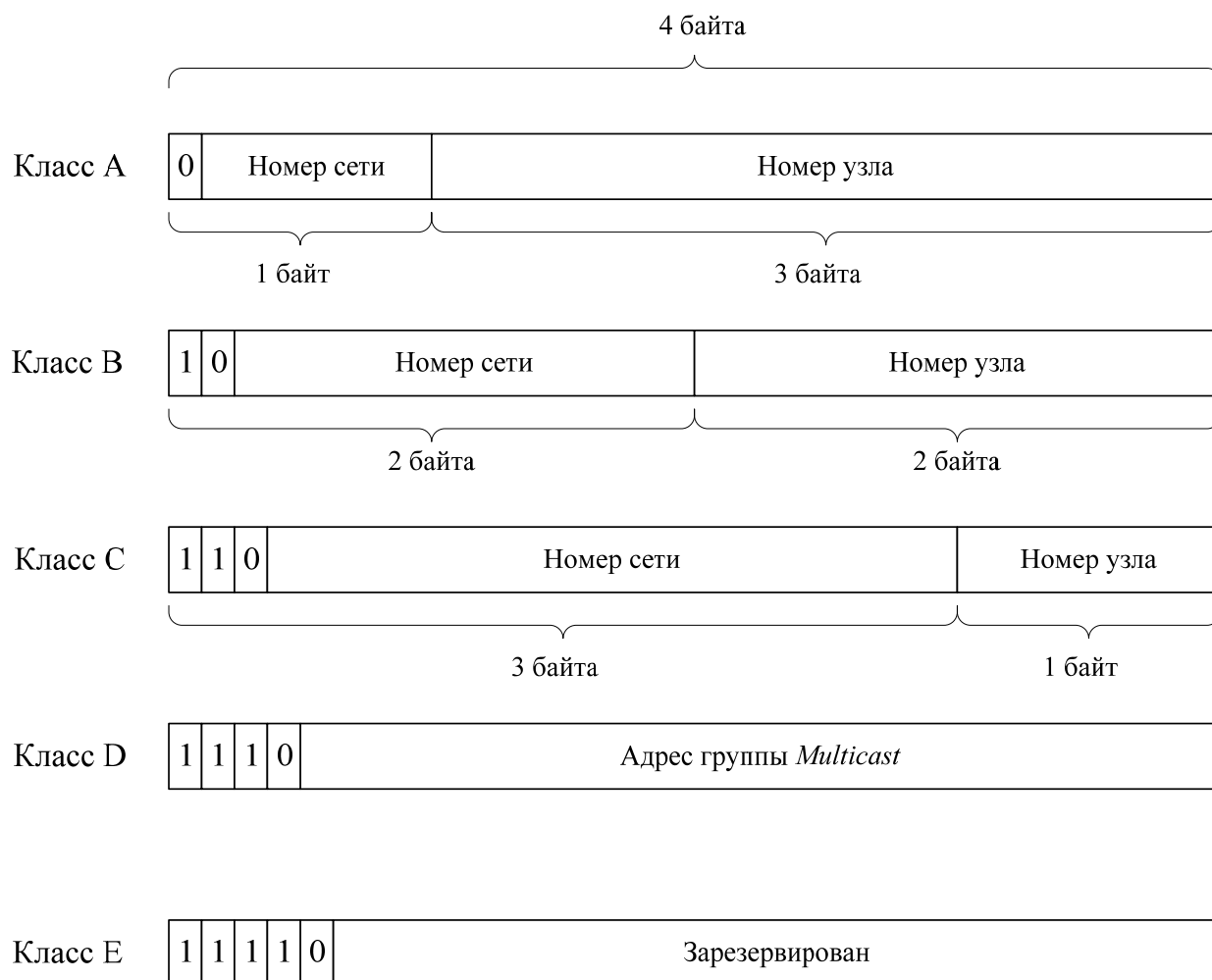


Рис. 3.1. Классы IP-адресов

Если адрес начинается с 0, то сеть относят к *классу А* и номер сети занимает один байт, остальные 3 байта интерпретируются как номер узла в сети. Сети класса А имеют номера в диапазоне от 1 до 126. Сетей класса А немного, зато количество узлов в них может достигать $2^{24} - 2$, то есть 16 777 214 узлов.

Если первые два бита адреса равны 10, то сеть относится к *классу В*. В сетях класса В под номер сети и под номер узла отводится по 16 бит, то есть по 2 байта. Таким образом, сеть класса В является сетью средних размеров с максимальным числом узлов $2^{16} - 2$, что составляет 65 534 узлов.

Если адрес начинается с последовательности 110, то это сеть *класса С*. В этом случае под номер сети отводится 24 бита, а под номер узла – 8 бит. Сети этого класса наиболее распространены, число узлов в них ограничено $2^8 - 2$, то есть 254 узлами.

Адрес, начинающийся с 1110, обозначает особый, *групповой адрес (multicast)*. Пакет с таким адресом направляется всем узлам, которым присвоен данный адрес.

Адреса класса Е в настоящее время не используются (зарезервированы для будущих применений).

Характеристики адресов разных классов представлены в таблице.

Класс	Первые биты	Наименьший номер сети	Наибольший номер сети	Количество сетей	Максимальное число узлов в сети
A	0	1.0.0.0	126.0.0.0	126	$2^{24} - 2 = 16777214$
B	10	128.0.0.0	191.255.0.0	16384	$2^{16} - 2 = 65534$
C	110	192.0.1.0	223.255.255.0	2097152	$2^8 - 2 = 254$
D	1110	224.0.0.0	239.255.255.255	Групповой адрес	
E	11110	240.0.0.0	247.255.255.255	Зарезервирован	

Применение классов удовлетворительно решало задачу деления на подсети в начале развития Интернета. В 90-е годы с увеличением числа подсетей стал ощущаться дефицит IP-адресов. Это связано с неэффективностью распределения при классовой схеме адресации. Например, если организации требуется тысяча IP-адресов, ей выделяется сеть класса В, при этом 64534 адреса не будут использоваться.

Существует два основных способа решения этой проблемы:

- 1) более эффективная схема деления на подсети с использованием масок (RFC 950);
- 2) применение протокола IP версии 6 (IPv6).

Использование масок

Маска подсети (subnet mask) – это число, которое используется в паре с IP-адресом; двоичная запись маски содержит единицы в тех разрядах, которые должны в IP-адресе интерпретироваться как номер сети.

Для стандартных классов сетей маски имеют следующие значения:

- класс А – 11111111. 00000000. 00000000. 00000000 (255.0.0.0);
- класс В – 11111111. 11111111. 00000000. 00000000 (255.255.0.0);
- класс С – 11111111. 11111111. 11111111. 00000000 (255.255.255.0).

Маска подсети записывается либо в виде, аналогичном записи IP-адреса, например 255.255.255.0, либо совместно с IP-адресом с помощью указания числа единичных разрядов в записи маски, например 192.168.1.1/24, т. е. в маске содержится 24 единицы (255.255.255.0).

При использовании масок можно вообще отказаться от понятия классов.

Пример

Пусть задан IP-адрес 17.239.47.94, маска подсети 255.255.0.0 (другая форма записи: 17.239.47.94/16).

Требуется определить ID подсети и ID хоста в обеих схемах адресации.

1) Адресация с использованием классов. Двоичная запись IP-адреса имеет вид:

00010001. 11101111. 00101111. 01011110

Так как первый бит равен нулю, адрес относится к классу А. Следовательно, первый байт отвечает за ID подсети, остальные три байта – за ID хоста:

ID подсети: 17.0.0.0.

ID хоста: 0.239.47.94.

2) Адресация с использованием масок. Запишем IP-адрес и маску подсети в двоичном виде:

IP-address: 17.239.47.94 = 00010001. 11101111. 00101111. 01011110
Subnet mask: 255.255.0.0 = 11111111. 11111111. 00000000. 00000000

Вспомним определение маски подсети: интерпретируем как номер подсети те биты, которые в маске равны 1, т. е. первые два байта. Оставшаяся часть IP-адреса будет номером узла в данной подсети.

ID подсети: 17.239.0.0.

ID хоста: 0.0.47.94.

Номер подсети можно получить другим способом, применив к IP-адресу и маске операцию логического умножения AND:

AND	00010001. 11101111. 00101111. 01011110
	11111111. 11111111. 00000000. 00000000
	<hr/>
	00010001. 11101111. 00000000. 00000000
	17 239 0 0

В масках количество единиц в последовательности, определяющей границу номера сети, не обязательно должно быть кратным 8.

Пример

Задан IP-адрес 192.168.89.16, маска подсети 255.255.192.0 (другая форма записи: 192.168.89.16/18).

Требуется определить ID подсети и ID хоста.

Воспользуемся операцией AND:

IP-address: 192.168.89.16 =	AND	11000000. 10101000. 01011001. 00010000
Subnet mask: 255.255.0.0 =		11111111. 11111111. 11000000. 00000000
subnet ID:		<hr/>
		11000000. 10101000. 01000000. 00000000
		192 168 64 0

Чтобы получить номер узла, нужно в битах, отвечающих за номер подсети, поставить нули:

Host ID: 00000000. 00000000. 00011001. 00010000 = 0.0.25.16.

Ответ: ID подсети = 192.168.64.0, ID хоста = 0.0.25.16.

Для масок существует важное правило: разрывы в последовательности единиц или нулей недопустимы. Например, не существует маски подсети, имеющей следующий вид:

11111111. 11110111. 00000000. 00001000 (255.247.0.8),

так как последовательности единиц и нулей не являются непрерывными.

С помощью масок администратор может структурировать свою сеть, не требуя от поставщика услуг дополнительных номеров сетей.

Пример

Допустим, организации выделена сеть класса В: 160.95.0.0 (рис. 3.2).

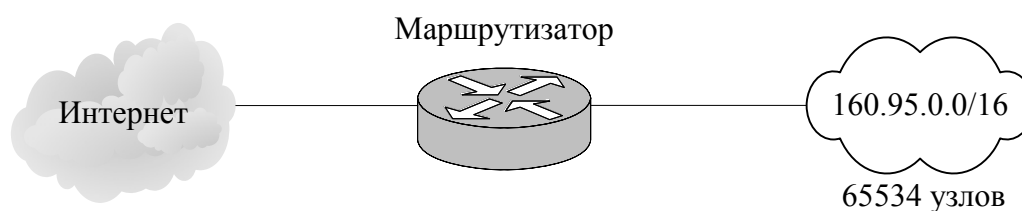


Рис. 3.2. Сеть класса В до деления на подсети

В такой сети может находиться до 65534 узлов. Однако организации требуется 3 независимые сети с числом узлов в каждой не более 254. В этой ситуации можно применить деление на подсети с помощью масок. Например, при использовании маски 255.255.255.0 третий байт адреса будет определять номер внутренней подсети, а четвертый байт – номер узла (см. рис. 3.3).

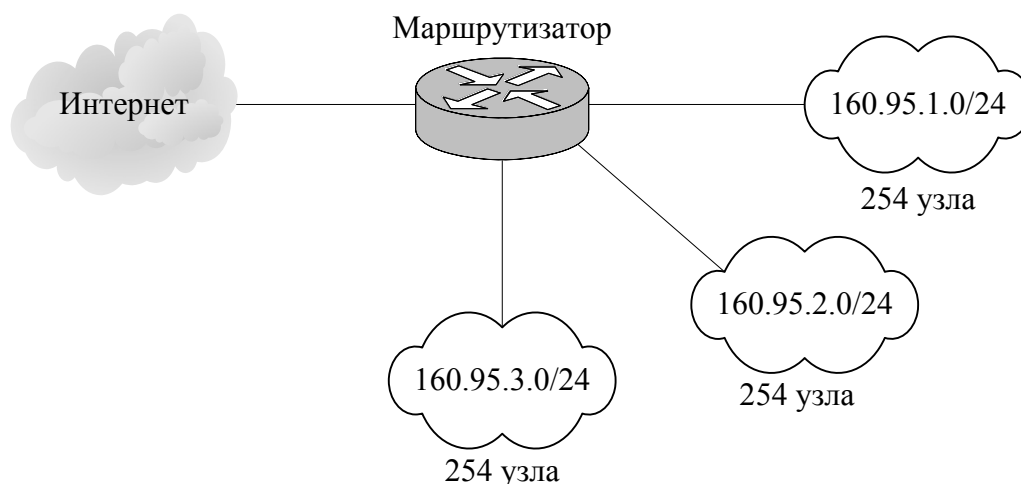


Рис. 3.3. Сеть класса В после деления на подсети

Маршрутизаторы во внешней сети (Интернете) ничего «не знают» о делении сети 160.95.0.0 на подсети, все пакеты направляются на маршрутизатор организации, который переправляет их в требуемую внутреннюю подсеть.

Протокол IPv6

Использование масок является временным решением проблемы дефицита IP-адресов, так как адресное пространство протокола IP не увеличивается, а количество хостов в Интернете растет с каждым днем. Для принципиального решения проблемы требуется существенное увеличение количества IP-адресов.

Используемый в настоящее время и рассматриваемый в данном курсе протокол IP называется IPv4 – протокол IP 4-й версии. Для преодоления ограничений IPv4 был разработан *протокол IP 6-й версии* – IPv6 (RFC 2373, 2460).

Протокол IPv6 имеет следующие основные особенности:

- длина адреса 128 бит – такая длина обеспечивает адресное пространство 2^{128} , или примерно $3.4 \cdot 10^{38}$ адресов. Такое количество адресов позволит присваивать в обозримом будущем уникальные IP-адреса любым устройствам;
- автоматическая конфигурация – протокол IPv6 предоставляет средства автоматической настройки IP-адреса и других сетевых параметров даже при отсутствии таких служб, как DHCP (протокол DHCP будет рассмотрен в лекции 6);
- встроенная безопасность – для передачи данных является обязательным использование протокола защищенной передачи IPsec. Протокол IPv4 также может использовать IPsec, но не обязан этого делать.

В настоящее время многие производители сетевого оборудования включают поддержку протокола IPv6 в свои продукты, однако

преобладающим остается протокол IPv4. Связано это с тем, что IPv6 обратно несовместим с IPv4 и процесс перехода сопряжен с определенными трудностями.

Особые IP-адреса

Некоторые IP-адреса являются особыми, они не должны применяться для идентификации обычных сетей.

- Если первый октет ID сети начинается со 127, такой адрес считается адресом машины-источника пакета. В этом случае пакет не выходит в сеть, а возвращается на компьютер-отправитель. Такие адреса называются *loopback* («петля», «замыкание на себя») и используются для проверки функционирования стека TCP/IP.
- Если все биты IP-адреса равны нулю, адрес обозначает узел-отправитель и используется в некоторых сообщениях ICMP.
- Если все биты ID сети равны 1, адрес называется *ограниченным широковещательным (limited broadcast)*, пакеты, направленные по такому адресу рассылаются всем узлам той подсети, в которой находится отправитель пакета.
- Если все биты ID хоста равны 1, адрес называется *широковещательным (broadcast)*, пакеты, имеющие широковещательный адрес, доставляются всем узлам подсети назначения.
- Если все биты ID хоста равны 0, адрес считается идентификатором подсети (subnet ID).

Наличие особых IP-адресов объясняет, почему из диапазона доступных адресов исключаются два адреса – это случаи, когда все биты ID хоста равны 1 или 0. Например, в сети класса C не 256 (2^8), а 254 узлов.

Протокол ARP

Протокол IP действует на сетевом уровне модели OSI, поэтому IP-адреса называются сетевыми. Они предназначены для передачи сообщений в составных сетях, связывающих подсети, построенные на различных локальных или глобальных сетевых технологиях, например Ethernet или ATM. Однако для непосредственной передачи сообщения в рамках одной подсети вместо IP-адреса нужно использовать локальный (аппаратный) адрес технологии канального уровня, чаще всего MAC-адрес. При этом к IP-пакету добавляются заголовок и концевик кадра канального уровня, в заголовке указываются MAC-адреса источника и приемника кадра (см. рис. 3.4).

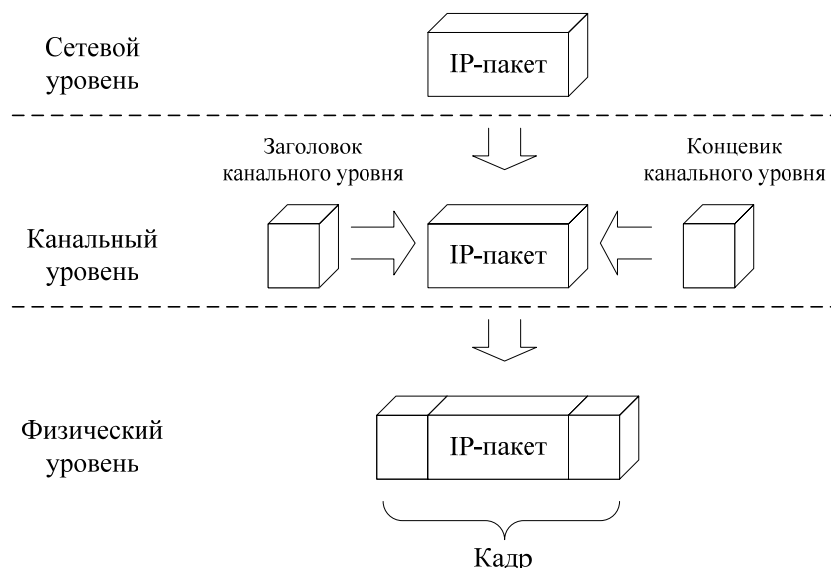


Рис. 3.4. Формирование кадра на канальном уровне

При формировании кадра канального уровня возникает проблема: каким образом по известному IP-адресу определить соответствующий MAC-адрес? Указанная проблема решается при помощи протокола ARP (Address Resolution Protocol – протокол разрешения¹ адресов).

Протокол ARP определяет MAC-адреса следующим образом. Осуществляется рассылка всем узлам сети специального кадра, который называется *ARP-запрос* (*ARP Request*). В этом кадре содержится IP-адрес компьютера, у которого требуется узнать MAC-адрес. Каждый узел сети принимает ARP-запрос и сравнивает IP-адрес из запроса со своим IP-адресом. Если адреса совпадают, узел высылает *ARP-ответ* (*ARP Reply*), содержащий требуемый MAC-адрес.

Результаты своей работы протокол ARP сохраняет в специальной таблице, хранящейся в оперативной памяти, которая называется *ARP-кэш*. При необходимости разрешения IP-адреса, протокол ARP сначала ищет IP-адрес в ARP-кэше и только в случае отсутствия нужной записи производит рассылку ARP-запроса.

ARP-кэш имеет следующий вид:

IP-адрес	MAC-адрес	Тип записи
192.168.1.1	03-E8-48-A1-57-7B	статический
192.168.1.2	03-E8-48-A1-43-88	динамический
192.168.1.3	03-E8-48-A1-F8-D9	динамический

Записи в ARP-кэше могут быть двух типов: статические и динамические. Статические записи заносятся в кэш администратором при помощи утилиты *arp* с ключом */s*. Динамические записи помещаются в кэш после полученного ARP-ответа и по истечении двух минут удаляются.

¹ Процесс получения по известному IP-адресу MAC-адреса называется *разрешением* IP-адреса.

Удаление происходит для того, чтобы при перемещении в другую подсеть компьютера с MAC-адресом, занесенным в таблицу, кадры не отправлялись бесполезно в сеть.

Иногда требуется по известному MAC-адресу найти IP-адрес (например, при начале работы компьютеров без жесткого диска, у которых есть MAC-адрес сетевого адаптера и им нужно определить свой IP-адрес). В этом случае используется реверсивный протокол RARP (Reverse ARP).

Резюме

В стеке TCP/IP используются три типа адресов: локальные (MAC-адреса), IP-адреса и доменные имена. IP-адрес действует на сетевом уровне и позволяет объединять разнородные локальные и глобальную сети в единую составную сеть.

IP-адрес состоит из 4 байт (октетов), разделенных точками. В его структуре выделяют две части – номер подсети и номер узла. Определение того, какая часть адреса отводится под номер подсети, осуществляется двумя способами – с помощью классов и с помощью масок. В схеме классовой адресации существует пять классов, основными являются классы А, В и С. Поле номера подсети определяется по первым битам адреса. При использовании масок номер подсети находится при помощи логического умножения маски на IP-адрес. Адресация с применением масок является более гибкой по сравнению с классами.

Уже довольно давно возникла проблема дефицита IP-адресов. Решение данной проблемы с помощью масок является временным. Принципиально другой подход заключается в существенном расширении адресного пространства и реализуется в протоколе IPv6.

Некоторые IP-адреса являются особыми и не используются при адресации конкретных узлов. Это нужно учитывать при назначении IP-адресов.

Для преобразования IP-адресов в аппаратные MAC-адреса применяется протокол ARP, для обратного преобразования – протокол RARP.

Контрольные вопросы

1. Что такое хост?
2. Перечислите виды и примеры адресов, используемых в стеке TCP/IP.
3. Из каких частей состоит IP-адрес?
4. Как определяется номер подсети в IP-адресе?
5. Каков диапазон возможных адресов у сети класса С?
6. Определите номер подсети на основе маски: 116.98.04.39/27.
7. Каковы основные особенности протокола IPv6?
8. Поясните принцип работы протокола ARP.

Лекция 4. Маршрутизация

План лекции

- Задача маршрутизации.
- Таблица маршрутизации.
- Принципы маршрутизации в TCP/IP.
- Создание таблиц маршрутизации.
- Протокол маршрутизации RIP.
- Протокол маршрутизации OSPF.
- Резюме.
- Контрольные вопросы.

Задача маршрутизации

Раскроем суть задачи маршрутизации. Пусть имеется составная сеть, задача состоит в том, чтобы доставить пакет из одной подсети в другую подсеть. Известны IP-адрес и маска подсети узла-отправителя (иными словами, ID подсети и ID хоста), IP-адрес узла-получателя. Сложность заключается в многочисленности возможных путей передачи пакета. Например, даже в простой сети, показанной на рис. 4.1, для передачи сообщения из подсети 1 в подсеть 4 существует восемь способов.

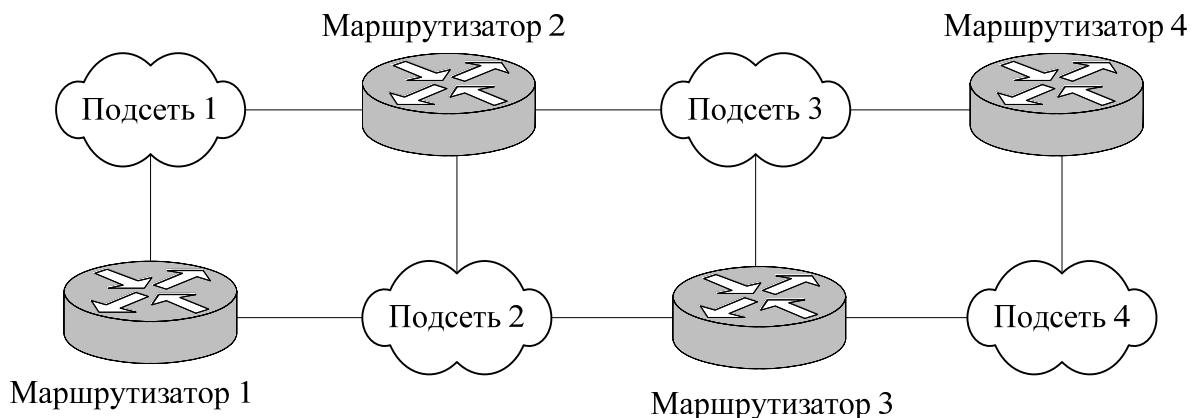


Рис. 4.1. Пример составной сети

Ещё одной проблемой является то, что из существующих путей требуется выбрать оптимальный по времени или по надежности. Кроме того, большинство составных сетей отличается динамичным изменением конфигурации, т. е. часть коммуникационных каналов может разрываться, другие, наоборот, возникают. Несмотря на все эти изменения, пакеты должны быстро и надежно доставляться в пункт назначения.

В сетях TCP/IP задача маршрутизации решается с помощью специальных устройств – маршрутизаторов, которые содержат *таблицы маршрутизации* (routing table). Компьютер с операционной системой Windows Server 2003 также может выступать в роли маршрутизатора. Вообще говоря, любой хост, на котором действует стек TCP/IP, имеет свою таблицу маршрутизации (естественно, гораздо меньших размеров, чем на маршрутизаторе).

Таблица маршрутизации

Таблица маршрутизации, создаваемая по умолчанию на компьютере с Windows Server 2003 (одна сетевая карта, IP-адрес: 192.168.1.1, маска подсети: 255.255.255.0), имеет следующий вид:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.1.2	192.168.1.1	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.1	192.168.1.1	20
192.168.1.1	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.1.255	255.255.255.255	192.168.1.1	192.168.1.1	20
224.0.0.0	240.0.0.0	192.168.1.1	192.168.1.1	20
255.255.255.255	255.255.255.255	192.168.1.1	192.168.1.1	1

В приведенной таблице имеются следующие поля:

- Network Destination (адрес назначения) – адрес хоста или подсети, для которых задан маршрут в таблице;
- Netmask (маска подсети) – маска подсети для адреса назначения;
- Gateway (шлюз – другое название маршрутизатора) – адрес для передачи пакета;
- Interface (интерфейс) – адрес собственного порта маршрутизатора (сетевой карты), на который следует передать пакет. Любой маршрутизатор содержит не менее двух портов. В компьютере в роли маршрутизатора с Windows Server 2003 портами являются сетевые карты;
- Metric (метрика) – число маршрутизаторов (число хопов), которые необходимо пройти для достижения хоста назначения. Для двух маршрутов с одинаковыми адресами назначения выбирается маршрут с наименьшей метрикой. Значение 20 в таблице соответствует 100-мегабитной сети Ethernet.

Кратко опишем записи в таблице по умолчанию.

- 0.0.0.0 – маршрут по умолчанию (default route). Эта запись выбирается в случае отсутствия совпадений с адресом назначения. В приведенной таблице маршруту по умолчанию соответствует шлюз 192.168.1.2 – это адрес порта маршрутизатора, который связывает данную подсеть с другими подсетями;

- 127.0.0.0 – маршрут обратной связи (loopback address), все пакеты с адресом, начинающимся на 127, возвращаются на узел-источник;
- 192.168.1.0 – адрес собственной подсети узла;
- 192.168.1.1 – собственный адрес узла (совпадает с маршрутом обратной связи);
- 192.168.1.255 – адрес широковещательной рассылки (пакет с таким адресом попадает всем узлам данной подсети);
- 224.0.0.0 – маршрут для групповых адресов;
- 255.255.255.255 – адрес ограниченной широковещательной рассылки.

Принципы маршрутизации в ТСР/IP

Рассмотрим, каким образом решается задача маршрутизации на примере составной сети, показанной на рис. 3.3, добавив некоторые подробности – IP-адреса и MAC-адреса узлов (рис. 4.2).

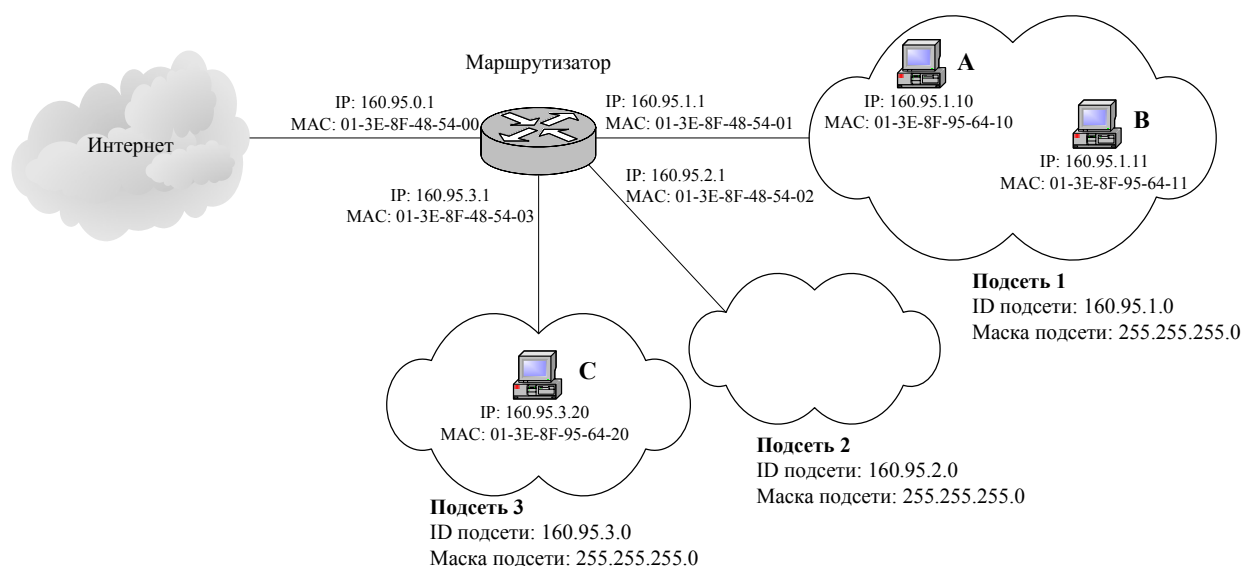


Рис. 4.2. Пример составной сети

В примере роль маршрутизатора играет компьютер с Windows Server 2003, который содержит четыре сетевые карты (четыре порта). Каждая карта имеет собственные MAC-адрес и IP-адрес, принадлежащий той подсети, к которой порт подключен.

Приведем часть таблицы маршрутизации для этого компьютера:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	160.95.0.2	160.95.0.1	20
160.95.0.0	255.255.255.0	160.95.0.1	160.95.0.1	20
160.95.0.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.0.255	255.255.255.255	160.95.0.1	160.95.0.1	20

Network Destination	Netmask	Gateway	Interface	Metric
160.95.1.0	255.255.255.0	160.95.1.1	160.95.1.1	20
160.95.1.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.1.255	255.255.255.255	160.95.1.1	160.95.1.1	20
160.95.2.0	255.255.255.0	160.95.2.1	160.95.2.1	20
160.95.2.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.2.255	255.255.255.255	160.95.2.1	160.95.2.1	20
160.95.3.0	255.255.255.0	160.95.3.1	160.95.3.1	20
160.95.3.1	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.3.255	255.255.255.255	160.95.3.1	160.95.3.1	20

Будем считать, что пакеты передает хост А. Его таблица маршрутизации может иметь следующий вид:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	160.95.1.1	160.95.1.10	20
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
160.95.1.0	255.255.255.0	160.95.1.10	160.95.1.10	20
160.95.1.10	255.255.255.255	127.0.0.1	127.0.0.1	20
160.95.1.255	255.255.255.255	160.95.1.10	160.95.1.10	20
224.0.0.0	240.0.0.0	160.95.1.10	160.95.1.10	20
255.255.255.255	255.255.255.255	160.95.1.10	160.95.1.10	1

Проанализируем, каким образом будет происходить передача пакетов от хоста А. Возможны три варианта местонахождения получателя:

- 1) подсеть 1 (хост А → хост В);
- 2) подсеть 2 или подсеть 3 (хост А → хост С);
- 3) внешняя сеть (хост А → Интернет).

Если узлом назначения является хост В, пакет не должен попадать на маршрутизатор, так как получатель находится в той же сети, что и отправитель. Хост А ищет в своей таблице маршрутизации подходящий маршрут. При этом для каждой строки на адрес назначения (IP хоста В: 160.95.1.11) накладывается маска подсети (операция логического умножения AND) и результат сравнивается с полем Network Destination. Подходящими оказываются два маршрута: 0.0.0.0 и 160.95.1.0. Из них выбирается маршрут с наибольшим числом двоичных единиц¹ – 160.95.1.0, т. е. пакет отправляется непосредственно хосту В. IP-адрес хоста В разрешается с помощью протокола ARP в MAC-адрес. В пересылаемом пакете будет указана следующая информация:

IP-адрес отправителя: 160.95.1.10
 MAC-адрес отправителя: 01-3E-8F-95-64-10

¹ Если окажется, что количество единиц совпадает, выбирается маршрут с наименьшей метрикой.

IP-адрес получателя: 160.95.1.11
MAC-адрес получателя: 01-3E-8F-95-64-11

Предположим теперь, что узел А отправляет пакет узлу С (подсеть 3). Поиск в собственной таблице маршрутизации не дает подходящих результатов, кроме маршрута по умолчанию – 0.0.0.0. Для этого маршрута указан адрес порта маршрутизатора 160.95.1.1 (default gateway – шлюз по умолчанию). Протокол ARP помогает определить MAC-адрес порта. Именно на него отправляется пакет сначала, причем указывается IP-адрес конечного получателя (узла С):

IP-адрес отправителя: 160.95.1.10
MAC-адрес отправителя: 01-3E-8F-95-64-10
IP-адрес получателя: 160.95.3.20
MAC-адрес получателя: 01-3E-8F-48-54-01

Модуль маршрутизации Windows Server 2003 анализирует полученный пакет, выделяет из него адрес узла С, осуществляет поиск в своей таблице маршрутизации (поиск происходит так же, как на хосте А). Находятся две подходящие записи: 160.95.3.0 и 0.0.0.0. Выбирается первый маршрут, так как в нем больше двоичных единиц. Пакет в подсеть 3 отправляется с порта 160.95.3.1:

IP-адрес отправителя: 160.95.1.10
MAC-адрес отправителя: 01-3E-8F-48-54-03
IP-адрес получателя: 160.95.3.20
MAC-адрес получателя: 01-3E-8F-95-64-20

Наконец, в случае, когда хост А осуществляет передачу во внешнюю сеть, пакет сначала попадает на маршрутизатор. Поиск в таблице маршрутизации дает единственный подходящий результат: 0.0.0.0. Поэтому пакет отправляется на порт внешнего маршрутизатора 160.95.0.2. Дальнейшее продвижение пакета выполняют маршрутизаторы Интернета.

Создание таблиц маршрутизации

Для построения таблиц маршрутизации существует два метода: статический и динамический. *Статический метод* заключается в том, что администратор вручную создает и удаляет записи в таблице. В состав операционной системы Windows Server 2003 входит утилита route. Она может использоваться с четырьмя командами:

- print – печать текущего содержимого таблицы;
- add – добавление новой записи;
- delete – удаление устаревшей записи;

- change – редактирование существующей записи.

Запись должна определяться следующим образом:

<destination> MASK <netmask> <gateway> METRIC <metric> IF <interface>

Например:

```
route add 160.95.1.0 mask 255.255.255.0 160.95.1.1 metric 20 IF 1
```

Кроме того, можно использовать два ключа:

- f – удаление из таблицы всех записей, кроме записей по умолчанию;
- p – создание постоянной записи (т. е. не исчезающей после перезагрузки). По умолчанию создаются временные записи.

Достоинством статического метода является простота. С другой стороны, для сетей с быстро меняющейся конфигурацией этот метод не подходит, так как администратор может не успевать отслеживать все изменения. В этом случае применяют *динамический метод* построения таблицы маршрутизации, основанный на протоколах маршрутизации. В Windows Server 2003 реализовано два таких протокола – RIP и OSPF.

Протокол маршрутизации RIP

Маршрутизаторы, работающие по протоколу RIP (Routing Information Protocol – протокол маршрутной информации), обмениваются содержимым своих таблиц путем групповых рассылок через каждые 30 секунд. Если за 3 минуты не получено никаких сообщений от соседнего маршрутизатора, линия связи между маршрутизаторами считается недоступной. Максимальное число маршрутизаторов, определенное в протоколе RIP, – 15. Узлы, находящиеся на большем расстоянии, считаются недоступными.

Так как обмен происходит целыми таблицами, при увеличении числа маршрутизаторов объем трафика сильно возрастает. Поэтому протокол RIP не применяется в крупных сетях.

В Windows Server 2003 реализована вторая версия протокола – RIP v2 (см. RFC 1723).

Протокол маршрутизации OSPF

Протокол OSPF (Open Shortest Path First – первыми открываются кратчайшие маршруты, описан в RFC 2328) в отличие от RIP может применяться в крупных сетях, так как, во-первых, в процессе обмена информацией о маршрутах передаются не таблицы маршрутизации целиком, а лишь их изменения. Во-вторых, в таблице содержится информация не о всей сети, а лишь о некоторой её области. Если адрес назначения отсутствует

в таблице, пакет направляется на специальный *пограничный маршрутизатор*, находящийся между областями.

Свое название протокол OSPF получил по алгоритму Дейкстры, лежащему в основе протокола и позволяющему найти наиболее короткий маршрут между двумя узлами сети.

Резюме

Задача маршрутизации заключается в определении оптимального пути передачи сообщения в составных сетях с меняющейся топологией. В сетях TCP/IP эту задачу решают маршрутизаторы на основе таблиц маршрутизации. В таблицы маршрутизации входит информация о номерах и масках подсетей назначения, адресах шлюзов и собственных портов маршрутизатора, а также о метриках. Решение о передаче пакета на тот или иной порт принимается на основании совпадения адреса назначения из пакета с адресом из таблицы, при этом оптимальный маршрут выбирается на основе метрики. Для адресов, отсутствующих в таблице, применяется специальный адрес – адрес шлюза по умолчанию.

Для создания таблиц маршрутизации в Windows Server 2003 используют два метода – статический, с помощью утилиты route, и динамический, с применением протоколов маршрутизации RIP и OSPF,

Контрольные вопросы

1. В чем заключается задача маршрутизации?
2. Для чего нужна таблица маршрутизации?
3. Назовите основные поля в таблице маршрутизации.
4. Что такое default gateway?
5. Перечислите ключи утилиты route.
6. Назовите преимущества и недостатки протокола RIP.
7. Назовите преимущества и недостатки протокола OSPF.

Лекция 5. Имена в TCP/IP

План лекции

- Необходимость применения символьных имен.
- Система доменных имен.
- Процесс разрешения имен.
- Записи о ресурсах.
- Утилита NSLOOKUP.
- Имена NetBIOS и служба WINS.
- Резюме.
- Контрольные вопросы.

Необходимость применения символьных имен

Как отмечалось в лекции 3, в стеке протоколов TCP/IP используются три типа адресов – аппаратные, IP-адреса и символьные доменные имена. Аппаратные адреса служат для адресации на канальном уровне. IP-адреса применяются на сетевом уровне, с их помощью можно построить большую составную сеть, например Интернет. Доменные имена кажутся в этом ряду необязательными; действительно, сеть будет работать и без них. Однако человеку-пользователю сети неудобно запоминать числовые IP-адреса, ассоциируя их с конкретными сетевыми объектами. Мы привыкли к символьным именам, и именно поэтому в стек TCP/IP была введена система доменных имен DNS (Domain Name System). Она описывается в RFC 1034 и RFC 1035. Полное название доменных имен – FQDN (Fully Qualified Domain Name – полностью определенное имя домена).

Кроме DNS-имен Windows Server 2003 поддерживает символьные имена NetBIOS (о них, а также о службе WINS, предназначенной для преобразования NetBIOS-имен в IP-адреса, рассказывается в конце этой лекции).

Система доменных имен

Система DNS основана на иерархической древовидной структуре, называемой *пространством доменных имен*. Доменом является каждый узел и лист этой структуры. На рис. 5.1 приведен фрагмент пространства доменных имен Интернета.

Самый верхний домен называется *корневым* (root domain). Корневой домен как реальный узел не существует, он исполняет роль вершины дерева. Непосредственные его потомки (поддомены) – домены первого уровня TLD (Top-Level Domain – домены верхнего уровня). Их можно разделить на три группы (см. Приложение II):

- **.arpa** – особый домен, используемый для преобразования IP-адресов в доменные имена (обратное преобразование). Содержит единственный дочерний домен – **in-addr**;
- домены организаций – **.com** (коммерческие организации), **.org** (некоммерческие организации), **.edu** (образовательные учреждения) и т. д.;
- домены стран (географические домены) – **.ru** (Россия), **.fr** (Франция), **.de** (Германия) и т. д.

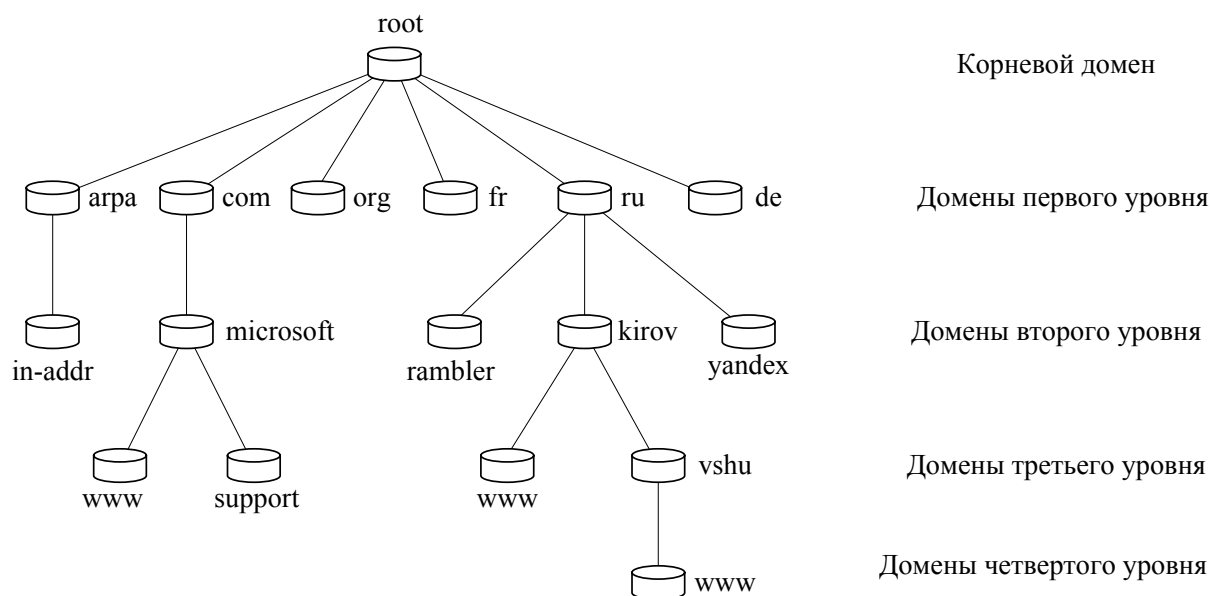


Рис. 5.1. Фрагмент пространства доменных имен Интернета

Домены первого уровня включают только домены второго уровня, записи об отдельных хостах могут содержаться в доменах, начиная со второго уровня.

Созданием и управлением доменами первого уровня с 1998 года занимается международная некоммерческая организация ICANN (Internet Corporation for Assigned Names and Numbers – Корпорация Интернет по присвоению имен и адресов, www.icann.org). Домены второго уровня, находящиеся в географических доменах, распределяются специальными национальными организациями, которым ICANN передало полномочия в этом вопросе. Управлением доменами третьего и следующего уровней занимаются владельцы соответствующих доменов второго уровня.

Полностью определенное доменное имя FQDN записывается следующим образом. Сначала идет имя хоста (лист в дереве пространства имен), затем через точку следует *DNS-суффикс* – последовательность доменных имен всех уровней до первого включительно. Запись оканчивается точкой, после которой подразумевается корневой домен. Пример FQDN для хоста **www** домена **vshu**:

www.vshu.kirov.ru.

В этой записи **www** – имя хоста, **vshu.kirov.ru.** – DNS-суффикс. Точку в конце FQDN обычно можно опускать.

Служба DNS

Пользователь работает с доменными именами, компьютеры пересылают пакеты, пользуясь IP-адресами. Для согласования двух систем адресаций необходима специальная служба, которая занимается переводом доменного имени в IP-адрес и обратно. Такая служба в TCP/IP называется *Domain Name Service* – *служба доменных имен* (аббревиатура DNS совпадает с аббревиатурой системы доменных имен). Процесс преобразования доменного имени в IP-адрес называется *разрешением доменного имени*.

В те времена, когда в сети ARPANET было несколько десятков компьютеров, задача преобразования символьного имени в IP-адрес решалась просто – создавался текстовый файл **hosts**, в котором хранились соответствия IP-адреса символьному имени. Этот файл должен был присутствовать на всех узлах сети. По мере увеличения числа узлов объем файла стал слишком большим, кроме того, администраторы не успевали отслеживать все изменения, происходящие в сети. Потребовалась автоматизация процесса разрешения имен, которую взяла на себя служба DNS.

Служба доменных имен поддерживает распределенную базу данных, которая хранится на специальных компьютерах – DNS-серверах. Термин «распределенная» означает, что вся информация не хранится в одном месте, её части распределены по отдельным DNS-серверам. Например, за домены первого уровня отвечают 13 корневых серверов, имеющих имена от A.ROOT-SERVERS.NET до M.ROOT-SERVERS.NET, расположенных по всему миру (большинство в США).

Такие части пространства имен называются *зонами* (zone). Пространство имен делится на зоны исходя из удобства администрирования. Одна зона может содержать несколько доменов, так же как информация о домене может быть рассредоточена по нескольким зонам. На DNS-сервере могут храниться несколько зон. В целях повышения надежности и производительности зона может быть размещена одновременно на нескольких серверах, в этом случае один из серверов является главным и хранит основную копию зоны (primary zone), остальные серверы являются дополнительными, на них содержатся вспомогательные копии зоны (secondary zone).

Для преобразования IP-адресов в доменные имена существуют *зоны обратного преобразования* (reverse lookup zone). На верхнем уровне пространства имен Интернета этим зонам соответствует домен **in-addr.arpa**. Поддомены этого домена формируются из IP-адресов, как показано на рис. 5.2.

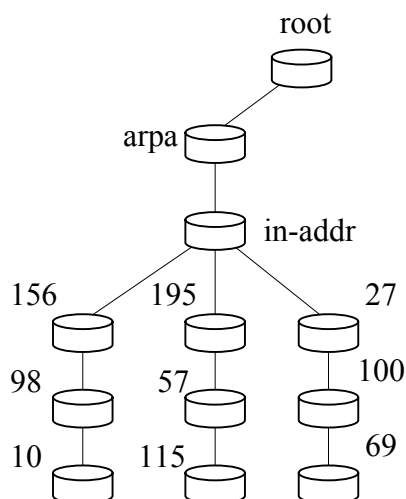


Рис. 5.2. Формирование поддоменов домена **arpa**

Следуя правилам формирования DNS-имен, зона обратного преобразования, соответствующая подсети 156.98.10.0, будет называться **10.98.156.in-addr.arpa**.

Процесс разрешения имен

Служба DNS построена по модели «клиент-сервер», т. е. в процессе разрешения имен участвуют DNS-клиент и DNS-серверы. Системный компонент DNS-клиента, называемый *DNS-распознавателем*, отправляет запросы на DNS-серверы. Запросы бывают двух видов:

- *итеративные* – DNS-клиент обращается к DNS-серверу с просьбой разрешить имя без обращения к другим DNS-серверам;
- *рекурсивные* – DNS-клиент перекладывает всю работу по разрешению имени на DNS-сервер. Если запрашиваемое имя отсутствует в базе данных и в кэше сервера, он отправляет итеративные запросы на другие DNS-серверы.

В основном DNS-клиентами используются рекурсивные запросы.

На рис. 5.3 проиллюстрирован процесс разрешения доменного имени с помощью рекурсивного запроса.

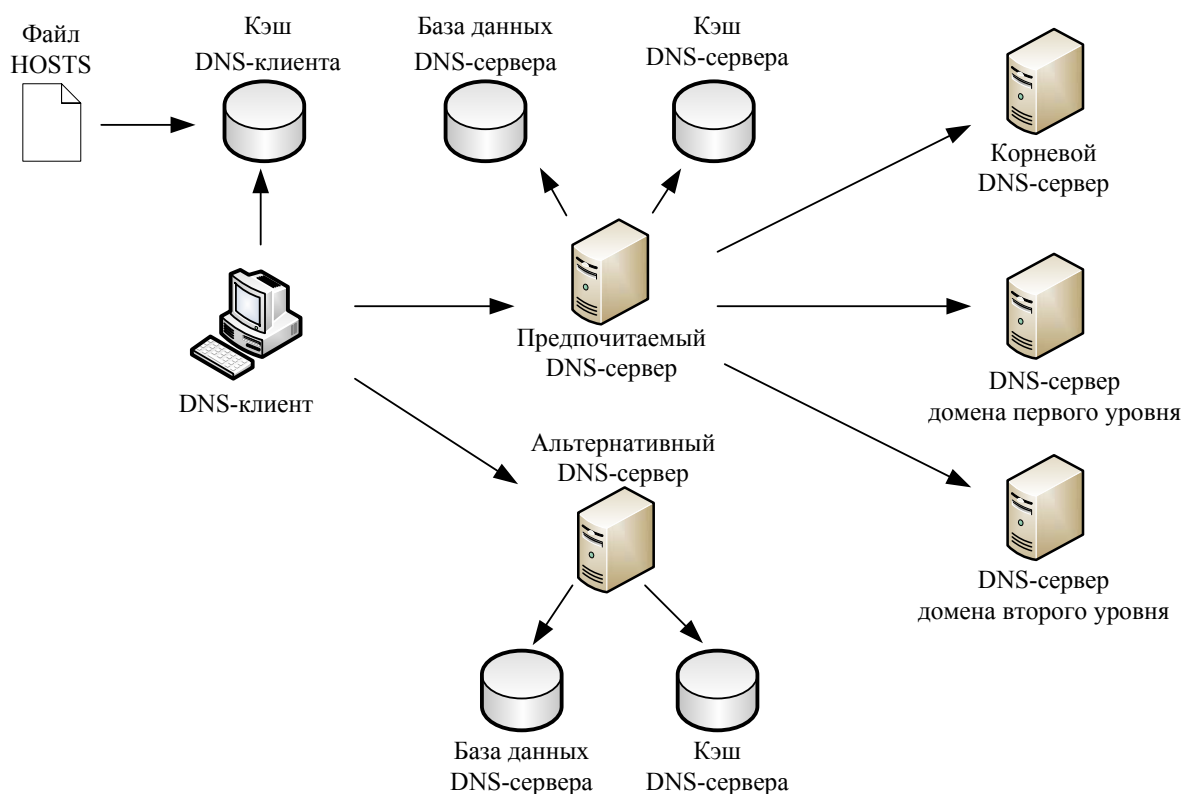


Рис. 5.3. Процесс обработки рекурсивного DNS-запроса

Сначала DNS-клиент осуществляет поиск в собственном локальном кэше DNS-имен. Это память для временного хранения ранее разрешенных запросов. В эту же память переносится содержимое файла HOSTS (каталог **windows/system32/drivers/etc**). Утилита IPconfig с ключом /displaydns отображает содержимое DNS-кэша.

Если кэш не содержит требуемой информации, DNS-клиент обращается с рекурсивным запросом к *предпочитаемому DNS-серверу* (Preferred DNS server), адрес которого указывается при настройке стека TCP/IP. DNS-сервер просматривает собственную базу данных, а также кэш-память, в которой хранятся ответы на предыдущие запросы, отсутствующие в базе данных. В том случае, если запрашиваемое доменное имя не найдено, DNS-сервер осуществляет итеративные запросы к DNS-серверам верхних уровней, начиная с корневого DNS-сервера.

Рассмотрим процесс разрешения доменного имени на примере. Пусть, требуется разрешить имя **www.microsoft.com**. Корневой домен содержит информацию о DNS-сервере, содержащем зону **.com**. Следующий запрос происходит к этому серверу, на котором хранятся данные о всех поддоменах зоны **.com**, в том числе о домене **microsoft** и его DNS-сервере. Сервер зоны **microsoft.com** может непосредственно разрешить имя **www.microsoft.com** в IP-адрес.

Иногда оказывается, что предпочитаемый DNS-сервер недоступен. Тогда происходит запрос по той же схеме к альтернативному DNS-серверу, если, конечно, при настройке стека TCP/IP был указан его адрес.

Записи о ресурсах

База данных DNS-сервера содержит записи о ресурсах (resource record), в которых содержится информация, необходимая для разрешения доменных имен и правильного функционирования службы DNS. Существует более 20 типов записей о ресурсах, приведем самые важные:

- A (Host Address – адрес хоста) – основная запись, используемая для непосредственного преобразования доменного имени в IP-адрес;
- CNAME (Canonical Name – псевдоним) – запись определяет псевдоним хоста и позволяет обращаться по разным именам (псевдонимам) к одному и тому же IP-адресу;
- MX (Mail Exchanger – почтовый обменник) – запись для установления соответствия имени почтового сервера IP-адресу;
- NS (Name Server – сервер имен) – запись для установления соответствия имени DNS-сервера IP-адресу;
- PTR (Pointer – указатель) – запись для обратного преобразования IP-адреса в доменное имя;
- SOA (Start Of Authority – начало авторизации) – запись для определения DNS-сервера, который хранит основную копию зоны;
- SRV (Service Locator – определитель служб) – запись для определения серверов некоторых служб (например, POP3, SMTP, LDAP).

Утилита NSLOOKUP

Утилита nslookup используется для проверки способности DNS-серверов выполнять разрешение имен. Утилита может работать в двух режимах:

- режим командной строки – обычный режим запуска утилит командной строки. Утилита nslookup выполняется в этом режиме, если указан какой-либо ключ;
- интерактивный режим – в этом режиме возможен ввод команд и ключей утилиты без повторения ввода имени утилиты.

Команды утилиты nslookup:

- help или ? – вывод справки о командах и параметрах утилиты;
- set – установка параметров работы утилиты;
- server <имя> – установка сервера по умолчанию (Default Server), используемого утилитой, с помощью текущего сервера по умолчанию;
- lserver <имя> – установка сервера по умолчанию утилиты с помощью первоначального;

- root – установка сервера по умолчанию утилиты на корневой сервер;
- ls <домен> – вывод информации о соответствии доменных имен IP-адресам для заданного домена;
- exit – выход из интерактивного режима.

Имена NetBIOS и служба WINS

Протокол NetBIOS (Network Basic Input Output System – сетевая базовая система ввода-вывода) был разработан в 1984 году для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. В операционных системах Microsoft Windows NT, а также в Windows 98, протокол и имена NetBIOS являлись основными сетевыми компонентами. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в связи с чем фундаментом сетевых решений стали протоколы TCP/IP и доменные имена.

Однако поддержка имен NetBIOS осталась и в операционной системе Windows Server 2003. Обусловлено это тем, что функционирование в сети таких операционных систем, как Windows NT и Windows 98, невозможно без NetBIOS.

Система имен NetBIOS представляет собой простое неиерархическое пространство, т. е. в имени NetBIOS отсутствует структура, деление на уровни, как в DNS-именах. Длина имени не более 15 символов (плюс один служебный).

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server 2003 используется служба WINS – Windows Internet Naming Service (служба имен в Интернете для Windows). Служба WINS работает, как и служба DNS, по модели «клиент-сервер». WINS-клиенты используют WINS-сервер для регистрации своего NetBIOS-имени и преобразования неизвестного NetBIOS-имени в IP-адрес. Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

Резюме

Символьные доменные имена введены в стек протоколов TCP/IP для удобства работы пользователей в сети. Доменные имена упорядочены иерархическую систему DNS, представляющую собой дерево доменов. Имеется единственный корневой домен, домены первого уровня делятся на три группы: по организационному признаку, по географическому признаку и специальный домен аgra, служащий для обратного преобразования IP-адресов.

Для преобразования доменных имен в IP-адреса в сетях TCP/IP функционирует служба DNS. Разрешение имен осуществляется при помощи локальных баз данных и запросов к DNS-серверам. Запросы бывают двух

видов – итеративные и рекурсивные. Итеративный запрос к DNS-серверу предполагает, что сервер будет осуществлять поиск только в своей базе данных. Рекурсивный запрос требует, чтобы DNS-сервер кроме поиска в локальной базе данных отправлял запросы на другие серверы.

Для диагностики работы службы DNS предназначена утилита nslookup.

Помимо доменных имен в сетях Microsoft используются имена NetBIOS. Для работы с ними устанавливается служба WINS.

Контрольные вопросы

1. Для чего необходимы доменные имена?
2. Для чего нужна служба DNS?
3. Что такое корневой домен?
4. Каково было предназначение файла hosts? Используется ли он сегодня?
5. Чем отличается служба DNS от системы DNS?
6. Объясните принцип действия итеративного запроса.
7. Объясните принцип действия рекурсивного запроса.
8. В чем отличие доменных имен от имен NetBIOS?

Лекция 6. Протокол DHCP

План лекции

- Проблема автоматизации распределения IP-адресов.
- Реализация DHCP в Windows.
- Параметры DHCP.
- Адреса для динамической конфигурации.
- DHCP-сообщения.
- Принцип работы DHCP.
- Авторизация DHCP-сервера.
- Резюме.
- Контрольные вопросы.

Проблема автоматизации распределения IP-адресов

Одной из основных задач системного администратора является настройка стека протоколов TCP/IP на всех компьютерах сети. Есть несколько необходимых параметров, которые следует настроить на каждом компьютере, – это IP-адрес, маска подсети, шлюз по умолчанию, IP-адреса DNS-серверов. Назначенные IP-адреса должны быть уникальны. В случае каких-либо изменений (например, изменился IP-адрес DNS сервера или шлюза по умолчанию) их нужно отразить на всех компьютерах. Если какие-либо параметры не указаны или не верны, сеть не будет работать стабильно.

Если в сети менее десяти компьютеров, администратор может успешно справляться с задачей настройки стека TCP/IP вручную, т. е. на каждом компьютере отдельно вводить параметры. IP-адрес, назначенный таким образом, называется *статическим*. При числе узлов сети более десяти (а многие сети включают десятки и сотни хостов) задача распределения параметров вручную становится трудной или вовсе невыполнимой.

В стеке TCP/IP существует протокол, позволяющий автоматизировать процесс назначения IP-адресов и других сетевых параметров, который называется DHCP – Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). Использование этого протокола значительно облегчает труд системного администратора по настройке сетей средних и больших размеров. Описание протокола DHCP приводится в документе RFC 2131.

Реализация DHCP в Windows

Протокол DHCP реализуется по модели «клиент-сервер», т. е. в сети должны присутствовать DHCP-сервер (роль которого может исполнять компьютер с операционной системой Windows Server 2003) и DHCP-клиент.

На компьютере-сервере хранится база данных с сетевыми параметрами и работает служба DHCP сервера. Компьютер-клиент (точнее, служба клиента DHCP) осуществляет запросы на автоматическую конфигурацию, и DHCP-сервер при наличии свободных IP-адресов выдает требуемые параметры.

Набор IP-адресов, выделяемых для компьютеров одной физической подсети, называется *областью действия* (scope). На одном сервере можно создать несколько областей действия. Важно только отслеживать, чтобы области действия не пересекались.

При запросе клиента DHCP-сервер выделяет ему произвольный свободный IP-адрес из области действия совместно с набором дополнительных сетевых параметров. При необходимости некоторые адреса из области действия можно *зарезервировать* (reserve) за определенным MAC-адресом. В этом случае только компьютеру с этим MAC-адресом (например, DNS-серверу, адрес которого не должен меняться) будет выделяться зарезервированный IP-адрес.

Адреса выделяются клиентам на определенное время, поэтому предоставление адреса называется *арендой* (lease). Время аренды в Windows Server 2003 может быть от 1 минуты до 999 дней (или неограниченно) и устанавливается администратором.

Параметры DHCP

Основная функция протокола DHCP – предоставление в аренду IP-адреса. Однако для правильной работы в сети TCP/IP хосту необходим ещё ряд параметров, которые также можно распространять посредством DHCP. Набор параметров указан в RFC 2132.

Перечислим только основные параметры:

- Subnet mask – маска подсети;
- Router – список IP-адресов маршрутизаторов;
- Domain Name Servers – список адресов DNS-серверов;
- DNS Domain Name – DNS-суффикс клиента;
- WINS Server Names – список адресов WINS-серверов;
- Lease Time – срок аренды (в секундах);
- Renewal Time (T1) – период времени, через который клиент начинает продлевать аренду;
- Rebinding Time (T2) – период времени, через который клиент начинает осуществлять широковещательные запросы на продление аренды.

Параметры могут применяться на следующих уровнях:

- уровень сервера;
- уровень области действия;
- уровень класса;
- уровень клиента (для зарезервированных адресов).

Параметры, определенные на нижележащем уровне, перекрывают параметры вышележащего уровня, например параметры клиента имеют больший приоритет, чем параметры сервера. Самый высокий приоритет имеют параметры, настроенные вручную на клиентском компьютере.

Уровень класса используется для объединения клиентов в группы и применения для этой группы отдельных параметров. Отнести клиента к определенному классу можно, применив утилиту IPconfig с ключом /setclassid.

Адреса для динамической конфигурации

При настройке областей действия перед администратором встает вопрос, какой диапазон адресов выбрать для сети своей организации? Ответ зависит от того, подключена ли сеть к Интернету.

Если сеть имеет доступ в Интернет, диапазон адресов назначается провайдером (ISP – Internet Service Provider, поставщик интернет-услуг) таким образом, чтобы обеспечить уникальность адресов в Интернете. Чаще всего бывает так, что провайдер выделяет один или несколько адресов для прямого доступа в Интернет и они присваиваются прокси-серверам, почтовым серверам и другим хостам, которые являются буферными узлами между сетью организации и Интернетом. Большинство остальных хостов получают доступ к интернет-трафику через эти буферные узлы. В этом случае диапазон внутренних адресов организации должен выбираться из множества частных адресов.

Частные адреса (Private addresses), описанные в RFC 1918, специально выделены для применения во внутренних сетях и не могут быть присвоены хостам в Интернете. Существует три диапазона частных адресов:

- ID подсети – 10.0.0.0, маска подсети: 255.0.0.0;
- ID подсети – 172.16.0.0, маска подсети: 255.240.0.0;
- ID подсети – 192.168.0.0, маска подсети: 255.255.0.0.

Внутри этих диапазонов адресов можно организовывать любые возможные подсети.

Если сеть не имеет доступа в Интернет, то теоретически можно выбрать любой диапазон IP-адресов, не учитывая наличия хостов с такими же адресами в Интернете. Однако на практике все равно лучше выбирать адреса из диапазона частных адресов, так как для сети, не имеющей выхода в Интернет, в ближайшем будущем подключение к глобальной сети может оказаться необходимым, и тогда возникнет проблема изменения схемы адресации.

Также следует отметить, что помимо описанных частных адресов существует диапазон *автоматических частных адресов* APIPA (Automatic Private IP Address): ID подсети – 169.254.0.0, маска подсети: 255.255.0.0. Адрес из этого диапазона выбирается хостом TCP/IP случайно, если отсутствует статический IP-адрес, DHCP-сервер не отвечает, и не указан

альтернативный статический адрес. После выбора IP-адреса, хост продолжает посылать запросы DHCP-серверу каждые пять минут.

DHCP-сообщения

Процесс функционирования служб DHCP заключается в обмене сообщениями между сервером и клиентом. Типы DHCP-сообщений приведены в таблице.

Тип сообщения	Направление	Значение
DHCPDISCOVER (DHCP-обнаружение)	Клиент → сервер	Широковещательный запрос для обнаружения DHCP-сервера
DHCPOFFER (DHCP-предложение)	Сервер → клиент	Ответ на DHCPDISCOVER, содержит предлагаемые сетевые параметры
DHCPREQUEST (DHCP-запрос)	Клиент → сервер	Запрос предложенных параметров
DHCPACK (DHCP-подтверждение)	Сервер → клиент	Подтверждение сетевых параметров
DHCPNAK (DHCP-несогласие)	Сервер → клиент	Отклонение запроса клиента
DHCPDECLINE (DHCP-отказ)	Клиент → сервер	Отказ клиента от предложенных параметров
DHCPRELEASE (DHCP-освобождение)	Клиент → сервер	Освобождение арендованного IP-адреса
DHCPINFORM (DHCP-информация)	Клиент → сервер	Запрос дополнительных параметров

Принцип работы DHCP

Диаграмма переходов, иллюстрирующая принципы работы протокола DHCP, приведена на рис. 6.1. На схеме овалами обозначены состояния, в которых может находиться DHCP-клиент. Из одного состояния в другое клиент может переходить только по дугам. Каждая дуга помечена дробью, числитель которой обозначает событие (чаще всего это сообщение от DHCP-сервера), после которого клиент переходит в соответствующее состояние, а знаменатель описывает действия DHCP-клиента при переходе. Черточка в числителе означает безусловный переход.

Начальное состояние, в котором оказывается служба DHCP-клиента при запуске, – это «Инициализация». Из этого состояния происходит безусловный переход в состояние «Выбор» с рассылкой широковещательного сообщения DHCPDISCOVER. DHCP-серверы (в одной сети их может быть несколько), принимая сообщение, анализируют свою

базу данных на предмет наличия свободных IP-адресов. В случае успеха, серверы отправляют сообщение DHCP OFFER, которое помимо IP-адреса содержит дополнительные параметры, призванные помочь клиенту выбрать лучшее предложение.

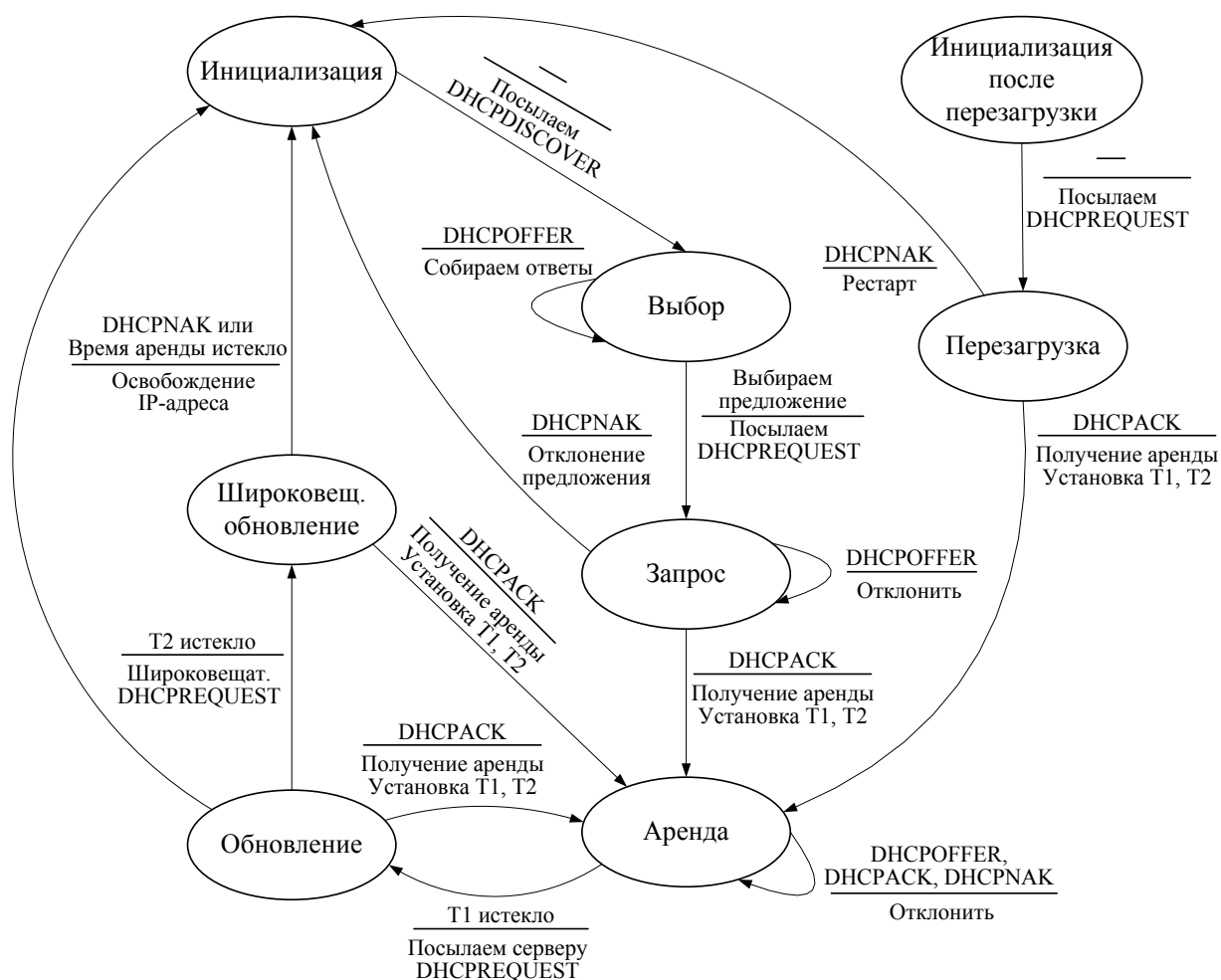


Рис. 6.1. Принцип работы протокола DHCP

Сделав выбор, клиент посылает широковещательное сообщение DHCPREQUEST, запрашивая предложенный IP-адрес и требуемые параметры (например, маска подсети, шлюз по умолчанию, IP-адреса DNS-серверов и др.) и переходит в состояние «Запрос». Данное сообщение требуется посылать широковещательно (т. е. оно должно доставляться всем компьютерам подсети), так как DHCP-серверы, предложения которых клиент отклонил, должны знать об отказе.

В состоянии «Запрос» клиент ожидает подтверждение сервера о возможности использования предложенных сетевых параметров. В случае прихода такого подтверждения (сообщение DHCPACK) клиент переходит в состояние «Аренда», одновременно начиная отсчет интервалов времени T1 и T2. Если сервер по каким-либо причинам не готов предоставить клиенту предложенный IP-адрес, он посылает сообщение DHCPNAK. Клиент

реагирует на это сообщение переходом в исходное состояние «Инициализация», чтобы снова начать процесс получения IP-адреса.

Состояние «Аренда» является основным рабочим состоянием – у клиента присутствуют все необходимые сетевые параметры, и сеть может успешно функционировать.

Через временной интервал T1 от момента получения аренды (обычно T1 равно половине общего времени аренды)¹ DHCP-клиент переходит в состояние «Обновление» и начинает процесс обновления аренды IP-адреса. Сначала клиент посылает DHCP-серверу сообщение DHCPREQUEST, включающее арендованный IP-адрес. Если DHCP-сервер готов продлить аренду этого адреса, то он отвечает сообщением DHCPACK и клиент возвращается в состояние «Аренда» и заново начинает отсчитывать интервалы T1 и T2.

В случае, если в состоянии «Обновление» по истечении интервала времени T2 (который обычно устанавливается равным 87,5% от общего времени аренды) все ещё не получено подтверждение DHCPACK, клиент переходит в состояние «Широковещательное обновление» с рассылкой широковещательного сообщения DHCPREQUEST. Такая рассылка делается в предположении, что DHCP-сервер поменял свой IP-адрес (или перешел в другую подсеть) и передал свою область действия другому серверу. В этом состоянии получение DHCPACK возвращает клиента в состояние «Аренда» и аренда данного IP-адреса продлевается. Если клиент получает от сервера сообщение DHCPNAK или общее время аренды истекает, то происходит переход в состояние «Инициализация» и клиент снова пытается получить IP-адрес.

В процессе работы может оказаться, что время аренды не истекло, а служба DHCP-клиента прекратила работу (например, в случае перезагрузки). В этом случае DHCP-клиент начинает работу в состоянии «Инициализация после перезагрузки», рассылает широковещательное сообщение DHCPREQUEST и переходит в состояние «Перезагрузка». В случае подтверждения продления аренды (сообщение DHCPACK от DHCP-сервера) клиент переходит в состояние «Аренда». Иначе (сообщение DHCPNAK) клиент оказывается в состоянии «Инициализация».

Авторизация DHCP-сервера

Неправильное функционирование DHCP-сервера в любой сети может привести к нарушению работы всей сети. Ошибки в настройке могут быть вызваны неправильным планированием, когда в одной подсети оказываются несколько DHCP-серверов, или действиями некомпетентного лица (а возможно, и злоумышленника). Для предотвращения последствий таких действий в Windows Server 2003 предусмотрен механизм *авторизации*

¹ Заблаговременные попытки продления аренды клиент предпринимает для того, чтобы в момент истечения времени аренды компьютер не оказался без IP-адреса. При этом работа клиента в сети была бы нарушена.

DHCP-серверов. Неавторизованный DHCP-сервер (unauthorized DHCP server) не будет работать в этой операционной системе.

Процедуру авторизации может выполнить только администратор. При этом адрес авторизованного DHCP-сервера регистрируется в каталоге Active Directory (см. лекцию 7). Затем при запуске служба DHCP-сервера проверяет наличие IP-адреса своего компьютера в списке авторизованных DHCP-серверов Active Directory и только после этого может продолжать свою работу.

Резюме

Существенной проблемой в компьютерных сетях является настройка сетевых параметров на всех узлах сети в условиях большого числа узлов и возможных изменений параметров. В сетях TCP/IP для решения указанной проблемы служит протокол DHCP, обеспечивающий автоматическую настройку сетевых параметров.

Протокол DHCP реализует соответствующая служба, работающая по модели «клиент-сервер». Служба DHCP по запросу клиентов выдает им IP-адреса из заданного диапазона и другие сетевые параметры в аренду на определенное время. По истечении времени аренды клиенты должны обновлять её.

Наиболее часто в локальных сетях применяются адреса из частных диапазонов, которые не используются в Интернете. В случае, если клиенту не назначен IP-адрес и он не смог получить его самостоятельно у DHCP-сервера, выбирается случайный автоматический частный адрес из подсети 169.254.0.0/16.

Для предотвращения несанкционированного использования DHCP-серверов в сетях Active Directory применяется механизм авторизации.

Контрольные вопросы

1. Для решения какой проблемы предназначен протокол DHCP?
2. Что такое область действия?
3. Почему адреса предоставляются в аренду на время, а не навсегда?
4. Перечислите основные параметры DHCP.
5. Назовите диапазоны частных адресов. Для чего они нужны?
6. Поясните значение сообщений DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.
7. По диаграмме переходов на рис. 6.1 объясните принципы работы DHCP-клиента.

Лекция 7. Служба каталога Active Directory

План лекции

- Понятие Active Directory.
- Структура каталога Active Directory.
- Объекты каталога и их именование.
- Иерархия доменов.
- Доверительные отношения.
- Организационные подразделения.
- Резюме.
- Контрольные вопросы.

Понятие Active Directory

В лекции 6 отмечалось, что в средних и крупных сетях задача настройки параметров протокола TCP/IP является очень сложной для администратора и вручную практически не выполнима. Для решения этой проблемы был разработан протокол DHCP, реализованный посредством службы DHCP.

Однако настройка сетевых параметров – лишь одна из множества задач, встающих перед системным администратором. В частности, в любой сети важнейшей является задача управления её ресурсами (файлами и устройствами, предоставленными в общий доступ), а также компьютерами и пользователями.

Для решения задач управления ресурсами в сетях под управлением Windows Server 2003 применяется служба каталога Active Directory (Активный Каталог). Данная служба обеспечивает доступ к базе данных (*каталогу*), в которой хранится информация обо всех объектах сети, и позволяет управлять этими объектами.

Группа компьютеров, имеющая общий каталог и единую политику безопасности¹, называется *доменом* (domain). Каждый домен имеет один или несколько серверов, именуемых *контроллерами домена* (domain controller), на которых хранятся копии каталога.

Перечислим основные преимущества, предоставляемые службой каталога Active Directory:

- централизованное управление – если в сети развернута служба Active Directory, системный администратор может выполнять большинство своих задач, используя единственный компьютер – *контроллер домена*;
- простой доступ пользователей к ресурсам – пользователь, зарегистрировавшись в домене на произвольном компьютере, может

¹ Политика безопасности – набор правил по применению средств обеспечения сетевой безопасности – паролей, учетных записей, протоколов аутентификации и защищенной передачи информации, шифрованной файловой системы и т. д.

получить доступ к любому ресурсу сети при условии наличия соответствующих прав;

- обеспечение безопасности – служба Active Directory совместно с подсистемой безопасности Windows Server 2003 предоставляет возможность гибкой настройки прав пользователей на доступ к ресурсам сети;

- масштабируемость – это способность системы повышать свои размеры и производительность по мере увеличения требований к ним. При расширении сети организации служба каталога Active Directory способна наращивать свои возможности – увеличивать размер каталога и число контроллеров домена.

Таким образом, служба каталога Active Directory, подобно службе DHCP, существенно облегчает работу системного администратора по управлению сетевыми объектами. Кроме того, пользователи получают возможность использовать ресурсы сети, не заботясь об их месторасположении, так как все запросы обрабатываются службой Active Directory.

Структура каталога Active Directory

Вся информация об объектах сети содержится в каталоге Active Directory. Физически эта база данных представляет собой файл **Ntds.dit**, который хранится на контроллере домена.

Каталог Active Directory может рассматриваться с двух позиций: с точки зрения логической структуры и с точки зрения физической структуры.

Логическая структура каталога Active Directory представлена на рис. 7.1. Цель такой структуризации – облегчение процесса администрирования.

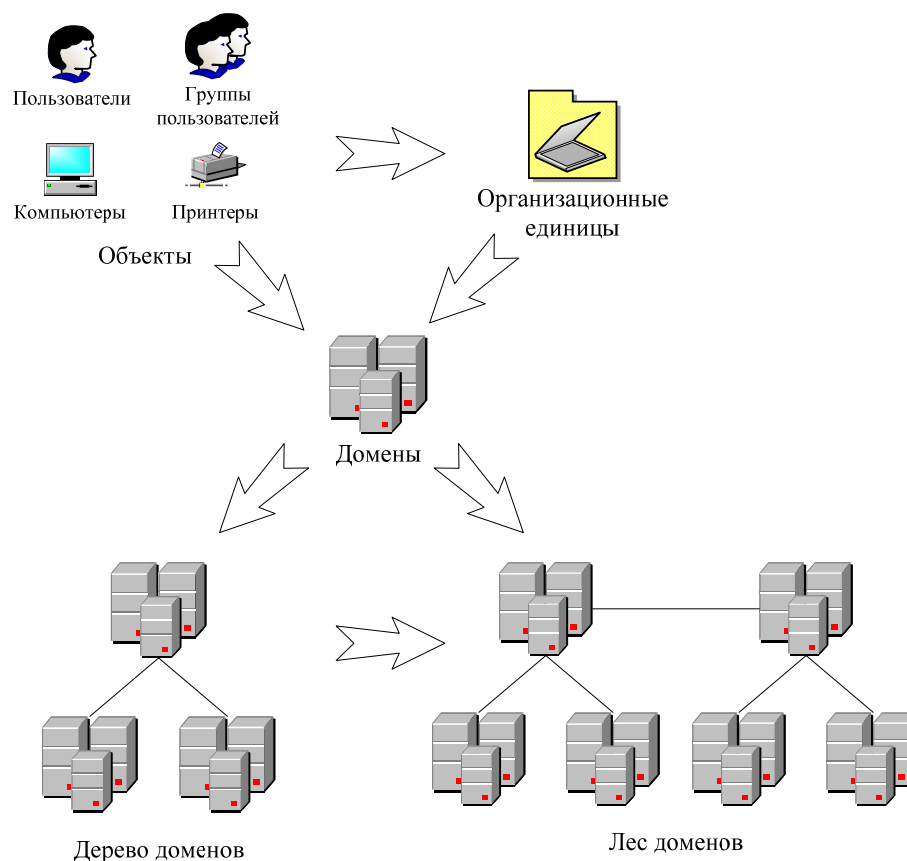


Рис. 7.1. Логическая структура Active Directory

Все сетевые объекты (пользователи, группы пользователей, компьютеры, принтеры) объединяются в домен, который является основной структурной единицей каталога. Для удобства управления объекты также могут быть сгруппированы при помощи *организационных подразделений (ОП)*. Несколько иерархически связанных доменов образуют *дерево доменов*. Совокупность деревьев, имеющих общие части каталога Active Directory и общих администраторов, называется *лесом доменов*. Более подробно эти понятия будут рассмотрены далее в этой лекции.

Имея возможность такой логической структуризации, администратор может подбирать конфигурацию сети в зависимости от своих задач и масштабов организации.

Основной целью *физической структуризации* каталога Active Directory является оптимизация процесса копирования изменений, произведенных на одном из контроллеров домена, на все остальные контроллеры. Этот процесс называется *репликацией (replication)*.

Основой физической структуры является *сайт (site)* – это часть сети, все контроллеры домена которой связаны высокоскоростным соединением. Между сайтами, наоборот, установлены более медленные линии связи (рис. 7.2).

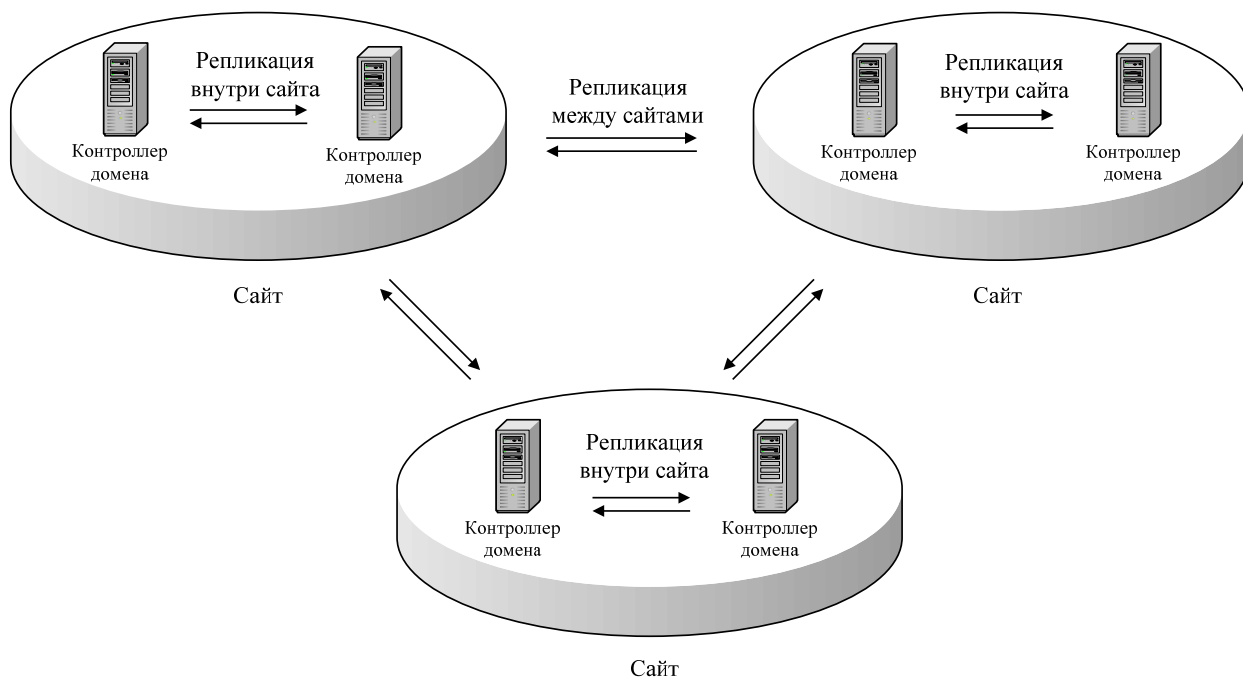


Рис. 7.2. Физическая структура Active Directory

Подобная структура позволяет планировать процесс репликации следующим образом: внутри сайта репликация осуществляется часто и могут передаваться большие объемы информации без сжатия; между сайтами изменения реплицируются редко и данные требуется сжимать.

Логическая и физическая структуры предназначены для решения разных задач и поэтому между собой практически не связаны: в одном домене может быть несколько сайтов, так же как один сайт может содержать несколько доменов. Общим объектом для той и другой структуры является контроллер домена с хранящимся на нем файлом каталога **Ntds.dit** (рис. 7.3).

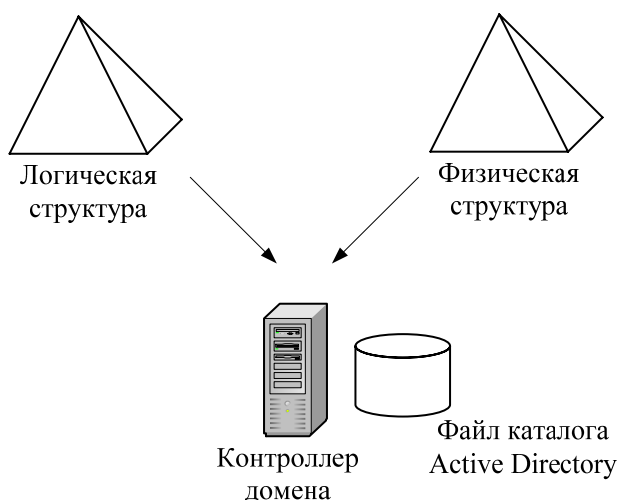


Рис. 7.3. Связь логической и физической структур

В файле каталога Active Directory содержится информация как о логической, так и о физической структурах. Этот файл состоит из нескольких разделов:

- раздел домена (domain partition) – содержатся данные обо всех объектах домена (пользователях, компьютерах, принтерах и т. д.);
- раздел схемы (schema partition) – хранится информация о типах всех объектов, которые могут быть созданы в данном лесе доменов;
- раздел конфигурации (configuration partition) – описывается конфигурация леса доменов – информация о сайтах, соединениях между сайтами и направлениях репликации;
- раздел приложений (application partition) – специальный раздел для хранения данных приложений, не относящихся к службе Active Directory. По умолчанию здесь создается подраздел для службы DNS;
- раздел глобального каталога (global catalog partition). *Глобальный каталог* – это база данных, в которой содержится список всех объектов леса доменов без информации об атрибутах этих объектов. Глобальный каталог необходим для поиска ресурсов леса из любого принадлежащего ему домена.

В зависимости от принадлежности к разделу информация реплицируется между контроллерами доменов следующим образом:

- раздел домена реплицируется между контроллерами одного домена;
- разделы схемы, конфигурации и глобального каталога реплицируются на все контроллеры леса;
- репликацией раздела приложений можно управлять – указывать, какие контроллеры будут получать реплику данного раздела.

Объекты каталога и их именование

Объект каталога Active Directory – это элемент, содержащийся в базе данных Active Directory и имеющий набор атрибутов (характеристик). Например, объектом является пользователь, а его атрибутами – имя, фамилия и адрес электронной почты.

Некоторые объекты являются контейнерами. Это означает, что данные объекты могут содержать в своем составе другие объекты. Например, объект *домен* является контейнером и может включать пользователей, компьютеры, другие домены и т. д.

Каталог Active Directory содержит следующие основные типы объектов, не являющихся контейнерами:

- пользователь (user);
- группы пользователей (group);
- контакты (contact);
- компьютеры (computer);
- принтеры (printer);
- общедоступные папки (shared folder).

В Active Directory для именования объектов используется несколько способов.

Различающееся имя (Distinguished Name, DN) – состоит из нескольких частей, например для пользователя **Петрова**, принадлежащего к организационному подразделению **Teachers** домена **faculty.ru**, различающееся имя выглядит так:

DC = ru, DC = faculty, OU = teachers, CN = users, CN = petrov.

При этом используются следующие сокращения:

- DC (Domain Component) – домен;
- OU (Organizational Unit) – организационное подразделение;
- CN (Common Name) – общее имя.

Различающиеся имена являются уникальными в пределах всего каталога Active Directory. В целях упрощения именования может использоваться *относительное различающееся имя* (Relative Distinguished Name, RDN). Для приведенного примера это имя **CN = petrov**. Имя RDN должно быть уникально в рамках объекта-контейнера, т.е. в пределах контейнера **CN = users** пользователь **petrov** должен быть единственным.

Основное имя пользователя (User Principal Name, UPN) – используется для входа пользователя в систему и состоит из двух частей: имени учетной записи пользователя и имени домена, к которому принадлежит пользователь. Например: **petrov@faculty.ru**.

Глобальный уникальный идентификатор (Global Unique Identifier, GUID) – это 128-битовое шестнадцатеричное число, которое ассоциируется с объектом в момент его создания и никогда не меняется. В случае перемещения или переименования объекта его GUID остается прежним.

Иерархия доменов

Домен является основным элементом в логической структуре Active Directory. В рамках домена действуют единые административные полномочия и политика безопасности, применяется общее пространство доменных имен.

Каждый домен имеет по крайней мере один контроллер домена, на котором хранится каталог Active Directory с информацией о домене.

Для организаций со сложной структурой может создаваться иерархия доменов. Первый образованный домен называется *корневым* (root domain). У него могут быть дочерние домены, имеющие общее пространство доменных имен. В свою очередь, у дочерних доменов могут быть свои домены-потомки. Таким образом, создается иерархия доменов, называемая *доменным деревом* (domain tree).

Если требуется в рамках одной организации организовать ещё одно пространство имен, то создается отдельное дерево доменов. При этом

несколько деревьев, входящих в состав одного каталога Active Directory, образуют *лес доменов* (forest).

Для именования доменов используются правила, принятые в системе доменных имен DNS. Вследствие этого доменная структура организации может при необходимости (и соблюдении требования уникальности имен) встраиваться в доменную структуру Интернета. Кроме того, для разрешения доменных имен становится возможным использование службы DNS.

На рис. 7.4 приведен фрагмент доменной структуры университета. В данном примере лес состоит из двух деревьев – дерева головной организации (домен **univ**) и дерева филиала-института (домен **institute**). Корневой домен головной организации имеет три дочерних домена – **rector** (ректорат), **math** (факультет математики), **physics** (факультет физики). Корневой домен института является родителем для двух доменов – **director** (руководство института) и **chemistry** (факультет химии).

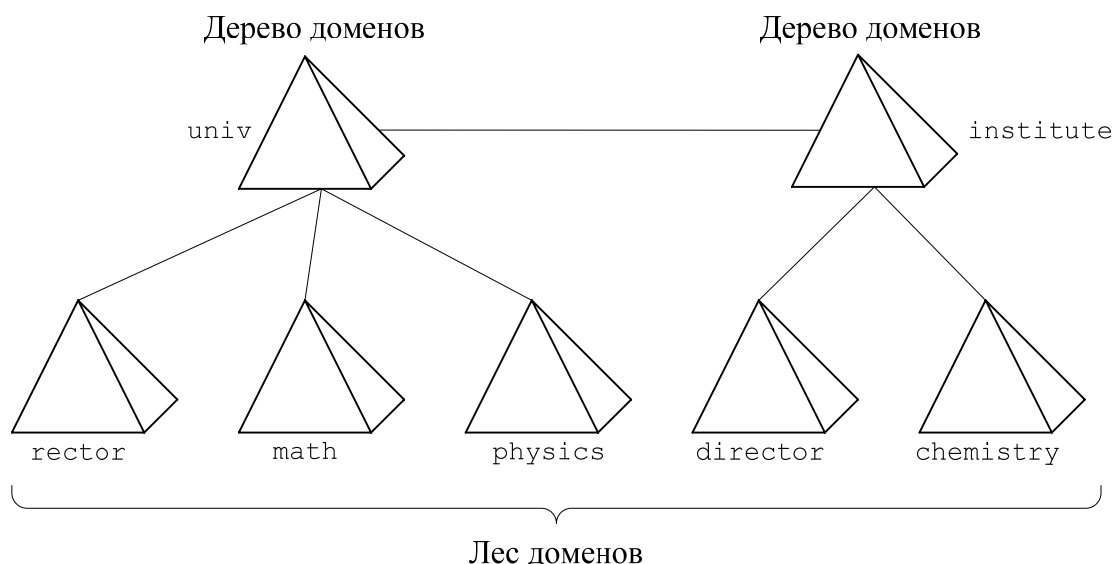


Рис. 7.4. Фрагмент возможной доменной структуры вуза

Следуя правилам DNS, полное имя (FQDN) домена **rector** будет иметь следующий вид: **rector.univ**, а полное имя домена **chemistry**: **chemistry.institute**.

Вопросы планирования доменной структуры рассмотрены в следующей лекции.

Доверительные отношения

Для доступа к ресурсам своего домена пользователю достаточно ввести имя своей учетной записи и пройти процедуры аутентификации и авторизации. *Аутентификация* (authentication) – это процесс проверки подлинности пользователя, т. е. подтверждение того, что пользователь является тем, за кого себя выдает. Аутентификация в Windows Server 2003

осуществляется путем предъявления системе пароля. В случае успешной аутентификации наступает этап *авторизации* (authorization) – это определение набора прав, которыми обладает пользователь.

При наличии необходимых прав (подробнее о правах доступа – в следующей лекции) пользователь может получить доступ к любому ресурсу домена. Однако для доступа к ресурсам другого домена между доменами должны быть установлены *доверительные отношения* (trust relationship).

Существует два вида доверительных отношений: *односторонние* (one-way trust relationship) и *двусторонние* (two-way trust relationship). Односторонние доверительные отношения означают, что пользователь одного домена (доверенного, trusted domain) получает доступ к ресурсам другого домена (доверяющего, trusting domain), но обратное неверно (рис. 7.5).

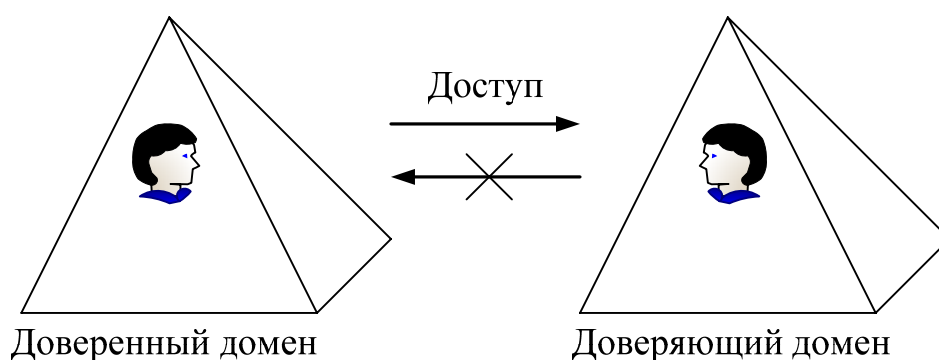


Рис. 7.5. Односторонние доверительные отношения

Иначе говоря, доверяющий домен делегирует право аутентификации пользователей доверенному домену.

Двусторонние доверительные отношения предполагают обоюдный процесс делегирования права аутентификации (рис. 7.6).

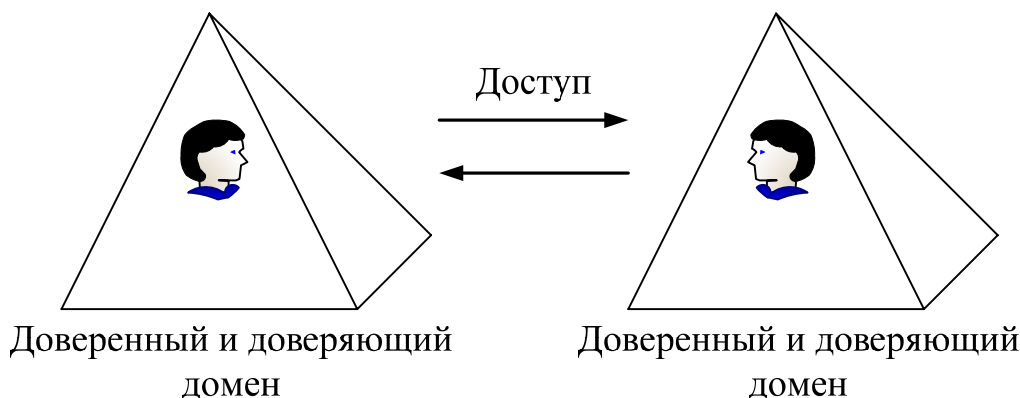


Рис. 7.6. Двусторонние доверительные отношения

При создании доменной структуры некоторые доверительные отношения устанавливаются автоматически, другие приходится настраивать вручную.

Перечислим автоматически устанавливаемые двусторонние доверительные отношения:

- внутри дерева доменов;
- между корневыми доменами деревьев одного леса;
- между деревьями одного леса (эти отношения являются следствием доверительных отношений между корневыми доменами деревьев).

В остальных случаях доверительные отношения следует устанавливать вручную (например, между лесами доменов или между лесом и внешним доменом, не принадлежащим этому лесу).

Организационные подразделения

Структурирование сетевых ресурсов организации при помощи доменов не всегда бывает оправданно, так как домен подразумевает достаточно крупную часть сети. Часто для администратора возникает необходимость группировки объектов внутри одного домена. В этом случае следует использовать *организационные подразделения* (organizational unit).

Организационные подразделения можно использовать в качестве контейнера для следующих объектов:

- пользователей;
- групп пользователей;
- контактов;
- компьютеров;
- принтеров;
- общих папок;
- других организационных подразделений.

Объекты группируются с помощью ОП для следующих целей¹:

- 1) управление несколькими объектами как одним целым – для этого используются групповые политики (см. следующую лекцию);
- 2) делегирование прав администрирования, – например начальнику отдела можно делегировать административные права на его отдел, при условии объединения всех объектов отдела в организационную единицу.

В качестве примера структуризации с использованием ОП можно привести возможную структуру домена факультета математики (см. рис. 7.7).

¹ Организационные подразделения не могут использоваться для назначения прав доступа к объектам. Для этих целей следует применять *группы безопасности* (security group).

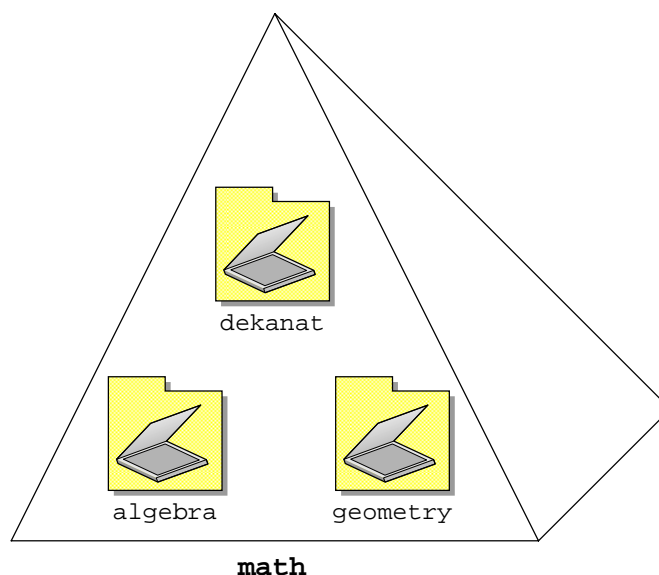


Рис. 7.7. Домен факультета математики

В данной ситуации выделение из домена **math** дочерних доменов не имеет смысла, так как факультет слишком мал. С другой стороны, требуется отразить в Active Directory внутреннюю структуру факультета. Решением является структуризация с применением организационных подразделений – в домене создаются ОП деканата и кафедр алгебры и геометрии. При этом для каждого подразделения администратор может назначить собственный набор правил (например, общие требования к паролям).

Резюме

В целях централизованного управления ресурсами сети в операционных системах Microsoft Windows Server 2003 существует служба каталога Active Directory.

Основой логической структуры каталога является домен – это группа компьютеров, имеющая общий каталог и единую политику безопасности. Несколько доменов могут быть объединены в дерево доменов, несколько деревьев составляют лес доменов. Для структуризации объектов внутри домена используются организационные подразделения.

Физическая структура основана на понятии сайта – это часть сети, все контроллеры домена которой связаны высокоскоростным соединением. Внутри сайта в процессе репликации (копирования изменений в структуре каталога на все контроллеры домена) информация не сжимается, а обмен осуществляется часто, между сайтами репликация происходит редко, а трафик репликации сжимается.

Информация как о логической, так и о физической структурах каталога хранится на контроллере домена в файле **Ntds.dit**.

Между доменами могут быть установлены доверительные отношения, чтобы пользователи одного домена могли получать доступ к ресурсам

другого домена. Доверительные отношения между всеми доменами леса устанавливаются автоматически. В других случаях их следует настраивать вручную.

Контрольные вопросы

1. Какая информация хранится в каталоге Active Directory? Где находится сам каталог?

2. Что такое домен?

3. Чем отличается контроллер домена от других узлов сети?

4. Какова цель логической структуризации каталог Active Directory?

5. По какому принципу следует осуществлять деление на сайты?

6. Для чего нужна репликация?

7. Сколько всего может быть создано глобальных идентификаторов

GUID?

8. Чем аутентификация отличается от авторизации?

9. Объясните понятия «доверенный» и «доверяющий» домен. В каком случае один домен может быть доверенным и доверяющим одновременно?

10. Для чего используют организационные подразделения?

Лекция 8. Планирование и управление Active Directory

План лекции

- Планирование Active Directory.
- Планирование логической структуры.
- Планирование физической структуры.
- Учетные записи.
- Группы пользователей.
- Групповые политики.
- Резюме.
- Контрольные вопросы.

Планирование Active Directory

Рассмотренная в предыдущей лекции служба каталога Active Directory играет центральную роль при выполнении задач сетевого администрирования. Успешная работа пользователей сетевых ресурсов, а также служб, реализующих протоколы TCP/IP, зависит от правильного функционирования Active Directory. Поэтому крайне важной становится задача планирования структуры каталога Active Directory. Удачно спроектированный каталог позволит сделать работу сети более эффективной и стабильной, а также намного облегчит труд администратора.

В процессе планирования Active Directory можно выделить два основных этапа (рис. 8.1):

- 1) планирование логической структуры, включающее проектирование доменов и организационных подразделений, а также проблему именования;
- 2) планирование физической структуры, состоящее из разделения сети на сайты и размещения контроллеров домена.

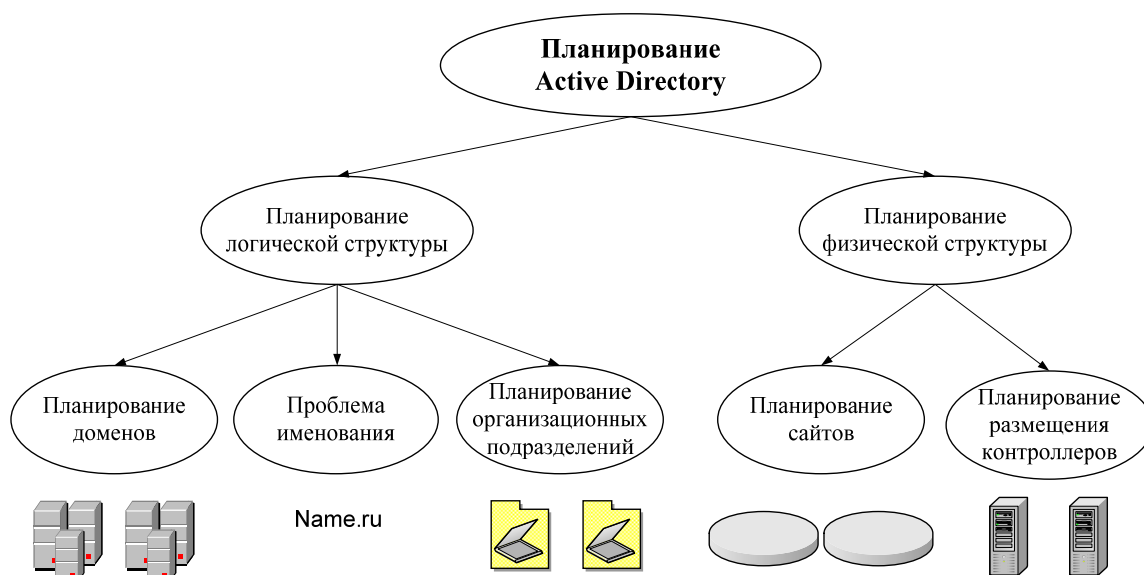


Рис. 8.1. Планирование Active Directory

Планирование логической структуры

При *планировании доменной структуры* нужно определить количество и способ организации доменов. Возможны три варианта: единственный домен, дерево доменов или лес. Критерии выбора следующие.

1. Размер организации – один домен может содержать несколько миллионов пользователей, рекомендуется не превышать 1–2 миллиона, однако организаций с таким количеством пользователей немного, поэтому данный критерий применяется нечасто.

2. Географическое расположение – имеются ли у организации филиалы или отделы, находящиеся на большом расстоянии и связанные с центральным офисом низкоскоростными каналами связи. Наличие таких филиалов при единственном в организации домене, скорее всего, вызовет перегрузку линий связи из-за трафика репликации.

3. Стабильность предприятия – насколько высока подвижность кадрового состава, не планируется ли в ближайшее время разделение предприятия или присоединения новых структур.

4. Потребности в разных доменных именах – в некоторых случаях в рамках одной организации требуются разные доменные имена. Например, в случае создания единой компьютерной сети двух университетов каждый из них, вероятно, захочет иметь свое собственное доменное имя.

5. Способ управления сетью – может быть централизованным и децентрализованным. Централизованный способ предполагает сосредоточение всей административной власти у единого коллектива администраторов и наличие однодоменной модели. При децентрализованном способе полномочия делегируются нескольким слабосвязанным удаленным группам администраторов, управляющих доменами дерева или леса.

6. Единство политики безопасности. Чаще всего политика безопасности в одной организации едина для всех отделов и сотрудников, однако бывают исключения, например, для отдельных цехов завода, работающих на нужды армии.

Исходя из перечисленных критериев, можно выделить те признаки, по которым выбирается вариант с одним доменом:

- 1) в организации менее миллиона пользователей;
- 2) отсутствие удаленных филиалов;
- 3) относительная стабильность структуры организации;
- 4) отсутствие потребности в разных доменных именах;
- 5) централизованный способ администрирования;
- 6) единая политика безопасности.

Отсутствие первых четырех признаков существенно склоняет выбор в пользу многодоменной модели. Последние два признака в меньшей степени должны влиять на выбор, так как задачи делегирования администрирования и разделения политик безопасности можно решить средствами организационных подразделений в рамках одного домена.

При выборе модели с несколькими доменами в большинстве ситуаций нужно использовать дерево доменов. Лес доменов приемлем в том случае, когда две независимые организации хотят иметь общие сетевые ресурсы.

После выбора доменной структуры следует продумать *имена для создаваемых доменов*. Особенно важно имя корневого домена. Хотя Windows Server 2003 позволяет переименовывать домены (при условии, что в домене нет контроллеров с Windows Server 2000 и Windows NT), делать это нежелательно: выбранное доменное имя уже может быть прочно ассоциировано с организацией.

Правил для выбора доменного имени немного: во-первых, оно должно отражать специфику организации, во-вторых, быть понятным всем пользователям ресурсов домена, а не только администратору и, в-третьих, не должно быть слишком сложным. Например, для обозначения домена университета необязательно называть его **vyatka_state_humanitarian_university** (хотя это имя отражает специфику организации и является понятным для пользователей, оно слишком сложное). Для имени такого домена достаточно обозначения **vshu**.

Планирование структуры организационных подразделений в каждом домене является важным шагом. От этой структуры зависит эффективность решения ежедневных административных задач, оптимальность управления объектами сети.

Как отмечалось в предыдущей лекции, ОП применяются в том случае, если для задач управления группой объектов или делегирования административных прав образование новых доменов нецелесообразно.

В связи с тем, что организационные подразделения можно использовать в качестве контейнеров, допускается строить иерархию ОП с несколькими уровнями вложений.

Иерархию можно строить с помощью двух основных подходов: либо следуя организационной структуре предприятия (*организационный подход*); либо исходя из задач управления сетевыми объектами (*административный подход*). Оба способа используются на практике, и задача администратора состоит в том, чтобы выяснить, какой из подходов (или их комбинация) применим в данной ситуации.

Иллюстрацией обоих подходов может служить следующий пример. На предприятии имеются три отдела – безопасности, маркетинга и планирования. Требуется спроектировать для данных отделов структуру организационных подразделений (рис. 8.2).

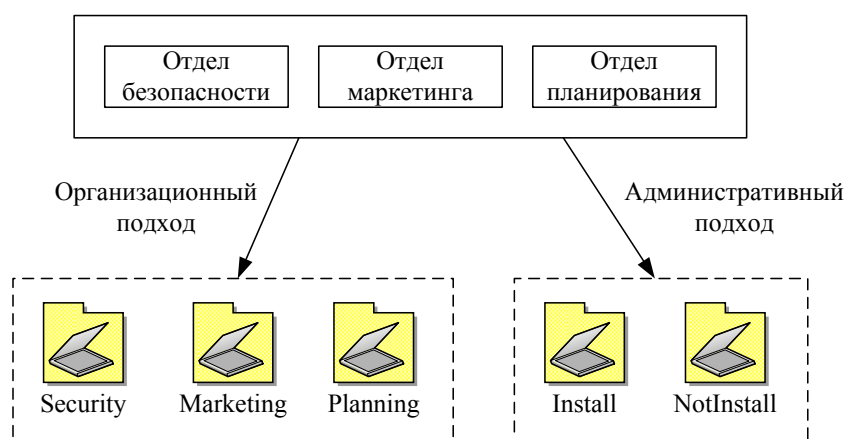


Рис. 8.2. Организационный и административный подходы к планированию структуры ОП

Применяя организационный подход, следует в структуре ОП отразить структуру предприятия. Таким образом, отделы представляются как организационные подразделения **Security**, **Marketing** и **Planning**. Административный подход во главу угла ставит задачи управления. Допустим, сотрудники отдела безопасности регулярно устанавливают на компьютеры новые приложения, а отделам маркетинга и планирования установка программ должна быть запрещена. Из этих соображений можно отдел безопасности поместить в ОП **Install** с правом установки программ, а отделы маркетинга и планирования объединить в ОП **NotInstall**.

Планирование физической структуры

Основная цель планирования физической структуры – оптимизация трафика репликации. Цель достигается путем продуманного расположения сайтов и контроллеров домена.

В принципе та же задача может быть решена с помощью изменения доменной структуры, так как основной объем данных репликации остается в рамках одного домена, междоменный трафик репликации существенно ниже внутридоменного. Однако рекомендуется при планировании иерархии

доменов применять критерии, описанные выше, а для оптимизации процесса репликации использовать механизм сайтов.

На начальном этапе следует проанализировать существующую сеть – её структуру, количество пользователей и компьютеров, пропускную способность, колебания трафика. Все эти данные нужно учитывать при планировании. Чем больше пользователей и компьютеров в сети, тем больше объем передаваемой информации при репликации. Линии с большой пропускной способностью могут быть сильно загружены, и большой трафик репликации внесет существенные проблемы, в то время как низкоскоростные каналы, возможно, практически свободны и выдержат дополнительный объем данных репликации.

Во время анализа следует учитывать возможность расширения сети и увеличения числа пользователей. Считается достаточным принимать коэффициент расширения в пределах 30–50 %.

Основной критерий при выделении сайтов – пропускная способность линий связи. Части домена, связанные высокоскоростными линиями, помещаются в один сайт. Если между частями домена имеются каналы с низкой скоростью передачи данных, их следует разместить в разных сайтах. При этом трафик межсайтовой репликации сжимается и его передача происходит во время наименьшей загрузки низкоскоростных линий.

Вопрос о необходимом количестве и размещении контроллеров домена решается тогда, когда известна доменная структура и расположение сайтов. Общее правило таково, что для каждого домена необходимо не менее двух контроллеров (при этом в случае отказа одного из контроллеров второй обеспечит работу сети). Количество контроллеров зависит от числа пользователей (а следовательно, числа обращений на контроллеры домена), принадлежащих данному домену или сайту. Например, если домен включает два сайта, связанных модемной линией, и к одному из сайтов принадлежит всего несколько пользователей, то совсем не обязательно в этом сайте располагать отдельный контроллер домена (при условии, что загрузка модемной линии невысока).

Учетные записи

После реализации спроектированной структуры Active Directory администратор должен добавить в каталог учетные записи всех пользователей системы и назначить каждой из них определенные права. *Учетная запись пользователя* – это набор атрибутов, сопоставленных с определенным пользователем. Самые важные атрибуты следующие:

- имя учетной записи, с помощью которого пользователь осуществляет вход в систему (в пределах домена должно быть уникально);
- полное имя пользователя;
- пароль;
- группы, в которые входит пользователь;

– права пользователя.

Создав все необходимые учетные записи, администратору следует продумать, какими правами должен обладать тот или иной пользователь. *Права пользователя* – это список действий, которые может выполнять пользователь. Права бывают следующих видов:

- *привилегия* (privilege) – право выполнения операций по изменению состояния или параметров системы (например, выключение компьютера или изменение системного времени);
- *право на вход в систему* (logon right);
- *разрешение доступа* (access permission) – право осуществления действий с файлами, папками, принтерами, объектами Active Directory, реестром (при условии, что используется файловая система NTFS).

Более подробно виды прав пользователя описаны в Приложении III.

При условии, что пользователей порядка десяти человек, определить необходимые права можно достаточно просто. Однако гораздо чаще на практике встречаются сети с сотнями и тысячами учетных записей. В таких масштабах задача распределения прав отдельным пользователям становится невыполнимой. В этом случае на помощь администратору приходит механизм групп пользователей.

Группы пользователей

Группа пользователей (группа безопасности, Security Group) – это объединение учетных записей пользователей, которому можно назначать права¹. С использованием групп распределение прав осуществляется следующим образом. Сначала выбираются такие пользователи, список прав которых должен быть одинаковым. Затем создается группа, членами которой являются выбранные пользователи. Требуемые права назначаются уже не отдельным пользователям, а группе, и эти права автоматически распространяются на всех пользователей группы.

Следует отметить, что группы пользователей и организационные подразделения представляют собой разные механизмы, предназначенные для разных целей. Создание групп безопасности преследует цель распределения прав доступа к ресурсам пользователям сети, в то время как основное назначение организационных подразделений – управление пользователями (а также компьютерами) (см. рис. 8.3).

¹ Это определение самого распространенного вида групп пользователей – *групп безопасности* (security groups). Кроме таких групп существуют ещё *группы рассылки* (distributed group), которые применяются для массовой передачи сообщений электронной почты. Следует отметить, что группу безопасности также можно использовать в качестве адреса электронной почты – сообщение придет всем членам группы.

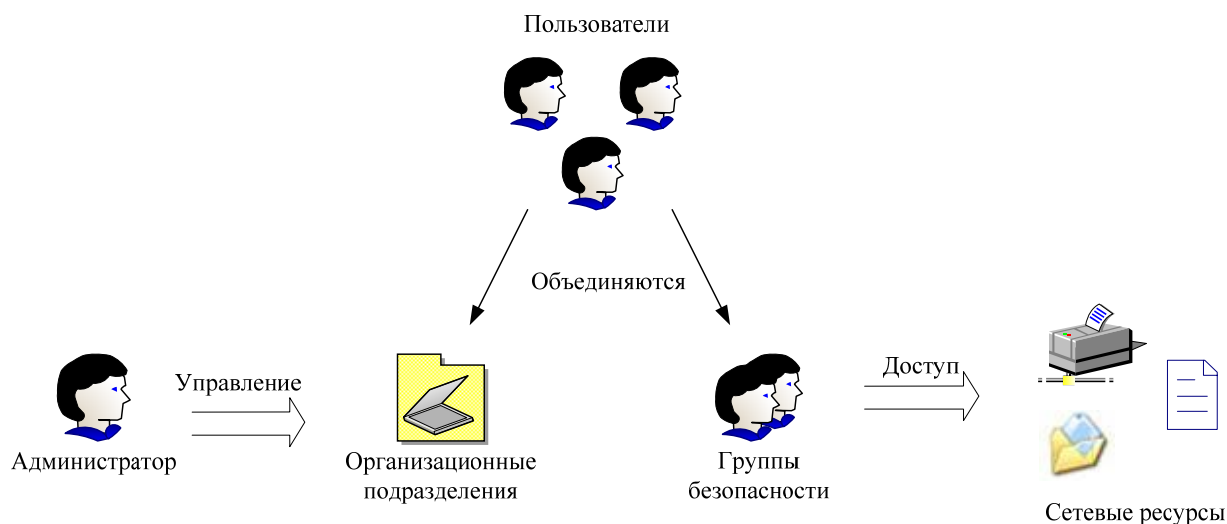


Рис. 8.3. Использование ОП и групп безопасности

Группы пользователей различаются по области действия. Выделяют три области действия:

- *доменную локальную* (domain local scope);
- *глобальную* (global scope);
- *универсальную* (universal scope).

Доменные локальные группы действуют в рамках только своего домена. За его пределами указывать локальную доменную группу нельзя. Такие группы обычно применяются для управления доступом к файлам, общим папкам и принтерам.

Глобальные группы могут использоваться в рамках всего леса доменов. Однако глобальная группа принадлежит определенному домену, и в её состав могут входить только объекты этого домена. Применяются глобальные группы в том случае, если пользователям одного домена нужно получить доступ к ресурсам другого домена.

Универсальные группы привязаны к корневому домену леса, но в их состав могут входить пользователи любого домена. Чаще всего универсальные группы используются для объединения глобальных групп.

Групповые политики

В заключение лекции рассмотрим один из наиболее эффективных и удобных инструментов администрирования – групповые политики.

*Групповые политики*¹ (group policy) – это способ автоматизации работы по настройке рабочих столов пользователей и параметров компьютеров. Групповые политики представляют собой наборы правил конфигурирования,

¹ Следует отметить один терминологический нюанс. Термин «групповые» не означает, что политики имеют отношение к группам безопасности. Групповые политики связаны с группами компьютеров и пользователей, объединенных в рамках сайтов, доменов и ОП.

применяемых к компьютеру или пользователю. Каждый такой набор правил называется *объектом групповой политики* (Group Policy Object, GPO).

Один или несколько объектов групповой политики могут применяться к трем видам объединений:

- сайтам;
- доменам;
- организационным подразделениям.

Кроме того, для каждого компьютера может быть определен *объект локальной групповой политики* (Local Group Policy Object, LGPO).

Объекты групповых политик являются наследуемыми. Это означает, например, что GPO, применяемый к домену, наследуется всеми его организационными подразделениями. В том случае, если правила одного объекта групповой политики конфликтуют с правилами другого, наибольший приоритет имеет GPO организационного подразделения, ниже по уровню GPO домена, затем следует GPO сайта, наименьший приоритет у LGPO.

Приведем краткий обзор возможностей, предоставляемых групповыми политиками (рис. 8.4).

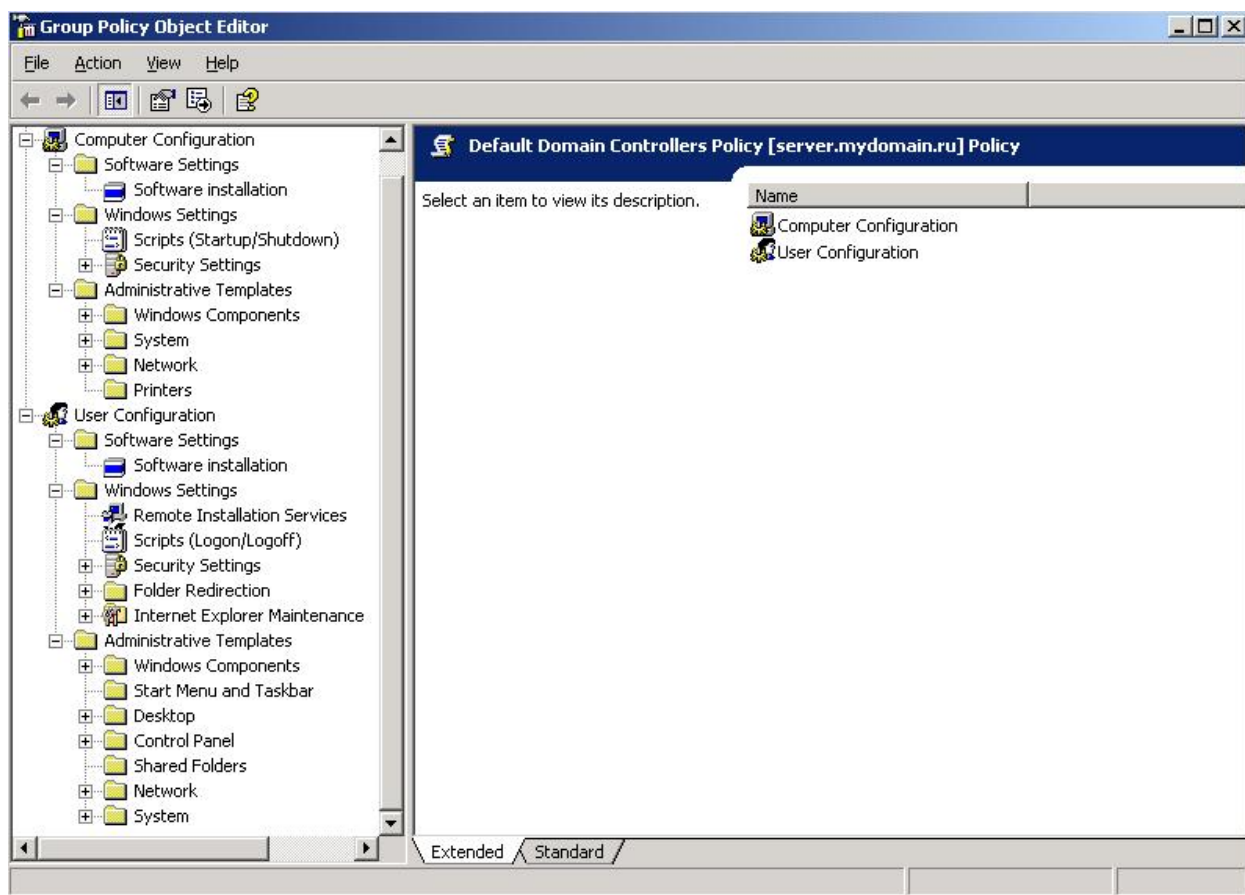


Рис. 8.4. Пример объекта групповой политики

Объект групповой политики содержит две основные части:

- **Конфигурация компьютера (Computer Configuration);**
- **Конфигурация пользователя (User Configuration).**

Каждая из частей включает три раздела:

- **Настройки приложений (Software Settings);**
- **Настройки Windows (Windows Settings);**
- **Административные шаблоны (Administrative Templates).**

В разделе **Настройки приложений** находится подраздел **Установка приложений (Software Installation)**, позволяющий автоматически устанавливать выбранные программы на компьютеры пользователей.

Правила, создаваемые в разделе **Настройки Windows**, позволяют:

- выполнять задаваемые сценарии (**Scripts**) при включении-выключении компьютера, при входе пользователя в систему и выходе из неё;
- настраивать параметры безопасности (**Security Settings**) компьютера и пользователя (требования к паролям, доступ к реестру, политику аудита событий);
- конфигурировать Internet Explorer (**Internet Explorer Maintenance**);
- изменять места расположения папок пользователей (**Folder Redirection**).

Раздел **Административные шаблоны** предназначен для настройки рабочего стола пользователя, ограничения доступа к системным компонентам и компонентам приложений.

Таким образом, Windows Server 2003 предоставляет мощный набор инструментов администрирования, способствующий эффективному управлению сети любой организации.

Резюме

При развертывании службы каталога Active Directory на первый план выходит задача планирования его структуры, от успешности решения которой зависит эффективность и стабильность работы сети. В процессе проектирования выделяют два этапа – планирование логической структуры и планирование физической структуры.

В ходе планирования логической структуры следует определиться с количеством доменов и способом их организации – одиночный домен, доменное дерево или лес. Затем нужно выбрать имена для созданных доменов и построить иерархию организационных подразделений.

Основной целью планирования физической структуры является оптимизации трафика репликации. На этом этапе в сети выделяют сайты и определяют количество и размещение контроллеров домена.

После проектирования и реализации структуры каталога должны быть созданы учетные записи пользователей и определены их привилегии. Задача управления пользователями решается при помощи групп безопасности организационных подразделений и групповых политик. Группы безопасности служат для объединения тех пользователей, которые имеют одинаковые разрешения доступа к ресурсам сети. Организационные подразделения создаются для удобства управления пользователями. Управление осуществляется с использованием групповых политик,

включающих множество настроек, облегчающих процесс администрирования.

Контрольные вопросы

1. В чем цель планирования логической структуры каталога?
2. В чем цель планирования физической структуры каталога?
3. Назовите признаки, по которым следует осуществлять выбор многодоменной модели?
4. Какой подход предпочтительнее при проектировании структуры организационных подразделений: организационный или административный?
5. Каким образом деление на сайты влияет на процесс репликации?
6. Как выбираются число и расположение контроллеров домена?
7. Чем отличаются организационные подразделения и группы безопасности?
8. Назовите основные элементы объектов групповых политик.

Лекция 9. Средства обеспечения безопасности

План лекции

- Средства сетевой безопасности Windows Server 2003.
- Протокол аутентификации Kerberos.
- Термины, используемые в протоколе Kerberos.
- Основные этапы аутентификации.
- Этап регистрации клиента.
- Этап получения сеансового билета.
- Этап доступа к серверу.
- Протокол IPsec.
- Функции протокола IPsec.
- Протоколы AH и ESP.
- Протокол IKE.
- Резюме.
- Контрольные вопросы.

Средства сетевой безопасности Windows Server 2003

Для обеспечения безопасности сетевого соединения в целом требуется обеспечить безопасность двух важнейших процессов:

- процесса аутентификации при установке соединения;
- процесса передачи данных.

Основной метод аутентификации в Windows Server 2003 – это протокол Kerberos v5. Также поддерживается протокол NTLM (NT LAN Manager), который был основным в операционной системе Windows NT и остался в Windows Server 2003 для совместимости со старыми версиями. В лекции будет подробно рассмотрен протокол Kerberos v5.

Для защищенной передачи сообщений наиболее надежным и перспективным считается протокол IPsec. В нем используется криптостойкое шифрование, а также собственные методы аутентификации и проверки целостности передаваемых данных. Этот протокол рассматривается во второй части лекции.

Протокол аутентификации Kerberos

Протокол аутентификации Kerberos разработан в начале 80-х годов в Массачусетском технологическом институте (Massachusetts Institute of Technology, MIT). Описан в RFC 1510. По-русски Kerberos – это Цербер, трехглавый пес, охраняющий вход в царство мертвых в древнегреческой мифологии.

В Windows Server 2003 используется модифицированная пятая версия протокола – Kerberos v5. Для шифрования применяется алгоритм DES (Data Encryption Standard – стандарт шифрования данных). Протокол обеспечивает аутентификацию в открытых сетях, т. е. там, где передаваемые пакеты могут быть перехвачены и изменены. Преимуществом протокола Kerberos по сравнению с протоколом NTLM является то, что в процессе аутентификации сервер не только удостоверяет подлинность клиента, но и по требованию клиента подтверждает свою достоверность. Ещё одно преимущество – время аутентификации при использовании Kerberos меньше, чем в случае применения NTLM.

Термины, используемые в протоколе Kerberos

Рассмотрим основные термины, используемые при описании протокола Kerberos.

Понятия *аутентификации* и *авторизации* рассматривались в лекции 7, в разделе «Доверительные отношения».

Шифрование (encryption) – процесс преобразования данных в такую форму, которая не может быть прочитана без процесса расшифрования. Шифрование осуществляется с применением *шифрующего ключа (encryption key)*, расшифрование использует *расшифровывающий ключ (decryption key)*.

В симметричных методах шифрования, к которым относится алгоритм DES, шифрующий и расшифровывающий ключи совпадают и такой единый ключ называется *секретным ключом (secret key)*. Секретный ключ пользователя получается путем хеширования его пароля.

Хеширование (hashing) обозначает такое преобразование исходной последовательности данных, результат которого – *хеш (hash)*, в отличие от результата шифрования, не может быть преобразован обратно в исходную последовательность. Это преобразование может осуществляться с помощью некоторого ключа. Хеширование часто применяют для проверки знания участниками соединения общего секретного ключа. При этом источник вычисляет хеш некоторого блока данных с использованием секретного ключа и отправляет эти данные совместно с хешем. Приемник также вычисляет хеш блока данных, и при условии совпадения ключей значения хешей должны быть равны.

Сеанс (session) – это период непрерывного соединения между двумя узлами (например, клиентом и сервером). В начале сеанса требуется пройти процедуру аутентификации. Соединение в течение сеанса осуществляется с использованием сеансового ключа.

Сеансовый ключ (session key) – секретный ключ, служащий для шифрования всех сообщений между участниками сеанса. Очевидно, должен быть известен всем участникам сеанса.

В протоколе Kerberos существует три основных участника сеансов – клиент, сервер и посредник.

Клиент – компьютер (пользователь, программа), желающий получить доступ к ресурсам сервера. Предварительно клиент должен пройти процедуры аутентификации и авторизации, используя свое удостоверение.

Сервер – компьютер (программа), предоставляющий ресурсы авторизованным клиентам.

Посредник – это специальный физически защищенный сервер, на котором работают две службы¹ – *центр распространения ключей* (Key Distribution Center, KDC) и *служба предоставления билетов* (Ticket Granting Service, TGS). В сетях Active Directory этим сервером является контроллер домена.

Центр распространения ключей KDC хранит секретные ключи всех клиентов и серверов и по запросу аутентифицированного клиента выдает ему удостоверение.

Служба предоставления билетов TGS выдает сеансовые билеты, позволяющие пользователям проверять подлинность серверов.

Удостоверения (credentials) – специальные сетевые пакеты, используемые для взаимной идентификации клиента и сервера. Удостоверения бывают двух видов: *билеты (tickets)* и *аутентификаторы (authenticators)*.

Билет (ticket) – специальный пакет, удостоверяющий подлинность своего владельца. В состав билета входят имя владельца, сеансовый ключ и другие параметры. Период действия билета ограничен параметром, который называется *время жизни (lifetime)*. По умолчанию время жизни равно 5 минутам.

Существует два типа билетов: *билеты TGT (Ticket-Granting Ticket – билеты на выдачу билетов)* и *сеансовые билеты (session ticket)*.

Билет TGT содержит учетные данные, выдаваемые пользователю центром распределения ключей KDC при входе пользователя в систему.

Сеансовый билет требуется для установления сеанса соединения клиента с сервером.

Аутентификатор (authenticator) – это пакет, доказывающий, что клиент действительно является обладателем секретного ключа.

Приведенные выше термины сведены в схему на рис. 9.1.

¹ Каждая служба может работать на отдельном компьютере, но на практике обе службы функционируют на одном сервере.

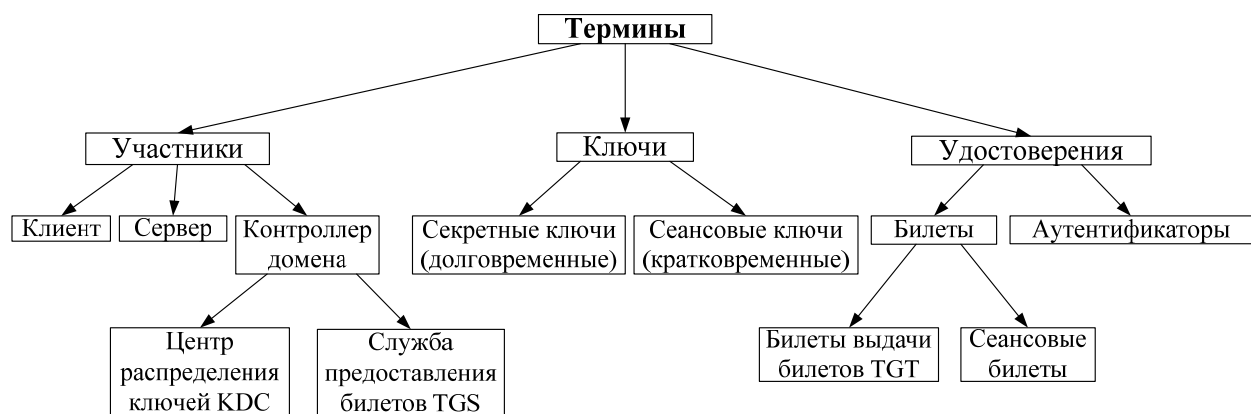


Рис. 9.1. Термины, используемые при описании протокола Kerberos

Для дальнейшего изложения введем обозначения, представленные в таблице.

Обозначение	Комментарий
A_C	Аутентификатор клиента
A_S	Аутентификатор сервера
K_C	Секретный ключ клиента
K_S	Секретный ключ сервера
$\{X\}K$	Сообщение X, зашифрованное ключом K
$\{A_C\}K_C$	Аутентификатор клиента, зашифрованный секретным ключом клиента
$K_{A,B}$	Сеансовый ключ для соединения узлов A и B
$K_{C,TGS}$	Сеансовый ключ для соединения клиента и службы TGS
TGT	Билет TGT
$T_{C,S}$	Сеансовый билет для соединения клиента и сервера
N	Имя клиента
S	Имя сервера
t	Момент времени отправки сообщения

Основные этапы аутентификации

Клиенту для получения доступа к ресурсам сервера предварительно требуется пройти проверку подлинности, т. е. аутентифицироваться. Процедура аутентификации состоит из трех основных этапов (рис. 9.2):

- 1) регистрация клиента;
- 2) получение сеансового билета;
- 3) доступ к серверу.



Рис. 9.2. Этапы получения клиентом доступа к ресурсам сервера

Рассмотрим эти этапы подробнее.

Этап регистрации клиента

При входе в систему под управлением Windows Server 2003 пользователь вводит имя своей учетной записи, пароль и указывает домен. Пароль при помощи хеширования преобразуется в секретный ключ клиента K_C . Точно такой же ключ хранится в центре распределения ключей KDC и сопоставлен с данным пользователем. Клиент создает аутентификатор $\{A_C\}_{K_C}$, зашифрованный с использованием ключа K_C , и отправляет его центру распределения ключей (рис. 9.3). Аутентификатор содержит информацию об имени клиента N и время отправки аутентификатора t .

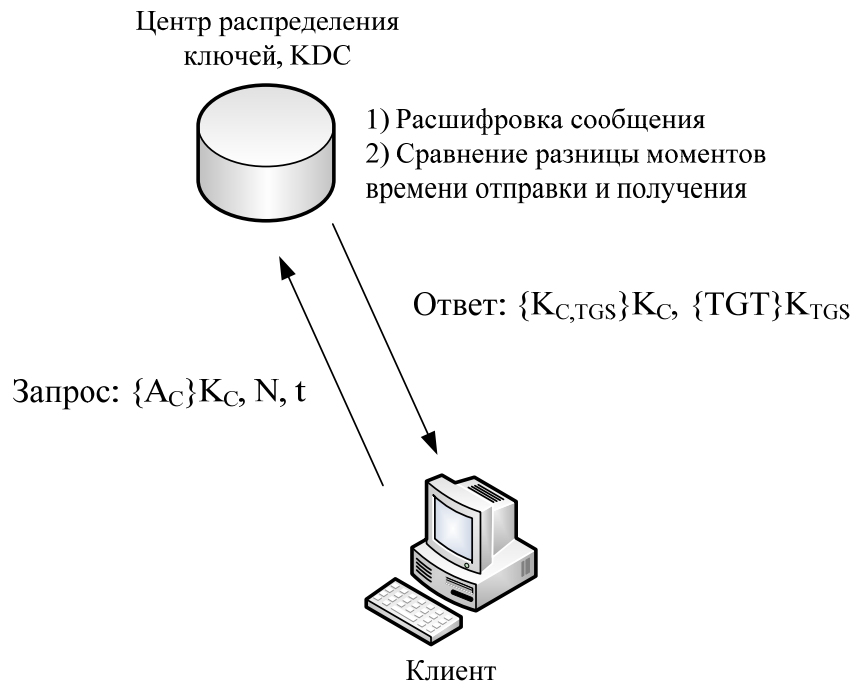


Рис. 9.3. Этап регистрации клиента

Используя свою копию ключа K_C , центр распределения ключей пытается расшифровать полученное сообщение. В случае успеха вычисляется разница между временем создания аутентификатора и временем его получения. Если разница не превышает пяти минут¹, то клиент считается аутентифицированным и ему высылается следующая информация:

- $\{K_{C,TGS}\}K_C$ – сеансовый ключ $K_{C,TGS}$ для связи клиента и службы TGS, зашифрованный ключом K_C ;
- $\{TGT\}K_{TGS}$ – билет на выдачу билетов TGT, зашифрованный ключом K_{TGS} , известным только службе TGS.

Сеансовый ключ $K_{C,TGS}$ клиент в состоянии расшифровать, используя свой ключ K_C , а расшифровка билета TGT клиентом невозможна, так как ключ K_{TGS} ему неизвестен. Билет TGT в зашифрованном виде сохраняется в кэш-память клиента и при необходимости извлекается оттуда.

В дальнейшем клиент будет использовать полученную информацию для запроса полномочий у службы TGS на доступ к конкретному серверу.

В том случае, если аутентификатор не удалось расшифровать или разница по времени превышает пять минут, клиент считается не прошедшим аутентификацию.

¹ Проверка разницы моментов времени осуществляется в целях защиты от перехвата аутентификатора и его несанкционированного использования. Так как аутентификаторы, генерируемые клиентом, не повторяются (для их создания применяется значение текущего момента времени), то перехваченный идентификатор может быть использован только в течение пяти минут. Однако центр распределения ключей ведет учет всех аутентификаторов, полученных за последние пять минут, и в случае совпадения аутентификатор отклоняется.

Отметим, что для правильного функционирования протокола Kerberos часы всех участников соединения должны быть синхронизированы с точностью до минут.

Этап получения сеансового билета

Когда клиенту требуется получить доступ к ресурсам некоторого сервера, он обращается к службе предоставления билетов TGS с запросом о выдаче сеансового билета для соединения с данным сервером. В запрос включается следующая информация (рис 9.4):

- $\{A_C\}K_{C,TGS}$ – аутентификатор клиента A_C , зашифрованный с помощью ключа $K_{C,TGS}$;
- $\{TGT\}K_{TGS}$ – билет на выдачу билетов TGT, зашифрованный ключом K_{TGS} ;
- S – информация о сервере, с которым требуется установить соединение;
- t – время отправки запроса.

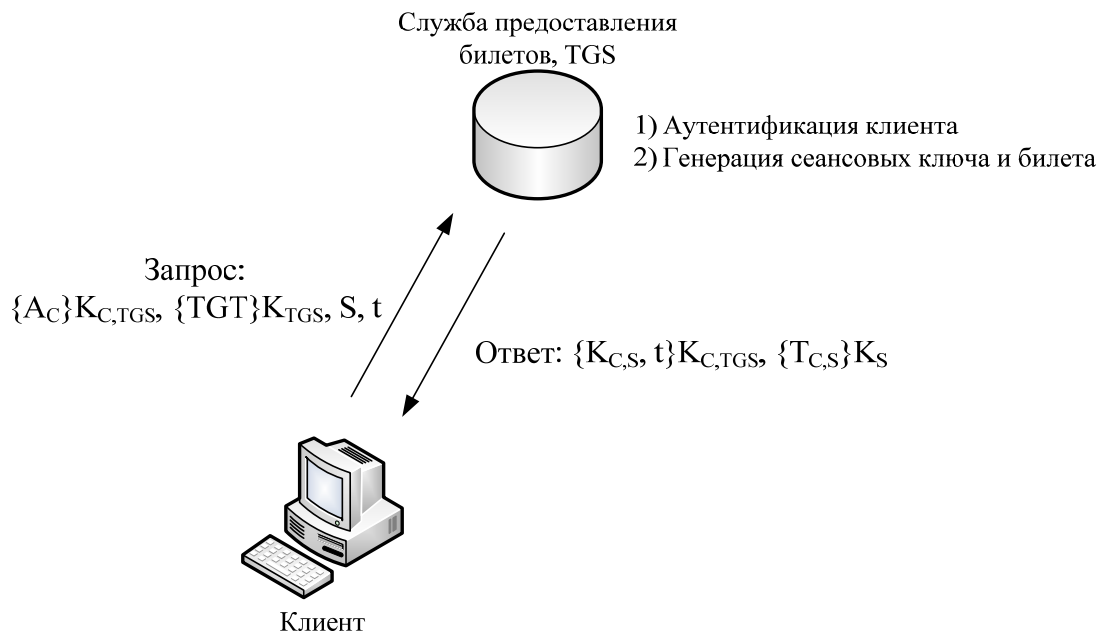


Рис. 9.4. Этап получения сеансового билета

Аутентификатор клиента позволяет службе TGS удостовериться, что клиент является тем, за кого себя выдает. Использование билетов TGT экономит время: служба предоставления ключей TGS не обращается к базе данных центра распределения ключей KDC.

На запрос клиента служба TGS в случае успешной аутентификации отвечает следующей информацией:

- $\{K_{C,S}, t\} K_{C,TGS}$ – сеансовый ключ $K_{C,S}$ для связи клиента с сервером, а также время создания ключа; оба параметра зашифрованы ключом $K_{C,TGS}$;
- $\{T_{C,S}\}K_S$ – сеансовый билет $T_{C,S}$, зашифрованный при помощи ключа K_S , известного только службе TGS и серверу. Сеансовый билет предназначен только серверу, клиент не в состоянии его прочитать.

Сеансовый ключ $K_{C,S}$ генерируется случайным образом, поэтому при каждом новом запросе (даже для связи с одним и тем же сервером) клиент будет получать новые сеансовые ключи. Клиент может расшифровать сеансовый ключ, так как он зашифрован ключом $K_{C,TGS}$, известным клиенту.

Сеансовый билет $T_{C,S}$ содержит следующие данные:

- имя сервера;
- имя клиента;
- сеансовый ключ;
- время начала действия билета;
- время окончания действия билета;
- список возможных сетевых адресов клиента.

Последний элемент является необязательным и применяется для дополнительной защиты – в этом случае клиенты не могут соединяться с сервером с адресов, не перечисленных в списке.

Сеансовые билеты, полученные клиентом для разных серверов, сохраняются в кэш-памяти. Таким образом, если клиенту требуется получить доступ к какому-либо серверу, сначала осуществляется поиск в кэш-памяти сеансовых билетов для этого сервера. При отсутствии таковых клиент извлекает билет TGT из кэш-памяти и обращается с запросом к службе TGS.

Этап доступа к серверу

Получив сеансовый билет $T_{C,S}$ и сеансовый ключ $K_{C,S}$, клиент может проходить процедуру аутентификации на требуемом сервере и в случае успешного прохождения начинать обмен данными. Запрос на аутентификацию включает следующие параметры (рис. 9.5):

- $\{A_C\}K_{C,S}$ – аутентификатор A_C , зашифрованный ключом $K_{C,S}$. Содержит информацию об имени клиента, времени отправления, а также ключ $K_{C,S}$;
- $\{T_{C,S}\}K_S$ – сеансовый билет, зашифрованный ключом K_S .

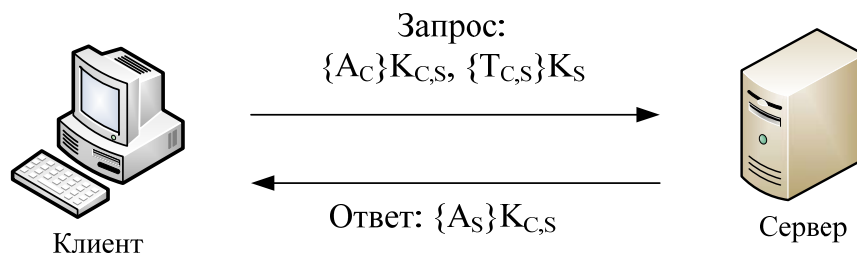


Рис 9.5. Этап доступа к клиенту

Подлинность клиента удостоверятся следующим образом. В аутентификатор A_C клиент записывает ключ $K_{C,S}$. Сервер, расшифровав сеансовый билет $T_{C,S}$ с помощью своего секретного ключа K_S , извлекает из него ключ $K_{C,S}$ и сравнивает с ключом, полученным из аутентификатора.

Если ключи совпадают, клиент является подлинным, так как он не мог изменить содержимое сеансового билета $T_{C,S}$.

Если клиенту требуется подтверждение подлинности сервера, тот отправляет ответ, который содержит аутентификатор сервера A_S , включающий параметр времени отправления из аутентификатора клиента A_C . Без знания секретного ключа K_S извлечь данный параметр из запроса клиента невозможно. Следовательно, если время отправления запроса сервер передал верно, он считается аутентифицированным.

Протокол IPsec

Протокол Kerberos применяется для аутентификации участников соединения. Но и после этапа аутентификации данные, передаваемые по сети, следует защищать. Стандартные протоколы стека TCP/IP, такие, как IP, TCP, UDP, не обладают встроенными средствами защиты. На эту проблему в 1994 году обратил внимание Совет по архитектуре Интернета (Internet Architecture Board, IAB), издав RFC 1636 «*Report of IAB Workshop on Security in the Internet Architecture*» («Отчет семинара IAB по безопасности в архитектуре Интернета»). Инициированная этим сообщением работа привела к появлению протокола *IPsec* (IP Security – безопасность IP), описанного в нескольких стандартах RFC (в частности, в RFC 2401-2412). Новая технология безопасности является необходимой частью протокола IPv6, а также может применяться и в сетях IPv4.

Протокол IPsec действует на сетевом уровне модели OSI и может применяться независимо от протоколов верхнего уровня, т. е. прикладной протокол может использовать IPsec, считая, что работает с обычным протоколом IP. При этом данные протоколов верхних уровней упаковываются в пакеты IPsec, которые, в свою очередь, помещаются в пакеты протокола IP.

Функции протокола IPsec

Протокол IPsec обеспечивает наличие следующих функций:

- аутентификация – приемник пакетов в состоянии проверить подлинность их источника;
- целостность – осуществляется контроль того, что данные дойдут до получателя в неизменном виде;
- конфиденциальность – шифрование данных обеспечивает их недоступность для несанкционированного просмотра;
- распределение секретных ключей – для правильной работы протокола IPsec необходимо автоматически обеспечивать источник и приемник пакетов секретными ключами для шифрования и расшифрования данных.

Для реализации представленных функций используются три основных протокола:

- АН (Authentication Header – заголовок аутентификации) обеспечивает целостность и аутентичность;
- ESP (Encapsulating Security Payload – инкапсуляция зашифрованных данных) предоставляет функции целостности, аутентичности и конфиденциальности;
- IKE (Internet Key Exchange – обмен ключами Интернета) генерирует и распределяет секретные ключи.

Можно заметить, что протокол ESP имеет схожие функции с протоколом АН. Пересечение функций вызвано тем, что на применение протоколов шифрования во многих странах накладываются определенные ограничения. В связи с этим оба протокола могут применяться независимо, хотя наивысший уровень защиты достигается при их совместном использовании.

На рис. 9.6 представлена структура протокола IPsec и взаимосвязь основных протоколов, входящих в его состав.

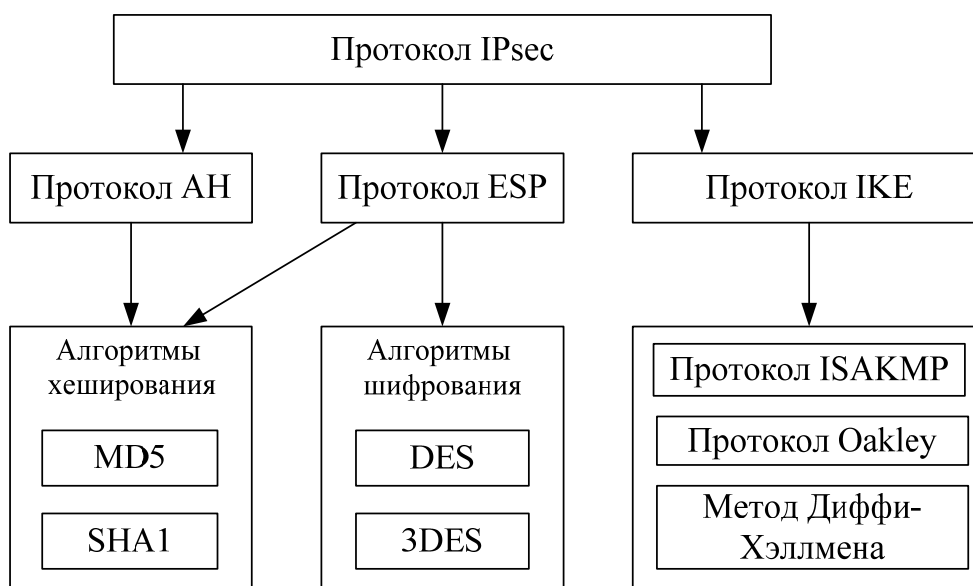


Рис. 9.6. Структура протокола IPsec

Протоколы АН и ESP

Протокол АН (описан в RFC 2402) снабжает пакет IPsec своим незашифрованным заголовком, который обеспечивает:

- аутентификацию исходных данных;
- целостность данных;
- защиту от дублирования уже полученных данных.

Первые две функции протокола АН реализуются путем применения алгоритмов хеширования (MD5¹ или SHA1²) к исходным данным. Процедура хеширования осуществляется источником с помощью секретного ключа, который был выдан источнику и приемнику пакета с использованием протокола IKE. Полученное значение хеша помещается в специальное поле заголовка АН. Приемник также осуществляет процедуру хеширования, применяя тот же секретный ключ. В том случае, если вычисленный хеш совпадает с хешем, извлеченным из пакета, данные считаются аутентифицированными и целостными. Иначе пакет в процессе передачи подвергся каким-либо изменениям и не является правильным.

Функция защиты от дублирования уже полученных пакетов осуществляется с помощью поля номера пакета в заголовке АН. В это поле приемник заносит значение счетчика, увеличивающееся при отправке каждого пакета на единицу. Приемник отслеживает номера получаемых пакетов, и, если такой номер совпадает с недавно полученным, пакет отбрасывается.

Протокол ESP (описан в RFC 2406) решает задачи, подобные протоколу АН, – обеспечение аутентификации и целостности исходных данных, а также защиту от дублирования пакетов. Кроме того, протокол ESP предоставляет средства обеспечения конфиденциальности данных при помощи алгоритмов шифрования.

Задачи аутентификации, целостности и защиты от дублирования решаются теми же методами, что и в протоколе АН. Передаваемый пакет, за исключением нескольких служебных полей, шифруется с применением алгоритмов шифрования DES и 3DES (DES с тремя ключами).

Протокол IKE

Управление секретными ключами в протоколе IPsec осуществляется при помощи протокола IKE (описан в RFC 2409). Данный протокол основан на двух протоколах: ISAKMP (Internet Security Association and Key Management Protocol – протокол межсетевой ассоциации защиты и управления ключами) и протоколе определения ключей Оакли (Oakley Key Determination Protocol).

Протокол IKE устанавливает соединение между двумя узлами сети, называемое *безопасной ассоциацией* (Security Association, SA). Безопасная ассоциация обеспечивает передачу защищенных данных только в одну сторону, поэтому для установки двустороннего соединения требуется определить две безопасные ассоциации. Для аутентификации узлов

¹ Алгоритм MD5 (Message Digest – алгоритм формирования профиля сообщения) разработан Рональдом Ривестом (Ronald Rivest). См. RFC 2403.

² Алгоритм SHA1 (Secure Hash Algorithm – алгоритм безопасного хеша) разработан Национальным институтом стандартов и технологий (NIST, National Institute of Standards and Technology). Является более стойким по сравнению с MD5. Описан в RFC 2404.

безопасной ассоциации, согласования между ними методов хеширования и шифрования IKE использует протокол ISAKMP (описан в RFC 2408).

Для генерации и обмена секретными ключами IKE использует протокол определения ключей Оакли (описан в RFC 2412), разработанный на основе метода обмена ключами Диффи-Хэллмена (Diffie-Hellman). В этом методе секретный ключ генерируется на двух узлах путем обмена двумя числами через открытую сеть. При этом перехват чисел не даст информации о ключах.

Резюме

Операционная система Windows Server 2003 предоставляет широкий набор инструментов по обеспечению безопасности в компьютерной сети. Основными инструментами являются протокол аутентификации Kerberos и протокол безопасной передачи данных IPsec.

Протокол Kerberos обеспечивает процесс безопасной аутентификации в открытых сетях, а также предоставляет возможность аутентификации сервера клиентом. Особенностью протокола является то, что в процессе аутентификации участвует кроме клиента и сервера контроллер домена, на котором работают центр распространения ключей и служба предоставления билетов.

Безопасность передачи сообщений в сетях обеспечивается протоколом IPsec. Протокол предоставляет средства аутентификации участников соединения, шифрования сообщений и процедуры обмена секретными ключами. Применение протокола IPsec является обязательным в сетях следующего поколения IPv6, а также может использоваться в современных сетях IPv4.

Контрольные вопросы

1. Безопасность каких основных процессов следует обеспечивать в сетях передачи данных?
2. Что такое сеанс?
3. Что такое хеширование?
4. Каковы функции центра распределения ключей?
5. В чем отличие билетов TGT от сеансовых билетов?
6. Опишите этап регистрации клиента.
7. Назовите основные функции протокола IPsec.
8. Для чего используются протоколы AH и ESP?

Лекция 10. Удаленный доступ и виртуальные частные сети

План лекции

- Удаленный доступ.
- Виды коммутируемых линий.
- Протоколы удаленного доступа.
- Протоколы аутентификации.
- Основные понятия и виды виртуальных частных сетей.
- Протоколы виртуальных частных сетей.
- Протокол RADIUS.
- Резюме.
- Контрольные вопросы.

Удаленный доступ

Компьютерная сеть многих организаций не ограничивается локальной сетью, размещенной в одном или нескольких близко расположенных зданиях. Пользователи могут находиться на большом удалении от основного офиса, например, если филиал находится в другом городе или если сотрудник организации уезжает в командировку в другую страну с ноутбуком.

Возможность использования удаленными пользователями ресурсов локальной сети называется *удаленным доступом* (remote access). Различают два основных вида удаленного доступа:

- соединение по коммутируемой линии (dial-up connection);
- соединение с использованием виртуальных частных сетей (Virtual Private Networks, VPN).

Оба вида соединений работают по модели «клиент-сервер». *Клиент удаленного доступа* – это компьютер, который имеет возможность подключаться к удаленному компьютеру и работать с его ресурсами или с ресурсами удаленной сети так же, как с ресурсами своей локальной сети. Единственное отличие удаленной работы от локальной с точки зрения клиента – более низкая скорость соединения. *Сервер удаленного доступа* (Remote Access Server, RAS) – это компьютер, способный принимать входящие запросы от клиентов удаленного доступа и предоставлять им собственные ресурсы или ресурсы своей локальной сети.

Компьютер с установленной операционной системой Windows Server 2003 может исполнять роль как клиента удаленного доступа, так и сервера. В последнем случае на нем должна быть запущена *Служба маршрутизации и удаленного доступа* (Routing and Remote Access Service, RRAS).

Виды коммутируемых линий

Соединения по коммутируемым линиям могут осуществляться с использованием следующих средств связи.

- Телефонные сети – наиболее распространенный и дешевый вариант, хотя и самый медленный (максимальная скорость передачи данных 56,6 кбит/с). Предполагает установку модемов на клиенте и сервере.
- Сети ISDN (Integrated Services Digital Network – цифровая сеть с комплексными услугами) обеспечивают скорость передачи данных 128 кбит/с, но их использование дороже, чем использование обычных телефонных сетей.
- ATM поверх ADSL – передача трафика ATM (Asynchronous Transfer Mode – асинхронный режим передачи) посредством линий ADSL (Asymmetric Digital Subscriber Line – асимметричная цифровая абонентская линия). В последнее время технология ADSL получила широкое развитие, так как обеспечивает высокую скорость передачи данных по обычным телефонным линиям, причем предел скорости постоянно увеличивается и составляет уже более 20 Мбит/с для входящего трафика и 1 Мбит/с для исходящего.

Для соединения посредством виртуальных частных сетей компьютер-клиент и компьютер-сервер должны быть подключены к Интернету.

В лекции сначала рассматриваются принципы организации соединений по коммутируемым линиям, затем основные понятия и протоколы виртуальных частных сетей.

Протоколы удаленного доступа

Подключение клиента к серверу удаленного доступа по коммутируемым линиям состоит из следующих основных этапов:

- установка соединения;
- аутентификация и авторизация клиента удаленного доступа;
- сервер удаленного доступа выступает в роли маршрутизатора, предоставляя доступ клиенту к ресурсам локальной сети – серверам баз данных, электронной почты, файловым серверам, принтерам и т. д.

Схема подключения представлена на рис. 10.1.

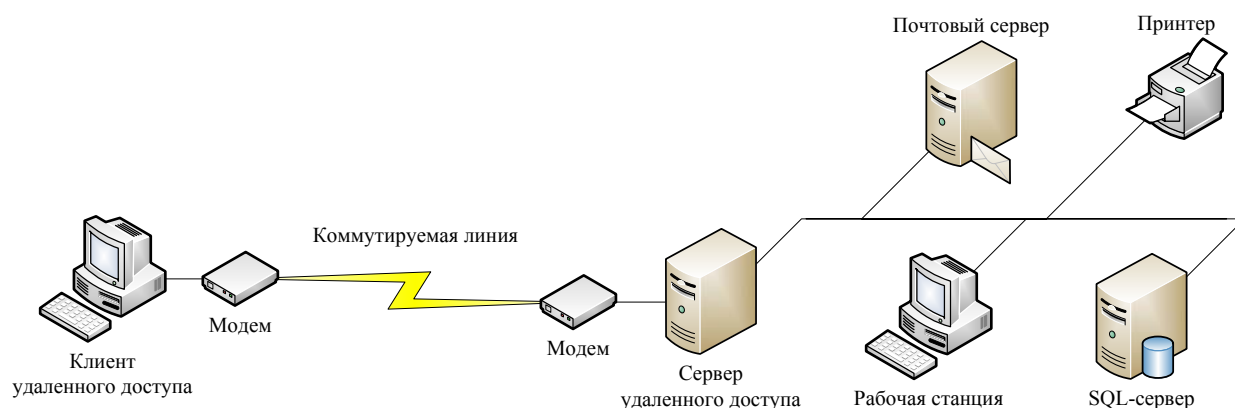


Рис. 10.1. Удаленный доступ по коммутируемым линиям

Для соединений удаленного доступа по коммутируемым линиям было разработано несколько специальных протоколов. Windows Server 2003 поддерживает два протокола удаленного доступа:

- протокол SLIP (Serial Line Internet Protocol – межсетевой протокол для последовательного канала);
- протокол PPP (Point-to-Point Protocol – протокол соединения «точка-точка»).

Протокол SLIP является одним из старейших протоколов удаленного доступа и предлагает передачу TCP/IP-пакетов без обеспечения безопасности данных и контроля целостности. Протокол описан в RFC 1055. В Windows Server 2003 поддержка протокола SLIP реализована только на уровне клиента.

Протокол PPP предназначен для коммутируемых соединений типа «точка-точка». Это означает, что в протоколе отсутствуют средства адресации, поэтому в процессе связи могут принимать участие только два компьютера – клиент и сервер¹.

Протокол PPP, в отличие от SLIP, обеспечивает функции безопасности и контроля ошибок. Описание протокола содержится в RFC 1332, 1661 и 1662.

Соединение «точка-точка» устанавливается в четыре этапа:

1. Настройка параметров канального уровня. Клиент и сервер согласовывают максимальный размер кадра, возможность сжатия, протокол аутентификации и некоторые другие параметры.

2. Аутентификация клиента. Сервер осуществляет аутентификацию и авторизацию клиента на основе протокола, выбранного на предыдущем этапе.

3. Обратный вызов (callback). В целях безопасности может использоваться процедура обратного вызова, когда сервер разрывает соединение с клиентом и сам вызывает его по определенному телефонному номеру.

¹ Существуют технологии удаленного доступа, которые имеют собственную систему адресации и могут обеспечить участие в соединении более чем двух компьютеров, например ATM.

4. Настройка протоколов верхних уровней. Сервер отправляет клиенту список протоколов верхних уровней, отвечающих за передачу данных, шифрование и сжатие. Клиент выбирает один из подходящих протоколов списка.

Протоколы аутентификации

Важнейшим этапом при установлении соединения удаленного доступа является аутентификация клиента. В большинстве случаев аутентификация осуществляется путем передачи пароля. Данный процесс осложнен отсутствием защиты открытых линий связи, поэтому данные, передаваемые в ходе аутентификации, должны шифроваться.

Разработано несколько протоколов, используемых для аутентификации удаленных клиентов.

- PAP (Password Authentication Protocol) – протокол аутентификации по паролю (описан в RFC 1334). Самый простой протокол аутентификации, в котором имя пользователя и пароль передаются открытым, незашифрованным способом. В Windows Server 2003 протокол PAP применяется только в том случае, если клиент удаленного доступа не поддерживает больше никаких протоколов.

- CHAP (Challenge Handshake Authentication Protocol) – протокол аутентификации с предварительным согласованием вызова (описан в RFC 1994). В этом протоколе клиент посылает серверу пароль в виде специальной хеш-последовательности, созданной с использованием алгоритма MD-5. Сервер принимает хеш пароля клиента, вычисляет хеш по хранимому у себя паролю и сравнивает обе последовательности. В случае совпадения соединение устанавливается, иначе происходит разрыв. Недостатком является отсутствие взаимной аутентификации, т. е. сервер аутентифицирует клиента, а клиент не получает информации о подлинности сервера.

- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) – реализация протокола CHAP, разработанная Microsoft (описан в RFC 2433). Действует по принципу протокола CHAP, за исключением того, что для хеширования используется алгоритм MD-4, а не MD-5.

- MS-CHAP v2 – вторая версия протокола MS-CHAP (описан в RFC 2759). Также применяется алгоритм хеширования MD-4, отличием является требование взаимной аутентификации. Между клиентом и сервером происходит обмен следующими сообщениями:

- сервер отправляет клиенту сообщение, содержащее некоторую последовательность символов, называемую строкой вызова;
- клиент отправляет серверу хеш-последовательность, полученную на основе строки вызова и пароля пользователя, а также свою строку вызова для сервера;
- сервер вычисляет хеш по своей строке вызова и пользовательскому паролю, сравнивает его с полученным хешем

от клиента и в случае успеха отправляет хеш, вычисленный на основе своей строки вызова, строки вызова от клиента, имени и пароля пользователя;

- клиент, получая сообщение сервера, вычисляет хеш на основе тех же данных, и в случае совпадения вычисленного хеша с полученным от сервера процесс взаимной аутентификации считается законченным успешно.

- EAP (Extensible Authentication Protocol) – расширяемый протокол аутентификации (описан в RFC 2284). Отличается от вышеописанных протоколов тем, что выбор типа аутентификации EAP происходит в процессе соединения. В Windows Server 2003 применяются следующие типы аутентификации EAP: EAP-MD5 CHAP, EAP-TLS (Transport Level Security, безопасность на транспортном уровне), PEAP (Protected EAP, защищенный EAP).

Информацию об именах пользователей-клиентов удаленного доступа серверы могут получать, используя либо каталог Active Directory, либо сервер RADIUS, рассмотренный далее в этой лекции.

Основные понятия и виды виртуальных частных сетей

Соединение посредством коммутируемых линий долгое время оставалось единственным решением проблемы связи локальных сетей с удаленными пользователями. Однако данное решение является довольно дорогим и недостаточно безопасным.

В последние годы стоимость использования каналов связи Интернета стала уменьшаться и скоро стала ниже, чем цена использования коммутируемых линий. Однако при установлении соединения через Интернет серьезной проблемой является обеспечение безопасности, так как сеть является открытой и злоумышленники могут перехватывать пакеты с конфиденциальной информацией. Решением этой проблемы стала технология виртуальных частных сетей.

Виртуальные частные сети (Virtual Private Network, VPN) – это защищенное соединение двух узлов через открытые сети. При этом организуется виртуальный канал, обеспечивающий безопасную передачу информации, а узлы, связанные VPN, могут работать так, как будто соединены напрямую.

Компьютер, иницирующий VPN-соединение, называется *VPN-клиентом*. Компьютер, с которым устанавливается соединение, называется *VPN-сервером*. *VPN-магистраль* – это последовательность каналов связи открытой сети, через которые проходят пакеты виртуальной частной сети.

Существует два типа VPN-соединений:

- соединение с удаленными пользователями (Remote Access VPN Connection);
- соединение маршрутизаторов (Router-to-Router VPN Connection).

Соединение с удаленными пользователями осуществляется в том случае, если одиночный клиент подключается к локальной сети организации через VPN (рис. 10.2). Другие компьютеры, подключенные к VPN-клиенту, не могут получить доступ к ресурсам локальной сети.

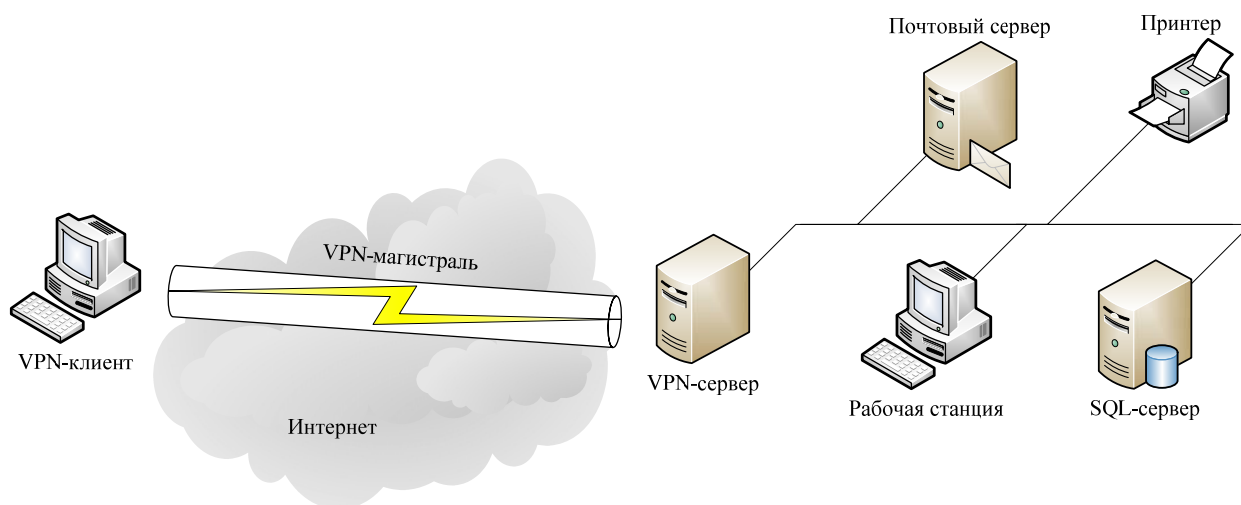


Рис. 10.2. VPN-соединение с удаленным пользователем

Соединение маршрутизаторов устанавливается между двумя локальными сетями, если узлы обеих сетей нуждаются в доступе к ресурсам друг друга (рис. 10.3). При этом один из маршрутизаторов играет роль VPN-сервера, а другой – VPN-клиента.

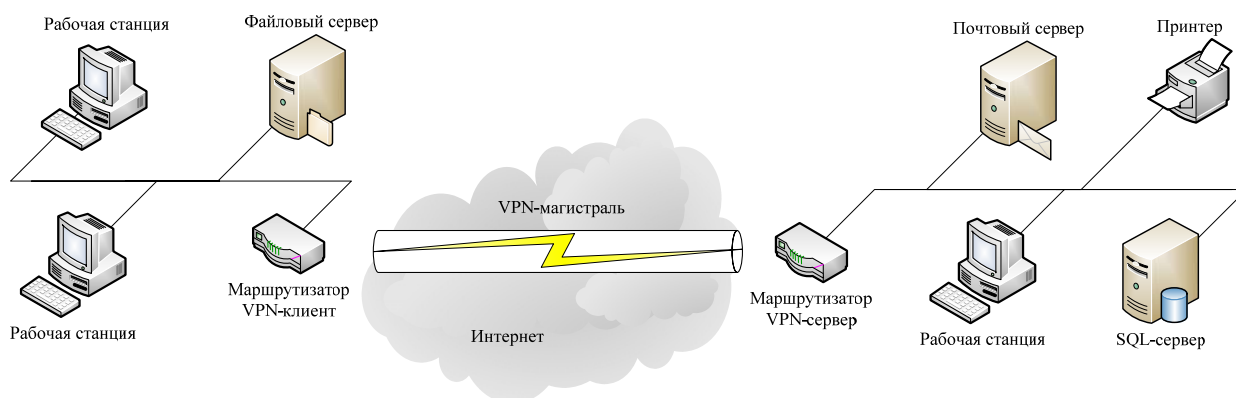


Рис. 10.3. VPN-соединение между маршрутизаторами

VPN-соединение возможно не только через Интернет, но и в рамках локальной сети. Например, если нужно организовать безопасный канал связи между двумя отделами или пользователями, недоступный другим подразделениям организации, можно применить один из типов VPN-соединений.

Протоколы виртуальных частных сетей

Безопасность передачи IP-пакетов через Интернет в VPN реализуется с помощью туннелирования. *Туннелирование* (tunneling) – это процесс включения IP-пакетов в пакеты другого формата, позволяющий передавать зашифрованные данные через открытые сети.

В Windows Server 2003 поддерживаются следующие протоколы туннелирования:

1. PPTP (Point-to-Point Tunneling Protocol) – протокол туннелирования соединений «точка-точка», основан на протоколе PPP (описан в RFC 2637). Поддерживает все возможности, предоставляемые PPP, в частности аутентификацию по протоколам PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP. Шифрование данных обеспечивается методом MPPE (Microsoft Point-to-Point Encryption), который применяет алгоритм RSA/RC4. Сжатие данных происходит по протоколу MPPE (Microsoft Point-to-Point Compression), описанному в RFC 2118.

Недостатком протокола является относительно низкая скорость передачи данных.

2. L2TP (Layer 2 Tunneling Protocol – туннельный протокол канального уровня) – протокол туннелирования, основанный на протоколе L2F (Layer 2 Forwarding), разработанном компанией Cisco, и протоколе PPTP. Описан в RFC 2661. Поддерживает те же протоколы аутентификации, что и PPP. Для шифрования данных используется протокол IPsec. Также поддерживает сжатие данных. Имеет более высокую скорость передачи данных, чем PPTP.

Протокол PPTP остается единственным протоколом, который поддерживают старые версии Windows (Windows NT 4.0, Windows 98, Windows Me). Однако существует бесплатный VPN-клиент Microsoft L2TP/IPsec, который позволяет старым операционным системам Windows устанавливать соединение VPN по протоколу L2TP.

Информация для аутентификации об именах пользователей и их паролях, так же как при удаленном доступе, извлекается либо из каталога Active Directory, либо из базы данных RADIUS-сервера.

Протокол RADIUS

Протокол RADIUS (Remote Authentication Dial-In User Service – служба аутентификации пользователей удаленного доступа) предназначен для аутентификации, авторизации и учета удаленных пользователей и обеспечивает единый интерфейс для систем на разных платформах (Windows, UNIX и т. д.). Протокол описан в RFC 2865 и 2866.

Протокол RADIUS работает по модели «клиент-сервер». RADIUS-сервер хранит данные о пользователях, RADIUS-клиенты обращаются к серверу за информацией.

В Windows Server 2003 протокол RADIUS входит в состав двух служб: служба Интернет-аутентификации IAS (Internet Authentication Service) реализует RADIUS-сервер, а при помощи службы маршрутизации и удаленного доступа RRAS можно настроить RADIUS-клиент.

Схема сети с применением RADIUS-сервера показана на рис. 10.4. В этой схеме RADIUS-сервер установлен на контроллер домена и интегрирован со службой каталога Active Directory.

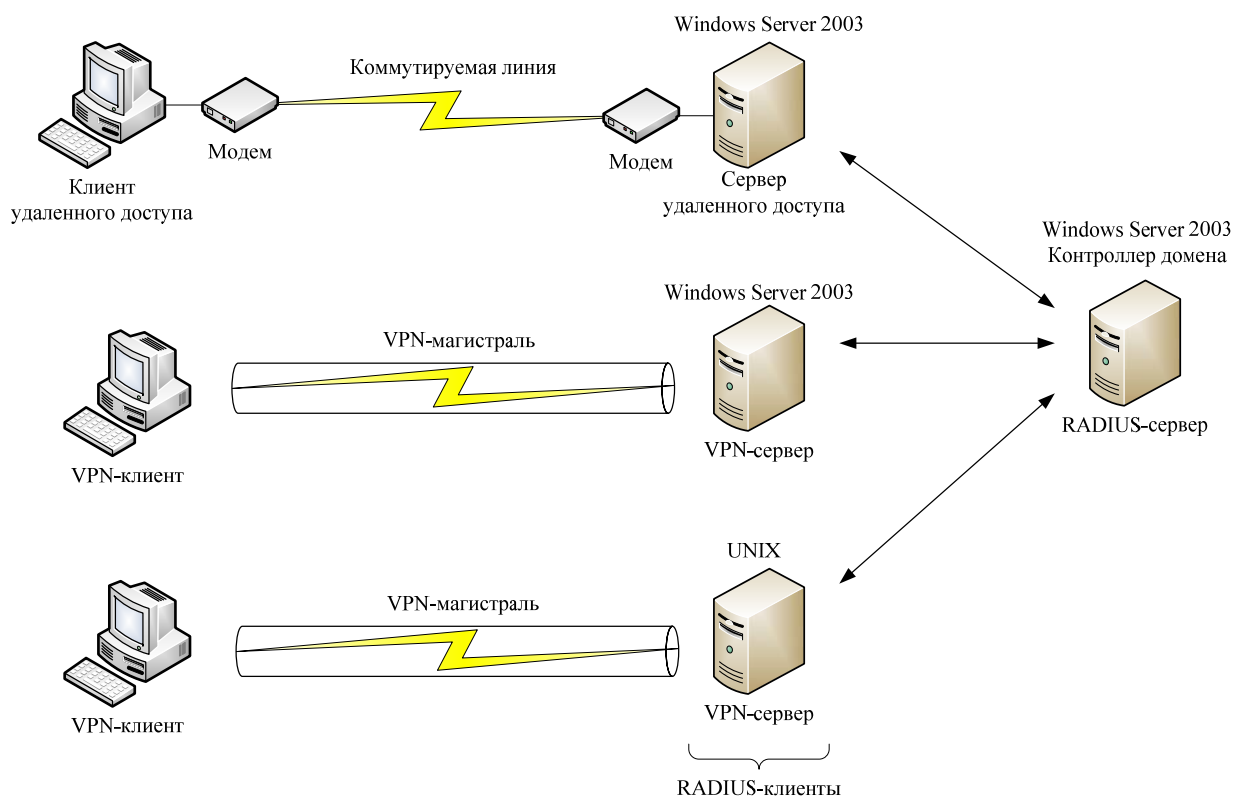


Рис. 10.4. Схема применения протокола RADIUS

Резюме

Удаленный доступ – это предоставление пользователям, находящимся вне локальной сети, возможности доступа к ресурсам этой сети. Существует два способа удаленного доступа – соединение по коммутируемой линии и соединение с использованием виртуальных частных сетей VPN. Участниками обоих видов соединений являются клиент и сервер удаленного доступа.

Доступ по коммутируемым линиям может осуществляться с использованием телефонных линий, линий ISDN или посредством ATM поверх ADSL. Для таких соединений применяются протоколы PPP и SLIP. При аутентификации клиентов удаленного доступа используются протоколы PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP.

Виртуальные частные сети VPN позволяют организовать канал безопасной передачи данных в Интернете или в локальной сети. Действие VPN основано на туннелировании, т. е. включении обычных IP-пакетов в

зашифрованные пакеты другого формата. В сетях VPN используются протоколы PPP и L2TP.

Для обеспечения единого интерфейса к базе данных учетных записей клиентов удаленного доступа в смешанных сетях (Windows, Unix и другие платформы) может использоваться протокол RADIUS.

Контрольные вопросы

1. Что такое удаленный доступ?
2. Назовите виды удаленного доступа.
3. В чем отличие протоколов удаленного доступа SLIP и PPP?
4. Для чего нужна аутентификация при удаленном доступе?
5. Опишите алгоритм работы MS-CHAP v2.
6. Каким образом сети VPN обеспечивают безопасную передачу пакетов?
7. Назовите виды VPN-соединений.
8. Перечислите достоинства и недостатки протоколов PPTP и L2TP.
9. Что такое RADIUS?

Библиографический список

1. Вишневский А. Windows Server 2003. Для профессионалов. – СПб.: Питер, 2004.
2. Дэвис Дж., Ли Т. Microsoft Windows Server 2003. Протоколы и службы TCP/IP. Техническое руководство. – М.: «СП ЭКОМ», 2005. – 752 с.
3. Зубанов Ф. В. Active Directory: подход профессионала. – М.: Русская редакция, 2003.
4. Иртегов Д. В. Введение в сетевые технологии. – СПб.: БХВ-Петербург, 2004.
5. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. – 3-е изд. – СПб.: Питер, 2006.
6. Реймер С., Малкер М. Active Directory для Windows Server 2003. Справочник администратора. – М.: «СП ЭКОМ», 2004.
7. Спилман Дж., Хадсон К., Крафт М. Планирование, внедрение и поддержка инфраструктуры Active Directory Microsoft Windows Server 2003. Учебный курс Microsoft. – М.: Русская редакция; СПб.: Питер, 2006.
8. Станек У. Microsoft Windows Server 2003: Справочник администратора. – М.: Русская редакция, 2006.
9. Хассел Дж. Администрирование Windows Server 2003. – СПб.: Питер, 2006.
10. Чекмарев А. П., Вишневский А. В., Кокорева О. И. Microsoft Windows Server 2003. Русская версия / Под общ. ред. Н. Чекмарева. – СПб.: БХВ-Петербург, 2004.

ПРИЛОЖЕНИЯ

Приложение I. Документы RFC

В этом приложении перечислены документы RFC, упоминаемые в лекционном курсе.

Номер	Название	Статус	Дата выхода
791	<i>Internet Protocol (IP)</i> (Протокол Интернета)	STANDARD	1981
950	<i>Internet Standard Subnetting Procedure</i> (Процедура деления Интернет на подсети)	STANDARD	1985
1001	<i>Protocol standard for a NetBIOS service on a TCP/UDP transport: Concepts and methods</i> (Стандарт протокола для NetBIOS на TCP/UDP транспорте: концепции и методы)	STANDARD	1987
1002	<i>Protocol standard for a NetBIOS service on a TCP/UDP transport: Detailed specifications</i> (Стандарт протокола для NetBIOS на TCP/UDP транспорте: детальные спецификации)	STANDARD	1987
1034	<i>Domain names – concepts and facilities</i> (Доменные имена – концепции и возможности)	STANDARD	1987
1035	<i>Domain names – implementation and specification</i> (Доменные имена – реализация и спецификация)	STANDARD	1987
1055	<i>Nonstandard for transmission of IP datagrams over serial lines: SLIP</i> (Нестандартная передача IP-дейтаграмм через последовательные линии: SLIP)	STANDARD	1988
1332	<i>The PPP Internet Protocol Control Protocol (IPCP)</i> (Управляющий протокол Интернет протокола PPP)	PROPOSED STANDARD	1992
1334	<i>PPP Authentication Protocols</i> (Протоколы аутентификации PPP)	PROPOSED STANDARD	1992
1510	<i>The Kerberos Network Authentication Service (V5)</i> (Служба сетевой аутентификации Kerberos, версия 5)	PROPOSED STANDARD	1993
1636	<i>Report of IAB Workshop on Security in the Internet Architecture</i> (Отчет семинара IAB по безопасности в архитектуре Интернета)	INFORMATIONAL	1994
1661	<i>The Point-to-Point Protocol (PPP)</i> (Протокол точка-точка)	STANDARD	1994
1662	<i>PPP in HDLC-like Framing</i> (PPP в кадрах, подобных HDLC)	STANDARD	1994
1723	<i>RIP Version 2 – Carrying Additional Information</i> (RIP версии 2 – перенос дополнительной информации)	STANDARD	1994
1918	<i>Address Allocation for Private Internets</i> (Распределение адресов для частных сетей)	BEST CURRENT PRACTICE	1996

Номер	Название	Статус	Дата выхода
1994	<i>PPP Challenge Handshake Authentication Protocol (CHAP)</i> (Протокол аутентификации PPP с предварительным согласованием вызова)	DRAFT STANDARD	1996
2026	<i>The Internet Standards Process – Revision 3</i> (Процесс стандартизации Интернета – 3-я редакция)	BEST CURRENT PRACTICE	1996
2118	<i>Microsoft Point-To-Point Compression (MPPC) Protocol</i> (Протокол сжатия Microsoft для PPP)	INFORMATIONAL	1997
2131	<i>Dynamic Host Configuration Protocol</i> (Протокол динамической конфигурации хостов)	DRAFT STANDARD	1997
2132	<i>DHCP Options and BOOTP Vendor Extensions</i> (Опции DHCP и расширения производителей)	DRAFT STANDARD	1997
2284	<i>PPP Extensible Authentication Protocol (EAP)</i> (Протокол расширяемой аутентификации PPP)	PROPOSED STANDARD	1998
2328	<i>OSPF Version 2</i> (OSPF версия 2)	STANDARD	1998
2373	<i>IP Version 6 Addressing Architecture</i> (Архитектура IP-адресации версии 6)	PROPOSED STANDARD	1998
2401	<i>Security Architecture for the Internet Protocol</i> (Архитектура безопасности для протокола Интернета)	PROPOSED STANDARD	1998
2402	<i>IP Authentication Header</i> (Заголовок аутентификации IP)	PROPOSED STANDARD	1998
2403	<i>The Use of HMAC-MD5-96 within ESP and AH</i> (Использование алгоритма HMAC-MD5-96 в протоколах ESP и AH)	PROPOSED STANDARD	1998
2404	<i>The Use of HMAC-SHA-1-96 within ESP and AH</i> (Использование алгоритма HMAC-SHA-1-96 в протоколах ESP и AH)	PROPOSED STANDARD	1998
2406	<i>IP Encapsulating Security Payload (ESP)</i> (Инкапсуляция безопасной нагрузки IP)	PROPOSED STANDARD	1998
2408	<i>Internet Security Association and Key Management Protocol (ISAKMP)</i> (Протокол межсетевой ассоциации защиты и управления ключами)	PROPOSED STANDARD	1998
2409	<i>The Internet Key Exchange (IKE)</i> (Обмен ключами Интернета)	PROPOSED STANDARD	1998
2412	<i>The OAKLEY Key Determination Protocol</i> (Протокол определения ключей Оакли)	INFORMATIONAL	1998
2433	<i>Microsoft PPP CHAP Extensions</i> (Расширения Microsoft PPP CHAP)	INFORMATIONAL	1998
2460	<i>Internet Protocol, Version 6 (IPv6) Specification</i> (Протокол Интернета, спецификация версии 6)	DRAFT STANDARD	1998
2637	<i>Point-to-Point Tunneling Protocol</i> (Протокол туннелирования «точка-точка»)	INFORMATIONAL	1999
2661	<i>Layer Two Tunneling Protocol "L2TP"</i> (туннельный протокол канального уровня «L2TP»)	PROPOSED STANDARD	1999

Номер	Название	Статус	Дата выхода
2759	<i>Microsoft PPP CHAP Extensions, Version 2</i> (Расширения Microsoft PPP CHAP, версия 2)	INFORMATIONAL	2000
2865	<i>Remote Authentication Dial In User Service (RADIUS)</i> (служба аутентификации пользователей удаленного доступа (RADIUS))	DRAFT STANDARD	2000
2866	<i>RADIUS Accounting</i> (Учетные записи RADIUS)	INFORMATIONAL	2000
3700	<i>Internet Official Protocol Standards</i> (Стандарты официальных протоколов Интернета)	STANDARD	2004

Приложение II. Домены первого уровня

1. Домены организаций

TLD	Применение
.aero	Зарезервировано для авиационных организаций
.biz	Коммерческие организации (домен, альтернативный домену .com)
.com	Коммерческие организации
.coop	Кооперативы
.edu	Образовательные учреждения США
.gov	Агентства правительства США
.info	Хосты домена предоставляют информацию в неограниченное пользование
.int	Международные организации
.mil	Вооруженные силы США
.museum	Музейные организации
.name	Домен для индивидуального использования (возможно, для глобальной идентификации пользователей)
.net	Домен интернет-провайдеров
.org	Другие некоммерческие организации
.pro	Профессиональный домен (для врачей, адвокатов, бухгалтеров и т. д.)

2. Географические домены

TLD	Страна	TLD	Страна	TLD	Страна
.ae	ОАЭ	.gi	Гибралтар	.ng	Нигерия
.al	Албания	.gl	Гренландия	.ni	Никарагуа
.am	Армения	.gm	Гамбия	.nl	Нидерланды
.ar	Аргентина	.gp	Гваделупа	.no	Норвегия
.at	Австрия	.gr	Греция	.np	Непал
.au	Австралия	.gt	Гватемала	.nz	Новая Зеландия
.ba	Босния и Герцеговина	.hk	Гонконг	.pa	Панама
.bd	Бангладеш	.hr	Хорватия	.pe	Перу
.be	Бельгия	.ht	Гаити	.ph	Филиппины
.bg	Болгария	.hu	Венгрия	.pk	Пакистан
.bh	Бахрейн	.id	Индонезия	.pl	Польша
.bo	Боливия	.ie	Ирландия	.pt	Португалия
.br	Бразилия	.il	Израиль	.py	Парагвай
.bz	Белиз	.in	Индия	.ro	Румыния
.ca	Канада	.iq	Ирак	.ru	Россия

TLD	Страна	TLD	Страна	TLD	Страна
.cd	Конго	.ir	Иран	.sa	Саудовская Аравия
.ch	Швейцария	.is	Исландия	.sd	Судан
.ci	Кот-д'Ивуар	.it	Италия	.se	Швеция
.cl	Чили	.jo	Иордания	.sg	Сингапур
.cm	Камерун	.jp	Япония	.si	Словения
.cn	Китай	.ke	Кения	.sk	Словакия
.co	Колумбия	.kr	Южная Корея	.sl	Сьерра-Леоне
.cr	Коста-Рика	.kw	Кувейт	.sn	Сенегал
.cu	Куба	.lb	Ливан	.sy	Сирия
.cv	Кабо-Верде	.li	Лихтенштейн	.td	Чад
.cy	Кипр	.lk	Шри-Ланка	.th	Таиланд
.cz	Чехия	.lt	Литва	.tn	Тунис
.de	Германия	.lu	Люксембург	.tr	Турция
.dk	Дания	.lv	Латвия	.tw	Тайвань
.do	Доминиканская Республика	.ly	Ливия	.ua	Украина
.dz	Алжир	.ma	Марокко	.uk	Великобритания
.ec	Эквадор	.mc	Монако	.us	США
.ee	Эстония	.md	Молдова	.uy	Уругвай
.eg	Египет	.mg	Мадагаскар	.ve	Венесуэла
.es	Испания	.mk	Македония	.vn	Вьетнам
.eu	Европейский союз	.mq	Мартиника	.ye	Йемен
.fi	Финляндия	.mt	Мальта	.za	Южная Африка
.fj	Фиджи	.mv	Мальдивы	.zm	Замбия
.fm	Микронезия	.mx	Мексика	.zw	Зимбабве
.fr	Франция	.my	Малайзия		
.gh	Гана	.na	Намибия		

Домен **.su** являлся доменом Советского Союза. После распада СССР новые страны получили свои национальные домены, однако домен **.su** действует до сих пор.

Приложение III. Права пользователей

В Windows Server 2003 существуют следующие типы прав пользователей:

- привилегия (privilege);*
- право на вход в систему (logon right);*
- разрешение доступа (access permission)*

1. Привилегии

В таблице приведены некоторые виды привилегий пользователя.

Привилегия	Примечание
Архивирование файлов и каталогов (Back up files and directories)	Независимо от разрешений доступа
Добавление рабочих станций к домену (Add workstations to domain)	
Завершение работы системы (Shut down the system)	
Загрузка и выгрузка драйверов устройств (Load and unload device drivers)	Позволяет пользователям устанавливать новые устройства и удалять уже установленные
Изменение системного времени (Change the system time)	
Принудительное удаленное завершение (Force shutdown of a remote system)	Позволяет пользователям выключать удаленный компьютер

2. Права на вход в систему

В таблице перечислены некоторые из возможных прав на вход в систему.

Права на вход в систему	Примечание
Доступ к компьютеру из сети (Access this computer from the network)	Разрешает удаленный доступ к компьютеру
Отказ в доступе к компьютеру из сети (Deny access to this computer from the network)	Запрещает удаленный доступ к компьютеру
Локальный вход в систему (Allow logon locally)	Разрешает доступ к компьютеру с клавиатуры этого компьютера
Отклонить локальный вход (Deny logon locally)	Запрещает доступ к компьютеру с клавиатуры этого компьютера

3. Разрешения на доступ к объектам¹

В таблице приведены виды разрешений на доступ к разным типам объектов. Для каждого вида разрешений может быть выбрано *Разрешить* (Allow) или *Запретить* (Deny).

Тип объекта	Разрешение	Описание
Объекты Active Directory	Control Access	Доступ к управлению объектом
	List Object	Просмотр свойств объекта
	List Contents	Просмотр содержимого объекта контейнерного типа
	Create Child	Возможность создания дочерних объектов внутри объектов-контейнеров
	Delete Child	Возможность удаления дочерних объектов внутри объектов-контейнеров
	Write Self	Возможность добавить самого пользователя в качестве объекта
	Delete Tree	Возможность удаления дерева в каталоге
	Read Property	Просмотр отдельного свойства объекта
	Write Property	Возможность изменения отдельного свойства объекта
Файлы	Read	Чтение файла
	Read & Execute	Чтение файла и запуск на выполнение
	Write	Запись в файл, а также изменение атрибутов файла
	Modify	Чтение, запись и возможность удаления файла
	Full Control	Полный доступ (любые действия, в том числе изменение разрешений)
Каталоги	List Folder Contents	Просмотр содержимого каталога
	Read	Просмотр содержимого каталога без возможности запуска файлов и просмотра содержимого подкаталогов
	Read & Execute	Просмотр содержимого каталога и всех его файлов и подкаталогов
	Write	Возможность создания файлов и подкаталогов
	Modify	Чтение, запись и возможность удаления файлов и подкаталогов
	Full Control	Полный доступ
Каталог общего доступа	Read	Просмотр содержимого каталога и чтение его файлов
	Change	Возможность изменения содержимого каталога
	Full Control	Полный доступ
Принтеры	Print	Возможность печати документов
	Manage Documents	Возможность печати документов, а также управление очередью печати
	Manage Printer	Полный контроль над принтером

¹ Разрешения на доступ к объектам файловой системы могут быть использованы только на дисках с файловой системой NTFS. Если диски отформатированы в FAT32, то разрешения могут устанавливаться лишь для каталогов общего доступа.